

NATIONAL ARCHIVES

July 16, 2024

Mr. William F. Marshall
Judicial Watch
425 3rd Street, SW
Suite 800
Washington, D.C. 20024

Re: Freedom of Information and Privacy Act Request NGC16-100

Dear Mr. Marshall:

This is in response to your Freedom of Information Act (FOIA) request dated December 2, 2015. Your request was received in our office on December 4, 2015 and assigned FOIA tracking number NGC16-100. We apologize for the long delay in responding to our request. In your request you asked for the access to,

“any and all records regarding, concerning or relating to the improper removal of documents from NARA facilities by former National Security Advisor Samuel (“Sandy”) Berger, including but not limited to investigative reports, incident reports, witness statements, logbook entries, investigators’ notes and audio/visual recordings associated with the removal(s). Any and all records of communication sent to or from NARA officials concerning the removal of the aforementioned documents. The time frame for the requested communications is September 2, 2003 through September 8, 2005. Copies of the documents that were improperly removed by Samuel Berger.”

After conducting a search, we identified 415 pages responsive to your FOIA request. We have reviewed the documents and are releasing 370 pages (combined into two (2) documents) with information withheld, in part, pursuant to FOIA exemptions 5 U.S.C. § 552(b)(5) for inter-agency and intra-agency deliberations and attorney-client privilege; 5 U.S.C. § 552(b)(6) for unwarranted invasion of personnel privacy; 5 U.S.C. § 552(b)(7)(e) for the protection to all law enforcement information that would disclose techniques and procedures for law enforcement investigations; and 5 U.S.C. § 552(b)(7)(c) for protection for personal information in law enforcement records. The released files consists of memorandums, notes, news reports, and emails (with attachments). Pages 140-175 within “Combined File b” have previously redacted

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION

8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001

www.archives.gov

information. Also included is a previously redacted version of the investigation report within “Combine File a”.

One (1) document totaling two (2) pages is being withheld in full pursuant to 5 U.S.C. § 552(b)(3) statute Fed. R. Crim. Pro 6(e) - Federal Grand Jury.

One (1) document, totaling one (1) page is being referred to the Federal Bureau of investigation (FBI) for review and direct response to you.

The documents that were improperly removed by Samuel Berger consisted of one (1) fax and three (3) printed emails totaling 42 pages. These documents are being withheld in full pursuant to 5 U.S.C. § 552(b)(1) which protects from disclosure information that has been deemed classified. You may file a Mandatory Declassification Review (MDR) request with the William J. Clinton Library to have these documents reviewed. Please see the following webpage for more information including how to submit an MDR with the Clinton Library:

<https://www.clintonlibrary.gov/research/mdr/>

This completes the processing of your request.

If you are not satisfied with our action on this request, you have the right to file an administrative appeal within ninety (90) calendar days from the date of this letter via regular U.S. mail or email. By filing an appeal, you preserve your rights under FOIA and give the agency a chance to review and reconsider your request and the agency’s decision. If you submit your appeal in writing, please address it to the Deputy Archivist of the United States (ND), National Archives and Records Administration, 8601 Adelphi Road, College Park, Maryland 20740. Both the letter and the envelope should be clearly marked “Freedom of Information Act Appeal.” If you submit your appeal by e-mail please send it to FOIA@nara.gov, also addressed to the Deputy Archivist of the United States. Please be sure to explain why you believe this response does not meet the requirements of the FOIA. All correspondence should reference your case tracking number NGC16-100.

If you would like to discuss our response before filing an appeal to attempt to resolve your dispute without going through the appeals process, you may contact our FOIA Public Liaison Gary M. Stern for assistance at:

National Archives and Records Administration
8601 Adelphi Road, Room 3110
College Park, MD 20740-6001
Tel: 301-837-1750
Email: NGC.public.liaison@nara.gov

If you are unable to resolve your FOIA dispute through our FOIA Public Liaison, the Office of Government Information Services (OGIS), the Federal FOIA Ombudsman’s office, offers mediation services to help resolve disputes between FOIA requesters and Federal agencies. The contact information for OGIS is noted below:


Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road–OGIS
College Park, MD 20740-6001
Email: ogis@nara.gov
Website: ogis.archives.gov
Tel: 202-741-5770 or 1-877-684-6448

Thank you for contacting the National Archives and Records Administration. Please feel free to contact me directly if you have any questions or further concerns.


Sincerely,

Jodi L. Foor
Deputy FOIA Officer
Office of General Counsel
Jodi.Foor@nara.gov
301-837-2099

MEMORANDUM OF INTERVIEW OR ACTIVITY

Type of Activity: <input checked="" type="checkbox"/> Personal Interview <input type="checkbox"/> Telephone Interview <input type="checkbox"/> Records Review <input type="checkbox"/> Other	Date and Time: July 8, 2005 9:30 a.m.
Activity or Interview of: Samuel R. Berger	Conducted by:  b6, b7C Location of Interview/Activity: Washington, DC




Subject Matter/Remarks

On July 8, 2005,  interviewed Samuel "Sandy" R. Berger, former National Security Advisor (NSA) to President William J. Clinton, at the Bond Building, 1400 New York Avenue, Washington, DC. Mr. Berger participated as part of his plea agreement. b6, b7C

Also present were  b6, b7C

Mr. Berger described his personality as intense and a uni-tasker. He did not believe anyone would describe him as arrogant. He did not feel he was overbearing and did not seek to intimidate anyone while at the Archives. Mr. Berger provided the following information:

Mr. Berger visited the Archives, Washington, DC, to review documents requested from the Clinton Presidential materials. Mr. Berger did not have a vivid recollection of visiting the Archives on May 30, 2002, to review documents in preparation for his testimony before the Graham-Goss / Joint Intelligence Committee. Mr. Berger did recall his visits to the Archives to review documents to determine if Executive Privilege needed to be exerted prior to documents being provided to the National Commission on Terrorist Attacks Upon the United States (hereafter, the 9/11 Commission).

On every visit to the Archives, Mr. Berger came in the Pennsylvania Avenue entrance of the Archives, proceeded through the magnetometer, and signed a log book at the security desk. Someone from security called , office and someone from  office would escort Mr. Berger to  office. Mr. Berger always left late in the b6, b7C

Case Number:  b2	Case Title: Samuel R. Berger  b2
---	--

ENCLOSURE (7)

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

evening, around 7 p.m. There were no guards in the lobby at that time. Therefore, no one ever checked his belongings on his way out.

[redacted] was very professional and courteous. However, [redacted] was not warm and "fuzzy" with Mr. Berger. [redacted] told Mr. Berger he could take notes while he was at the Archives but [redacted] made it clear he could not remove them. He did not understand the documents could have been sent to the National Security Council (NSC) for review and classification. [Mr. Berger did ask that his notes from his May 2002 review be sent to the NSC for review. The NSC returned his notes as classified.] He did understand the notes would remain at the Archives for him to use on subsequent visits.

b6,
b7C

All document reviews by Mr. Berger were conducted in [redacted] office. Mr. Berger sat at a small table in [redacted] office. [redacted] did not brief Mr. Berger on security procedures. [redacted] must have assumed a briefing was not required due to his previous positions as the NSA. [redacted] did not advise Mr. Berger on what he could and could not bring into the Archives. [redacted] did not provide Mr. Berger paper. On every visit, Mr. Berger brought his leather portfolio with a note pad inside. It was his practice to wear a suit but he did not recall if he wore a coat to the Archives.

b6,
b7C

Mr. Berger did not believe he received preferential treatment until after his visits when he learned [redacted] office was not an appropriate facility to view classified material. Mr. Berger believed he was afforded the opportunity to review documents in a more comfortable environment after someone described the [redacted] accommodations to him. At the time of his review, Mr. Berger did not know nor did he consider the nature of [redacted] office and whether [redacted]. He believed he was in a suitable location to review the documents. Mr. Berger did not consider asking that the documents be sent to another location for review as he was not aware of another convenient location to conduct the review.

b2,
b6,
b7C

Mr. Berger stated [redacted] of the protocol in reviewing these records [redacted] his notes had to remain at the Archives and the Archives would send them to the NSC for classification.

b6,
b7C

Mr. Berger made a general statement that he went to the restroom on an average of every thirty minutes to one hour to use the facilities and stretch his legs. This was the only room he went to besides [redacted] office.

b6,
b7C

Mr. Berger explained that after 9/11, the Clinton Administration was inundated with calls on their response to this terrorist attack. It was obvious he was going to have to testify on their actions. Mr. Berger put in over 100 hours of his time, unpaid, in order to be responsive. Everyone else stepped back from the questions but Mr. Berger felt responsible.

Mr. Berger reviewed the documents at the Archives not only for privilege but also to refresh his recollection for his testimony and assisting in preparing others [redacted] for their testimony. [redacted] only had tangential contact with the records. Mr. Berger had unique knowledge of the records and the appropriate clearances.

b5, b6
b7C

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

In May or June 2003, [redacted] called Mr. Berger to say [redacted] received a request from the 9/11 Commission. [redacted] acted as the liaison between the Clinton Administration and the Archives. [redacted] asked Mr. Berger to go to the Archives to review records in response to the Executive Office of the President's (EOP) requests.

b6,
b7c

On July 18, 2003, Mr. Berger reviewed material in response to EOP 2. The boxes of materials were on a cart in [redacted] office between Mr. Berger's seat and the coffee table, or off to his side. [redacted] handed Mr. Berger "bunches" of folders. Once he completed the review, [redacted] would hand him another bunch. If [redacted] was not sitting with Mr. Berger, [redacted] was working at [redacted] desk, usually on the computer at an angle to him where he could see [redacted] over his right shoulder.

b6,
b7c

The documents were not organized chronologically. Mr. Berger would read the documents, trying to save all his questions instead of interrupting [redacted] work. He was trying to be sensitive to [redacted] work responsibilities. [redacted] and Mr. Berger would read over the documents on which he had questions. [redacted] ruled on responsiveness to the 9/11 Commission.

b6,
b7c

There were more questions to be answered in July 2003, as this was the first EOP request he was involved with. Some of the questions included what constitutes a document, does the 9/11 Commission want duplicate copies of the same information, do they want copies of the same document that contained additional notes, etc. There were two or three calls to [redacted] on these issues during Mr. Berger's review.

b6,
b7c

Mr. Berger started his own company, Stonebridge, in 2001. [redacted] had [redacted] phone number from setting up appointments for Mr. Berger's visits. He told his secretary not to call him at the Archives unless there was a time sensitive issue. His secretary probably called him at [redacted] number about a half dozen times on this visit. Mr. Berger told [redacted] he was happy to go outside [redacted] office to take the calls. [redacted] asked Mr. Berger if he needed privacy to which he said "yes." [redacted] said instead that [redacted] would go outside [redacted] office while he was on the phone, which [redacted] did. Once this pattern was established, he thought the offer for [redacted] to leave [redacted] office was "standing." [redacted]. Mr. Berger had no intent to order [redacted] out of [redacted] office. While Mr. Berger was on the phone, he was left alone in [redacted] office. He used the phone closest to the couch. It was a hard line and he wanted that privacy with his clients. Mr. Berger did not use his cell phone and never told [redacted] it was not working.

b6,
b7c

Mr. Berger could not recall specifically if [redacted] left [redacted] office when [redacted] made phone calls. The only other time [redacted] left [redacted] office during his reviews was maybe to step out to get more boxes or consult with [redacted] staff. He did not recall if any of [redacted] staff stepped in the office with him when [redacted] stepped for these moments. Mr. Berger did not take any breaks to leave the building during this visit.

b6,
b7c

[redacted]. At some point, Mr. Berger took notes. He realized he was not going to be able to reconstruct in detail all the documents he had reviewed, so he needed to take his notes with him, about ten to twenty pages.

b6,
b7c

Case Number: [redacted] b2 Case Title: Samuel R. Berger [redacted] b2

At the end of the day, Mr. Berger tri-folded his notes and put them in his suit pocket. He took the opportunity to do this when [redacted] was out of [redacted] office due to him being on a private phone call. Mr. Berger said he did not recall being hesitant to remove his suit jacket during this visit. However, at some point, him not removing his jacket could have been related to the fact he placed the notes in his jacket. Mr. Berger knew he had to leave some notes behind so it would not be obvious he removed notes. He had been making notes and if he did not leave any behind it would have been noticeable. [Mr. Berger was surprised to learn he left only two pages of notes at the Archives.]

b6
b7C

The notes he removed were torn from the top of the note pad. Mr. Berger did not have time to sort through and determine which pages he wanted to take and which to leave. He said this was the scenario on all three occasions when he removed notes from the Archives. He was aware he would not have a complete set but some notes were better than none.

b6, b7C

Mr. Berger did not recall asking [redacted] to have the documents arranged chronologically on his next visit. However, he might have mentioned they were not arranged chronologically.

The Millennium Alert After Action Review (MAAR) should have been with the documents Mr. Berger was reviewing on this visit, but he does not recall seeing it. The Principals meeting was in June 2000 and invariably before these meetings a memo reflecting what they were going to talk about would have been circulated. The Principals consisted of the [redacted]

b6
b7C

[redacted], and others.

Mr. Berger did not remove any documents on this visit.

[redacted] came to the Archives in July 2003, to review documents in response to EOP 2. Mr. Berger did not ask [redacted] to look for the MAAR or any other specific documents.

b6
b7C

On **September 2, 2003**, Mr. Berger came to the Archives to review documents in response to EOP 3. Again, the boxes of materials were on a cart in [redacted] office between Mr. Berger's seat and the coffee table, or off to his side. [redacted] was working with Mr. Berger in the review of the documents. [redacted] spent about the same amount of time with Mr. Berger as [redacted] had on his visit in July 2003. Mr. Berger could not estimate a percentage on the amount of time. His recollection was that the documents were Xerox copies.

b6
b7C

Again, [redacted] always stepped out of [redacted] office when Mr. Berger made or received phone calls. [redacted] may have also stepped out to consult with [redacted] staff, for a minute, but he has no recollection of whether [redacted] staff would step in when [redacted] was out.

b6
b7C

Mr. Berger was not told anything about the process of the documents after his review and their presentation to the 9/11 Commission. It never occurred to Mr. Berger that by removing the MAAR from the Archives, it would not be provided to the 9/11 Commission. It was his assumption the box of documents he was reviewing at the Archives, or a copy of them, was going from the Archives to the

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

White House. He did not assume that his removal of documents kept them from going forward to the 9/11 Commission. Mr. Berger knew he was not reviewing originals.

In late November and early December 1999, there were five to fifteen [terrorist] attacks. During this time, the Principals met every day for about an hour. They were operating more like a working group to get through the millennium. During this time, Ahmed Ressam was caught in Washington State with explosives to be used at the Los Angeles International Airport.

b6, b7C

After the millennium, Mr. Berger asked [redacted], to prepare the MAAR to determine where they were exposed and the vulnerabilities. There were fights over the jurisdiction of the funding. In March 2001, the Principals approved the recommendations and they were funded. After 9/11, the MAAR was widely discussed in the press. Mr. Berger commented the MAAR was not the most sensitive document he reviewed at the Archives.

Mr. Berger believed the MAAR was widely distributed among the FBI, the CIA, and the Department of State, for a total of about fifteen people. The MAAR was circulated three to four times to four or five people at each agency. All these agencies were subject to the EOP requests. [redacted] was going to testify concerning the MAAR.

b6, b7C

Mr. Berger read through the MAAR and took notes. There were twenty-nine topics for recommendations under four categories. He thought the 9/11 Commission would want to know what the Clinton Administration did to "fill in the holes." He was trying to move quickly through the document review. [redacted] had told him he still had three more days' worth of documents to review. Mr. Berger now says it was a foolish decision to take the MAAR and the notes out of the Archives.

b6, b7C

Mr. Berger believed this MAAR to be the final report. However, this would have been more likely if this version had a cover page/sheet. Mr. Berger did not return the MAAR to the pile that was returned to [redacted]. He did not have a recollection of putting other documents in this folder but he did have the intent to take the document. [There were two documents in what had been an empty folder after he removed the MAAR. [redacted] archivists did not move any documents into this folder.] He did not put any intentional markings on the documents. Mr. Berger did not recall receiving this folder separately from other folders. He did not recall seeing any other versions of the MAAR on this visit.

b6, b7C

During this visit, Mr. Berger received more calls as there were two op-ed articles out. One article stated Sudan offered Osama Bin Laden to the United States in 1996 but the Clinton Administration did not take the offer. Mr. Berger referred to this as an urban legend. The other article was by former Secretary of Defense Casper Weinberger who said the Clinton Administration was responsible for the attacks on September 11, 2001. These articles initiated a "flurry" of activities.

Mr. Berger took the first opportunity when [redacted] was out of [redacted] office to remove the document. He most likely put it in his jacket pocket, after folding it, but he does not have a precise recollection of where he put the document. It is perceivable he put it in his pants pocket. It was also possible he placed it in his portfolio and took it out. The document was twelve to thirteen pages. The notes were folded and put in his pocket. He would have put the notes on his person at the end of the day.

b6, b7C

Case Number: [redacted] b7	Case Title: Samuel R. Berger [redacted] b7
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

Mr. Berger did not believe [redacted] personnel were suspicious that he was removing documents. They did not give him any indications of this.

6
b6
b7c

Mr. Berger denied removing any documents in his socks. [He asked us to describe what the potential witness saw, which we did.] He stated his shoes frequently come untied [To which [redacted] said he was a witness.] and his socks frequently fall down. [At that point, Mr. Berger lifted his pant leg to reveal a sock falling down his ankle and pale skin.] Besides, it would have fallen out of his sock. He said this story was absurd and embarrassing.

b6
b7c

After leaving the Archives for the day, Mr. Berger went back to his office and put the document in an envelope on his desk.

On September 2, 2003, Mr. Berger called someone who was helping him review materials. He told them they should be prepared to answer the 9/11 Commission's questions concerning the MAAR.

It was asked that [redacted], former Clinton staffer, be cleared to review these documents. Mr. Berger had not worked on a document search in thirty years. If he was working at the NSC, this is certainly something someone on his staff would have done for him. [redacted] was able to [redacted] cleared for [redacted] material but the [redacted] clearance.

b2
b6
b7c

On **October 2, 2003**, Mr. Berger was reviewing documents at the Archives. The documents were in accordion files. [redacted] had the documents in a box, on the floor, by [redacted] desk. The time spent with him in reviewing the documents did not change. He did not recall NARA staff being more or less restrictive with the documents than on other visits.

b6
b7c

[redacted] first provided Mr. Berger the documents marked for review by [redacted]. A version of the MAAR was with these documents, marked [redacted]. Mr. Berger did not know why it was classified differently than the version he removed in September which was [redacted]. It was obvious to him this was a different version of the MAAR. Mr. Berger wanted to know how it was edited to now be classified as [redacted]. He needed to compare the two versions of the MAAR. [redacted] had mentioned the MAAR went through several iterations but the changes were over money not substantive. Mr. Berger placed this version under his portfolio while [redacted] assistant was in the office. He then returned the folder to [redacted] assistant. Mr. Berger has no recollection of post-it notes on this document or moving them to another document. The assistant was standing in the area by [redacted] desk where the files were.

b2
b6
b7c

Next, [redacted] provided him all but two documents the White House had sent back from the documents he reviewed for EOP 2. [The White House sent those two documents on to the 9/11 Commission.] [redacted]

b5
b1
b7c

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

Then they turned to the documents of the day. This time, the emails were organized. He recalled being handed the documents individually, not in a folder. About mid-day, Mr. Berger came across another version of the MAAR. In October, Mr. Berger saw a version of the MAAR and now had doubts that what he removed in September was the final report. At this point, he wanted to track the evolution of the MAAR. He slid the document under his portfolio.

██████████ told Mr. Berger there was a missing document, one that ██████████ could not find. Mr. Berger said at this point "the bomb should have burst in the air, but obviously it did not." However, Mr. Berger did apprehend the consequences of what ██████████ said. Mr. Berger disassembled first, then he asked ██████████ if the document could have been misfiled. ██████████ said "No." Mr. Berger asked if they had not produced this document already. ██████████ said it was a different version.

b6,
b7C

██████████ gave him another copy of the document. Mr. Berger slid this document under his portfolio also. ██████████ did not ask for it back. If ██████████ had asked for it back, it would have "triggered" a decision for him to give the documents back.

b6,
b7C

In total, he removed four documents, all versions of the MAAR. Mr. Berger does not recall if he placed all the documents on his person at once or at different times. He did not put the documents on his person until he was alone. He removed the notes, about fifteen pages, towards the end of the day.

Mr. Berger had a long day and wanted to go home around 6 p.m. ██████████ wanted him to finish the review and said they only had about an hours worth of work left. He understood ██████████ was getting pressure from the White House to provide a response so he agreed. ██████████ suggested he take a walk and come back and finish up. Mr. Berger left the building with all the documents he put in his pockets. He was aware of the risk he was taking, but he also knew ██████████

b2,
b6, b7C

Mr. Berger exited the Archives on to Pennsylvania Avenue, the north entrance. It was dark. He did not want to run the risk of bringing the documents back in the building risking the possibility ██████████ might notice something unusual. He headed towards a construction area on Ninth Street. Mr. Berger looked up and down the street, up into the windows of the Archives and the DOJ, and did not see anyone. He removed the documents from his pockets, folded the notes in a "V" shape and inserted the documents in the center. He walked inside the construction fence and slid the documents under a trailer.

b6,
b7C

Mr. Berger came back into the building without fearing the documents might slip out of his pockets or that ██████████ and ██████████ staff would notice that his pockets were bulging. ██████████

b2,
b6, b7C

If Mr. Berger had been aware ██████████ staff was tracking the documents he was provided, he would not have removed them. He also said that if staff had escorted him out of the building for his walk, he would have felt less confident that no one was in the area and someone might be watching his actions.

b6,
b7C

Case Number: ██████████ b2	Case Title: Samuel R. Berger ██████████ b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

8

Mr. Berger does not recall reviewing his notes or [REDACTED] notes on this visit. b6, b7C

It is possible that [REDACTED], stopped by to introduce [REDACTED] but Mr. Berger did not have a vivid memory of this. b6, b7C

Mr. Berger was trying to balance his review carefully but was also trying to be expeditious. He skipped meals and drank diet cokes. He did go to the restroom, possibly with documents in his pockets, but did not discard documents there or rearrange them on his person. b6, b7C

On this visit, [REDACTED].

[REDACTED] did not tell Mr. Berger that [REDACTED] had numbered the documents or that [REDACTED] had a way of tracking these records. Mr. Berger said he would have "picked-up" on that comment. He said "I may be stupid, but I am not self destructive." As he left for the day between 7 and 7:30 p.m., [REDACTED] asked Mr. Berger [REDACTED]. He totally missed that signal later realizing it was [REDACTED] subtle way to ask him if he removed documents. Mr. Berger believed no one knew he removed documents. b6, b7C

Mr. Berger left the building, retrieved the documents and notes from the construction area, and returned to his office. b6, b7C

On **October 4, 2003**, late in the afternoon, [REDACTED] called Mr. Berger to tell him [REDACTED] called from the Archives. Mr. Berger was aware [REDACTED] was the [REDACTED]. [REDACTED] said documents were missing after Mr. Berger's visit on October 2, 2003. Mr. Berger panicked because he realized he was caught. Mr. Berger lied to [REDACTED] telling [REDACTED] he did not take the documents. b6, b7C

Mr. Berger remembers next calling [REDACTED] at [REDACTED] office. He knew it was not a good sign [REDACTED] was there on a Saturday. [REDACTED] described the documents stating there were four copies of three documents missing. Mr. Berger asked [REDACTED] if the four documents they were missing were copies of the MAAR. He told [REDACTED] he would see if he accidentally took them. Mr. Berger was agitated because he realized he was caught. b6, b7C

[REDACTED] called Mr. Berger and said "I hope you can find them because if not, we have to refer this to the NSC's [REDACTED]." [REDACTED] did not say what would be done if Mr. Berger returned the documents. When asked again, Mr. Berger became unsure whether [REDACTED] said this to him. However, he was sure the source of the statement was [REDACTED] asked Mr. Berger to go to his office to see if he could find the documents. b5, b6, b7C

Mr. Berger drove to his office late that afternoon. On the night of October 2, 2003, he had destroyed, cut into small pieces, three of the four documents. These were put in the trash. By Saturday, the trash had been picked-up. He tried to find the trash collector but had no luck. Neither [REDACTED] nor [REDACTED] offered to help him look through the trash. b6, b7C

Case Number:

b2

Case Title:

Samuel R. Berger [REDACTED] b2

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

About 7 p.m., Mr. Berger called [REDACTED] and said "I think I solved the mystery." [REDACTED] said [REDACTED] was going into [REDACTED] and would call as soon as it was over. About 11:30 p.m., Mr. [REDACTED] called Mr. Berger. Mr. Berger told [REDACTED], "I found two documents but not the other two." [REDACTED] told him to get the documents from his office and lock them in the safe in his home. [REDACTED] was glad he found two but three were still missing. b6, b7C

Mr. Berger did not recall [REDACTED], unless [REDACTED] picked-up the documents. b6, b7C

On **October 5, 2003**, Mr. Berger recalled NARA staff picking up the two documents at his home. He understands that NARA staff recalled picking up the documents at his office. Mr. Berger was willing to accept that NARA staff came to his office.

There were additional conference calls. [REDACTED] was surprised when Mr. Berger returned the documents he removed in September. He knew he was caught, so he purported he must have removed the documents accidentally or inadvertently by sweeping them up with his documents. Later, Mr. Berger made a decision, on his own, to tell the truth. He said "I realized I was giving a benign explanation for what was not benign." Mr. Berger wanted to return everything he had taken. He realized he was returning documents he removed in September. He did not realize he returned more than they knew he removed. Mr. Berger was aware of the consequences but he knew returning the documents was the right thing to do. b6, b7C

Mr. Berger called [REDACTED] told [REDACTED] what happened, and asked what he should do. [REDACTED] told Mr. Berger to get a lawyer. Mr. Berger and [REDACTED] did not discuss this issue any further as they were [REDACTED] and knew it was better not to talk about this. b6, b7C

Mr. Berger specifically recalled returning his notes to NARA staff at his home. He had flown in from New York, spent about an hour at his home, then flew back to New York to continue his travel. NARA staff never mentioned his notes. Mr. Berger believed if he had not returned them, they would never have known he removed his notes.

Mr. Berger does not know [REDACTED], nor did he have any contact with [REDACTED]. Mr. Berger had not met [REDACTED] prior to these visits to the Archives. Additionally, he did not contact the NSC on this matter. b6, b7C

There were not any handwritten notes on the documents Mr. Berger removed from the Archives. Mr. Berger did not believe there was unique information in the three documents he destroyed. Mr. Berger never made any copies of these documents.

Mr. Berger said as a general point, he has dealt with classified information for twelve years. Some documents are sensitive and some are not super sensitive. This may not have anything to do with the documents classification. Other documents he reviewed had more sensitive information in them such as the Presidential Findings. He had seen most of the information in the MAAR disclosed in the press. He substituted his sense of sensitivity instead of thinking of classification. The MAAR did not involve sources and methods. It was a policy document.

Case Number:

[REDACTED]

b2

Case Title:

Samuel R. Berger [REDACTED]

b2

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

Some of the notes he removed did have information about the Presidential Findings. This was the authority from the President for actions to be taken.

██████████ had no reason to believe he was not acting in an appropriate manner. Mr. Berger said if there was always someone with him, he would not have taken any documents. After learning he was given special treatment by viewing the documents in ██████████ office, he suggested no exceptions to the rules should be given to former National Security Advisors or others. The Archives should thoroughly check people when they enter and exit the building. *b6, b7c*

Mr. Berger received enough phone calls which gave him the opportunity to remove the documents. He never sent ██████████ out of the room for the sole purpose of removing the documents. *b6, b7c*

The DOJ asked Mr. Berger if he removed any other documents from the Archives that we were not aware of to which Mr. Berger replied no.

Case Number: ██████████ <i>b2</i>	Case Title: Samuel R. Berger ██████████ <i>b2</i>
--------------------------------------	--



REPORT OF INVESTIGATION

Title (Name and address): Samuel R. Berger [redacted] b2		Type of Investigation: Criminal	Type of Report: <input checked="" type="checkbox"/> Final <input type="checkbox"/> Supplemental
Social Security Number: NA		<input type="checkbox"/> Employee	<input checked="" type="checkbox"/> Non-employee
<input type="checkbox"/> Former Employee	Date of Birth: NA	Date Entered on Duty: NA	Position and Grade: NA
Post of Duty: NA		Organization and Office: NA	
Period of Investigation: October 2003 to October 2005			

BASIS FOR INVESTIGATION

The Office of Investigations (OI), Office of Inspector General (OIG), received information that Samuel R. Berger, former National Security Advisor, removed classified documents from the National Archives and Records Administration (NARA), constituting a violation of criminal law. The investigation pertaining to Mr. Berger's actions was referred to the Department of Justice (DOJ) per the Inspector General (IG) Act (as amended) and 18 U.S.C. § 402a – Coordination of counterintelligence activities. The DOJ and Federal Bureau of Investigation (FBI), with the assistance of the OIG, conducted the criminal investigation involving Mr. Berger.

The NARA OI investigated and is reporting on the activities addressing NARA's responsibilities concerning Presidential records and Mr. Berger's access to those records.

ALLEGED VIOLATIONS

1. [redacted]
2. [redacted] **b6, b7c**
3. [redacted]

Distribution	No.	Case Number:	Signature of Special Agent Making Report:
Office of Inspector General	1	[redacted] b2	
National Archives and Records Administration	2	Signature of Person Examining Report:	
Assistant U.S. Attorney	1		
Other (Specify):		Title: Assistant Inspector General for Investigations	Office (City): College Park, MD
		Division Office: Headquarters	Date of Report: 11/4/05

OFFICIAL USE ONLY

Obtained via FOIA by Judicial Watch, Inc.

- 4. [REDACTED]
- 5. [REDACTED]
- 6. [REDACTED]

b6, b7C

RESULTS OF INVESTIGATION

The investigation substantiated that Mr. Berger unlawfully removed and retained classified documents from NARA. On September 8, 2005, Mr. Berger was sentenced to two years of probation, subsequent to pleading guilty to Unauthorized Removal and Retention of Classified Material, a misdemeanor. The court ordered a \$25.00 special assessment, a fine of \$50,000, 100 hours of community service, and no access to any classified material for 3 years.

This investigation substantiated that [REDACTED] b2, b5, b6, b7C
 facilitated access to [REDACTED] on at least five occasions.
 [REDACTED] documents were provided to Mr. Berger on four occasions. [REDACTED] documents were provided to [REDACTED], on one occasion.

[REDACTED] b2, b6, b7C
 [REDACTED]

On September 2, 2003, there was a suspicion Mr. Berger may have removed classified material from the Archives. Neither [REDACTED] b6, b7C
 [REDACTED] nor [REDACTED] reported this suspicion to any law enforcement entity. [REDACTED]

On October 3, 2003, [REDACTED] b6, b7C
 verified Mr. Berger removed classified material from NARA. Neither [REDACTED] nor [REDACTED] reported this incident to any law enforcement entity before conducting an investigation of the incident.

[REDACTED] b6, b7C
 conducted an investigation, including contacting the subject of the investigation, [REDACTED] b6, b7C
 [REDACTED]

Case Title: Samuel R. Berger [REDACTED] b2	Case Number: [REDACTED] b2
---	-------------------------------

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

[REDACTED] Archives employees contend Mr. Berger did not remove documents to disburse their contents and/or commit espionage. [REDACTED]

b2,
b5,
b6,
b7C

INVESTIGATIVE SUMMARY

EXHIBIT

The Presidential Records Act (PRA) of 1978 and Executive Order 13233 govern the official records of Presidents and Vice Presidents created or received after January 20, 1981. Upon the conclusion of a President's term of office, or if a President serves consecutive terms upon the conclusion of the last term, the Archivist of the United States shall assume responsibility for the custody, control, and preservation of, and access to, the Presidential records of that President. The Archivist shall deposit all such Presidential records in a Presidential archival depository or another archival facility operated by the United States.

The William J. Clinton Presidential material was transferred to the legal custody of NARA at the end of President Clinton's administration. The [REDACTED] at NARA is responsible for Presidential records. [REDACTED]

b6, b7C

[REDACTED]. The majority of the Clinton Presidential records were sent to the Clinton Project [now the William J. Clinton Presidential Library] in Little Rock, AR. [REDACTED]

b2, b5

[REDACTED]. These documents designated as the "W" intelligence files, contain classified information [REDACTED] material.

On April 12, 2002, President Clinton signed a letter designating Mr. Berger and [REDACTED] as agents on his behalf to review relevant NSC documents regarding Osama Bin Laden/Al Qaeda, Sudan, and Presidential correspondence from or to Omar Bashir, contained in the Clinton Presidential records. This request was made to facilitate Mr. Berger's testimony to the Joint Intelligence Committee (Graham-Goss Commission). This request was forwarded by [REDACTED], [REDACTED], [REDACTED], in a letter dated April 15, 2002.

b6, b7C

The NSC's [REDACTED] sent a letter to [REDACTED], dated May 14, 2002, designating the guidelines for access to these highly sensitive records. The letter stated Mr. Berger was the only person from the Clinton administration who had been designated and had all clearances required for access

b6, b7C

Case Title: Samuel R. Berger [REDACTED] b2	Case Number: [REDACTED] b2
---	-------------------------------

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

to the most sensitive "W" files. [redacted] said [redacted] repeatedly briefed Mr. Berger that he was not allowed to remove any documentation from NARA. The letter also stated notes may be taken but must be retained by NARA staff and forwarded to the NSC for a classification review and appropriate marking. [redacted] said the NSC told [redacted] Mr. Berger was made aware of this requirement.

b6, b7C

[redacted]

b2, b5

On May 30, 2002, Mr. Berger reviewed Clinton Presidential materials at Archives I (Washington, DC) for the purpose of preparing his testimony to the Graham-Goss Commission. Additionally, in response to requests from the National Commission on Terrorist Attacks Upon the United States (hereinafter the 9/11 Commission), Mr. Berger conducted a constitutional Presidential Privilege review of Clinton Presidential materials at Archives I on three occasions: July, September, and October 2003. On all of these visits, Mr. Berger reviewed documents including [redacted] material.

b2, b6, b7C

Under the PRA the Congressional committee agreed the incumbent President would request the records and turn them over to the 9/11 Commission. This was facilitated through Executive Office of the President (EOP) requests. According to [redacted], the established protocol was for NARA to conduct a review, at Archives I and at the Clinton Project, and determine which Clinton Presidential records were responsive to the EOP requests, with [redacted] making the final call on responsiveness for NARA. Clinton representatives reviewed the documents for privilege and discussed responsiveness with [redacted]. After the reviews, copies were sent to the NSC for the representative of the incumbent President to review before forwarding to the 9/11 Commission.

b2, b6, b7C

On all four visits to Archives I, Mr. Berger signed in as a visitor and was escorted to [redacted] office, room [redacted], where he conducted his review of documents including [redacted] material. Mr. Berger was allowed to bring personal items into the room including his portfolio and cell phone. [redacted]

b2, b6, b7C

[redacted]

pursuant to DCID 6/9: Physical Security

Case Title:
Samuel R. Berger [redacted]

b2

Case Number:

b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General

National Archives and Records Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

Standards for Sensitive Compartmented Information Facilities, Section 2.3.2.

[REDACTED]

b2, b6, b7C

Some NARA employees believed room [REDACTED] was "cleared" as it contained [REDACTED]

[REDACTED] acknowledged [REDACTED] received a [REDACTED] classified document from Little Rock, AR, [REDACTED], in response to an EOP request.

b2, b5, b6, b7C

[REDACTED]. According to NARA documentation, [REDACTED] since about 1993. During this investigation, this [REDACTED].

The Director of the CIA is the overall authority [REDACTED]. [REDACTED] material is governed by the DCIDs. According to CIA officials, NARA can make agency specific regulations requiring additional security measures as long as they exceed the requirements of the DCIDs. [REDACTED]

b2, b6, b7C

[REDACTED] CIA Office of Security, advised that the CIA Director delegates their authority to the Senior Official of the Intelligence Community (SOIC). While some agencies have a designated SOIC, NARA does not. Therefore, NARA falls under the Director of Security, CIA, SOIC. Waivers to DCIDs have to be signed by the SOIC.

On May 30, 2002, Mr. Berger was provided original NSC numbered documents and original Staff Member Office Files (SMOFs). [REDACTED] indicated Mr. Berger did not have many questions for [REDACTED] as this review was in preparation for his testimony. [REDACTED] said Mr. Berger left his notes at NARA, and requested these notes be sent to the NSC for classification review.

b2, b6, b7C

On July 18, 2003, Mr. Berger was provided original NSC numbered documents and original SMOFs. [REDACTED] and Mr. Berger were sitting at the table in [REDACTED] office going over the documents during most of this visit. They were discussing responsiveness to the EOP2 request. Mr. Berger said he took several phone calls on this visit where [REDACTED] stepped out of [REDACTED] office.

b2, b6, b7C

Mr. Berger said he realized he was not going to be able to reconstruct in detail all the documents he had reviewed, so he needed to take his notes with him, about ten to

b2, b6, b7C

Case Title: Samuel R. Berger [REDACTED] b2

Case Number: [REDACTED] b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General National Archives and Records Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

twenty pages. Mr. Berger said at the end of the day, he folded his notes and put them in his suit pocket. Mr. Berger said he took the opportunity to do this when [redacted] was out of [redacted] office.

b6, b7C

[redacted] came to Archives I in July 2003 to assist Mr. Berger by reviewing Presidential records sent to Archives I from the Clinton Project in response to EOP2. [redacted] visit was separate from Mr. Berger's visit in July. [redacted] verified [redacted] reviewed documents classified to the [redacted] in [redacted] office.

b2, b6, b7C

[redacted] said Mr. Berger's handling of the documents on July 18, 2003, caused archival concerns in maintaining provenance. [redacted] said [redacted] and Mr. Berger [redacted] and Mr. Berger would pull out other documents. [redacted]

b2, b6, b7C

[redacted], therefore the documents became disorganized. [redacted] said Mr. Berger requested that on his next visit he preferred to see the documents in chronological order. [redacted] suggested to the [redacted] that on Mr. Berger's next visit they provide him with copies to allow for placement of the documents in chronological order.

On September 2, 2003, Mr. Berger was provided original NSC numbered documents and copies of SMOFs for review in response to EOP3. [redacted] said Mr. Berger was also provided a document faxed from the Clinton Project to Archives I on July 22, 2003.

b2, b6, b7C

[redacted] said [redacted] did not spend as much direct time with Mr. Berger as [redacted] had on the previous visit. According to [redacted], during this visit, Mr. Berger asked [redacted] to leave [redacted] office several times so he could talk privately on the phone. [redacted] said [redacted] left as [redacted] trusted Mr. Berger and was aware that Mr. Berger, as National Security Advisor, had generated most of the documents [redacted] was reviewing. However, [redacted] said [redacted] did not like leaving [redacted] office because [redacted] works with sensitive items [redacted] and did not feel comfortable leaving Mr. Berger alone with this material. [redacted] said [redacted] knew of no statutory authority that allowed [redacted] to refuse to leave the room.

b2, b5, b6, b7C

Mr. Berger said he would say: "Sorry, I have to make a private phone call," and [redacted] would take this as [redacted] cue to leave. Mr. Berger said he told [redacted] he was happy to go outside [redacted] office to take the calls. Mr. Berger said instead [redacted] offered to leave [redacted] office while he was on the phone. Mr. Berger said once this pattern was established, he thought the offer for [redacted] to leave [redacted] office was "standing." [redacted] denied there was any such agreement.

b2, b6, b7C

Case Title:
Samuel R. Berger [redacted]

b2

Case Number:

b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General

National Archives and Records Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

asked staff member to buy a soda for Mr. Berger. said Mr. Berger stepped out of office, out of the suite, and into the hallway headed for the men's room. said came out of the suite and had to "side step" Mr. Berger. said saw Mr. Berger bent down, fiddling with something white, which could have been paper, around his ankle. said continued to the basement to buy the soda. said attempted to call but could not recall extension. said returned to the suite and asked to step out. said briefly explained to what had witnessed. According to asked to write the information down. said sent an email to before Mr. Berger left for the day.

b2, b6, b7C

said read the email. According to, when Mr. Berger stepped out to the men's room, discussed with if was sure enough of what saw to confront Mr. Berger. said that did not believe there was enough information to confront someone of Mr. Berger's stature. said did not mention the email to or discuss this matter until after Mr. Berger left.

b2, b5, b6, b7C

Mr. Berger said he took the first opportunity when was out of office to remove a document (a facsimile sent from in July). He said he folded the notes and put them in his pocket at the end of the day. Mr. Berger denied removing any documents in his socks. He stated his shoes frequently come untied and his socks frequently fall down.

b2, b6, b7C

On either September 2, 2003, or September 3, 2003, contacted and advised of what occurred. According to said "we have a problem." said said was worried Mr. Berger might be taking documents out of Archives I and that and staff were going to watch Mr. Berger closely on his next visit. When asked, said did not make these statements to

b2, b6, b7C

stated mentioned the incident to supervisor, neither nor provided further guidance to said does not recall having a conversation with about this incident in preparation for Mr. Berger's visit on October 2, 2003. However, stated approved a more aggressive action to be taken by and the when Mr. Berger returned but did not give specific direction.

b2, b6, b7C

Case Title: Samuel R. Berger b2

Case Number: b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General National Archives and Records Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

On September 4, 5, and 8, 2003, [redacted], formerly of President Clinton's National Security staff, reviewed classified documents responsive to EOP3 [redacted]. [redacted] said [redacted] inquired as to why [redacted] was not allowed to conduct the review in [redacted] office. [redacted] said [redacted] advised [redacted] [redacted] had other matters to attend to and that [redacted] staff would assist him.

b2, b6, b7C

Next, [redacted] prepared for Mr. Berger's return. According to [redacted], the incident on September 2, 2003, in which [redacted] thought [redacted] witnessed Mr. Berger with something in his sock was in [redacted] thoughts as [redacted] prepared for Mr. Berger's next visit. [redacted] said they decided to hand number the documents provided to Mr. Berger on the back of each document as a means of controlling the documents. [redacted] said they numbered documents to feel secure that Mr. Berger was not removing documents. [redacted] said they numbered these documents themselves, without consultation with NARA General Counsel, Security, management, the OIG, or law enforcement. However, [redacted] said [redacted] told [redacted] of their intention to number the documents (by September 28th at the latest). [redacted] said [redacted] thought it was a good idea.

b2, b6, b7C

Mr. Berger next came to Archives I on October 2, 2003. He reviewed copies of NSC numbered documents, copies of SMOFs, and hard copies of emails, including those which [redacted] had reviewed, in response to EOP3. [redacted] said [redacted] told Mr. Berger [redacted] was not leaving [redacted] office for him to take private calls. [redacted] said [redacted] was working at [redacted] desk while Mr. Berger reviewed the documents. [redacted] also recounted that Mr. Berger made numerous visits to the men's room.

b2, b6, b7C

[redacted] said on this visit Mr. Berger was provided one file folder of documents at a time. Once Mr. Berger finished reviewing a file folder, [redacted] said they reviewed the hand numbering to ensure all the documents were returned. [redacted] said in the afternoon [redacted] was returning a file folder to a [redacted] member during one of Mr. Berger's many visit's to the men's room. The [redacted] member said they discovered a numbered document (#217) was missing from a file folder Mr. Berger had reviewed. [redacted] said they printed another copy of the document which was missing. [redacted] said [redacted] gave this second copy (#217) to Mr. Berger. [redacted] said [redacted] told Mr. Berger [redacted] had a way of "legally controlling" the emails. [redacted] said [redacted] emphasized to Mr. Berger that the document was numbered and apparently when he was provided the emails he had not been provided this one. [redacted] said Mr. Berger indicated he was sure he had seen this email and asked [redacted] if [redacted] remembered seeing this email. [redacted] said [redacted] told Mr. Berger [redacted] had seen similar information but that this unique email number was missing.

b2, b6, b7C

Mr. Berger said he saw a version of the Millennium Alert After Action Review

Case Title: Samuel R. Berger [redacted] b2 Case Number: [redacted] b2

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

(MAAAR) and now had doubts that what he removed from Archives I in September was the final report. He said at this point, he wanted to track the evolution of the MAAAR. Mr. Berger said he slid the document (#217) under his portfolio.

b2, b6, b7C

Mr. Berger said that when [redacted] told him there was a missing document "the bomb should have burst in the air, but obviously it did not." Mr. Berger said when [redacted] gave him another copy of the document (#217), he slid this document under his portfolio also. Mr. Berger said [redacted] did not ask for it back. Mr. Berger said if [redacted] had asked for the document back, it would have "triggered" a decision for him to give the documents back.

b2, b6, b7C

According to [redacted], about five minutes later, Mr. Berger told [redacted] he had to make a private phone call and [redacted] had to leave [redacted] office. [redacted] said [redacted] was uncomfortable with this request but left [redacted] office. [redacted] said [redacted] stepped over to the desk outside [redacted] office that had a phone on it with [redacted] line accessible. [redacted] said [redacted] noticed [redacted] phone line was not lit. According to [redacted], [redacted] opened [redacted] office door at which point Mr. Berger "mowed" [redacted] down on the way to the men's room, a location from which he had recently returned.

b2, b6, b7C

Later that evening, Mr. Berger took a break to go outside. No one escorted him out of Archives I. In total, during this visit he removed four documents, all versions of the MAAAR. Mr. Berger said he left the building with all four documents (#150, #323, and two copies of #217) in his pockets. [redacted] Mr. Berger said if [redacted] had escorted him out of the building, he would have felt less confident that no one was in the area and more concerned someone might be watching his actions.

b2, b6, b7C

Mr. Berger said he did not want to take the risk of bringing the documents back in the building and the possibility [redacted] might notice something unusual. Mr. Berger said he placed the documents under a trailer in an accessible construction area outside Archives I. He returned to [redacted] office to finish his review. He said he removed the notes, about fifteen pages, near the end of the day. Mr. Berger said he then left Archives I, retrieved the documents from the construction area, and returned to his office.

b2, b6, b7C

[redacted] was working on other projects, therefore, all the documents were not checked before Mr. Berger left. Also, the folders were only given to staff when Mr. Berger went to the men's room. After Mr. Berger left, [redacted] said [redacted] and [redacted] returned the documents [redacted]. [redacted] said the folders were not checked at this time to determine if any additional hand numbered documents were missing as it was late, other staff had already left for the day, and they had no reason

b2, b6, b7C

Case Title: Samuel R. Berger [redacted] b2

Case Number: [redacted] b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General National Archives and Records Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

to believe Mr. Berger removed documents. At that time, [redacted] said they believed the email (#217) might not have been provided to Mr. Berger initially.

The first thing the next morning, Friday, October 3, 2003, the [redacted] said they began verifying that all documents provided to Mr. Berger on October 2, 2003, were present. [redacted] stated four numbered, classified, emails were missing from those provided to Mr. Berger on October 2, 2003. According to [redacted], all the missing documents had the MAAAR as an attachment.

b2, b6, b7C

[redacted]

b2, b6, b7C

Upon discovery that classified documents were missing, [redacted] contacted [redacted], as [redacted] supervisor, [redacted], was on travel. [redacted] had also been working with the [redacted] on the production of the EOP requests [redacted] traveled to Archives I where [redacted] and [redacted] discussed what action should be taken. [redacted] said [redacted] stated the normal reporting process would be notification of the NSC as the equity holder and [redacted] may have raised the issue of who in the agency should be notified, mentioning the Archivist of the United States, NARA security, and the Inspector General. [redacted] said [redacted] called [redacted], to report the matter and seek guidance on how to proceed but [redacted] was on travel. [redacted] said [redacted] asked [redacted] if [redacted] contacted [redacted] boss, [redacted]. [redacted] said [redacted] told [redacted] had tried but [redacted] was not available.

b2, b6, b7C

The next day, Saturday, October 4, 2003, [redacted] said [redacted] talked with [redacted] who asked that [redacted] and [redacted] come up with a plan to handle this matter and report back to [redacted]. [redacted] said [redacted] received a call from [redacted] asking [redacted] to contact [redacted]. [redacted] said they were treating this incident as an unauthorized removal of classified documents, a breach of National Security Information. According to [redacted], it was [redacted] job to handle security violations. [redacted] said [redacted] was acting at [redacted] direction and if [redacted] had asked [redacted] to work with the OIG [redacted] would have. [redacted] stated NARA personnel conducted an inquiry per the NARA ISM.

b2, b6, b7C

[redacted] stated [redacted] led the investigation [redacted] expanded that [redacted]

b2, b6, b7C

Case Title: Samuel R. Berger [redacted]

b2

Case Number: [redacted]

b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General National Archives and Records Administration

OFFICIAL USE ONLY

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

was on leadership team, had expertise in Archives' matters, and was the Mr. Berger removed only copies of documents. said this did not effect belief this was a serious matter.

b6, b7C

said told asked to head up this investigation. It was clear to and that was not in charge.

b2, b6, b7C

considered to be in charge of the incident even though was a and was believed was only in charge until was briefed. said that, and all provided input on how to proceed.

b2, b6, b7C

said stated was stepping away from the decision making in this matter. said kept the lead and decisions on this matter separate from because was a said made this clear to and; and they indicated they agreed with decision. believed this was clear to because never said had to run their ideas by said, in view, was leading the inquiry

b2, b6, b7C

said considered this incident to be a potential crime and the unauthorized removal of classified documents should be reported to the FBI. said believed the FBI might want to look into this matter due to the level of classified materials involved. said either or suggested the FBI be contacted. However, said never contacted the FBI and could not explain why the FBI was never contacted. said recalled mentioning something about the FBI. said did not recall anyone mentioning contacting the FBI.

b2, b6, b7C

That afternoon, and met at Archives I. said advised them the normal procedures were to recover the documents as quickly as possible and to report the incident to the equity holder. and decided to contact Mr. Berger and ask to return the documents. said they ran the idea of calling Mr. Berger by and authorized the contact. said indicated just wanted to do what was right and deferred to said while was not in charge, wanted to be informed on how this matter was proceeding.

b2, b6, b7C

said

Case Title: Samuel R. Berger

b2

Case Number:

b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General

National Archives and Records Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

they decided to contact [redacted] as Mr. Berger would be more responsive to [redacted]. [redacted] said [redacted], and [redacted] called [redacted], on speaker phone, and told [redacted] copies of emails were missing from the material Mr. Berger reviewed. They asked [redacted] to call Mr. Berger. [redacted] said at some point during the day, they explained how they had numbered the documents and now they were missing. [redacted] said they told [redacted] if Mr. Berger took the documents by mistake then gave them back it would be reported as an inadvertent removal. [redacted] said it was clear to [redacted] NARA intended on reporting this incident regardless.

b2, b6, b7C

[redacted] said [redacted] called Mr. Berger who told [redacted] that he did not think he had any documents. [redacted] said [redacted] called [redacted] (others were possibly on the line) and told [redacted] Mr. Berger's response. [redacted] said [redacted] was instructed to ask Mr. Berger a specific question. [redacted] said [redacted] suggested they contact Mr. Berger directly as asking a question through [redacted] was not efficient.

b2, b6, b7C

[redacted] said [redacted] called Mr. Berger and advised him NARA was treating this matter as a security infraction and [redacted] was going to report this to the NSC. According to [redacted], Mr. Berger said they were mistaken and that he gave the documents back to [redacted] assistant. [redacted] said they asked Mr. Berger to see if he could find any documents.

b2, b6, b7C

That evening, after [redacted] left Archives I, [redacted] said [redacted] took a call from Mr. Berger. According to [redacted], Mr. Berger asked if one of the misplaced emails was the one [redacted] had mentioned was missing and had given to him individually; and if the document that was missing contained information that was in several emails. [redacted] confirmed all the emails that were missing contained similar information.

b2, b6, b7C

[redacted] said around 8:00 p.m., Mr. Berger called [redacted] cell phone and asked if [redacted] could talk, as he wanted to explain something. [redacted] said [redacted] was at [redacted] and could not speak then but agreed to call him later that night.

b2, b6, b7C

Near midnight, [redacted] called Mr. Berger who said he found two documents. [redacted] advised Mr. Berger NARA would make arrangements to pick the documents up in the morning.

b2, b6, b7C

On Sunday, October 5, 2003, [redacted] said [redacted] informed [redacted] of the developments and [redacted] recommended [redacted] ask Mr. Berger to search his office again. [redacted] said [redacted] called Mr. Berger and asked him to search his office. [redacted] said Mr. Berger called back to say he was unable to locate any additional documents and it was possible that documents could have been disposed of in his

b2, b6, b7C

Case Title: Samuel R. Berger [redacted] b2 Case Number: [redacted] b2

OFFICIAL USE ONLY

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

office trash. [redacted] said [redacted] recommended to Mr. Berger he search his trash.

Later that morning, [redacted] and [redacted] picked-up documents from Mr. Berger. [redacted] said one document was an email which they had numbered by hand (#323) and the other was a facsimile of a textual document sent [redacted]. [redacted] identified the document from [redacted] as one Mr. Berger would have reviewed on September 2, 2003, not October 2, 2003, as thought. [redacted] said this was another copy of the MAAAR. [redacted] said they realized the implications that Mr. Berger took copies of documents on two separate visits (September 2, 2003 and October 2, 2003) and that the missing items all included the MAAAR.

b2, b6, b7C

[redacted] said that afternoon [redacted] and [redacted] called [redacted] and told [redacted] what Mr. Berger had provided and the significance of the dates Mr. Berger reviewed the documents. [redacted] said [redacted] told [redacted] had to talk to Mr. Berger. [redacted] said [redacted] and [redacted] spoke with Mr. Berger to explain that one of the documents he returned was from his visit on September 2, 2003, and that documents removed on October 2, 2003, were still missing.

b2, b6, b7C

According to [redacted], later that day, [redacted] called and told [redacted] Mr. Berger called [redacted] and said he [Mr. Berger] may have been incorrect and took the textual document on September 2, 2003.

b2, b6, b7C

[redacted] said that evening, after talking with [redacted] and [redacted], a decision was made to contact the NSC. [redacted] said later that evening [redacted] spoke with the NSC's [redacted]. [redacted] gave him a short briefing and they set up a meeting for Monday, October 6, 2003. [redacted] said [redacted] also called [redacted], and gave [redacted] a short briefing and asked [redacted] to inform [redacted].

b2, b5, b6, b7C

According to [redacted], on October 6, 2003, the NSC's [redacted] met with [redacted] and [redacted] and advised [redacted] should formally report this to [redacted]. [redacted] said on October 6, 2003, [redacted] briefed [redacted]. [redacted] said that on October 6, 2003, [redacted] removed [redacted] by delegating [redacted], to handle this matter.

b2, b6, b7C

[redacted] said [redacted] recounted what [redacted] knew of the matter and stressed that [redacted] wanted [redacted] to manage the situation so that [redacted] was not directly involved. [redacted] said [redacted] asked [redacted] to review NARA policies to ensure this did not happen again. [redacted] said [redacted] was now in charge of an issue [redacted] saw as two fold. One issue being the change in procedures that was required concerning

b2, b6, b7C

Case Title: Samuel R. Berger [redacted] b2

Case Number: [redacted] b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General National Archives and Records Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

the prevention of such an incident in the future. The other issue was the leak of national security information.

[redacted] stated [redacted] believed it was NARA's responsibility to recover the documents and report to the NSC. [redacted] said on October 7, 2003, [redacted] and [redacted] met with NSC officials. [redacted] said [redacted] assumed once they reported this to the NSC that the NSC would take over the investigation.

b2, b5, b6, b7c

[redacted]

[redacted] and [redacted] said the NSC wanted to ensure all documents responsive to EOP3 were provided to the White House so the NSC could then assure the 9/11 Commission that all documents were provided. [redacted] said NARA had to be sure that no responsive records were removed by Mr. Berger and therefore not provided to the NSC.

[redacted] said the [redacted] reconstructed computer searches for the NSC numbered documents and SMOF files; and were confident to the best of their ability that all documents deemed responsive to EOP3 were provided to the White House. [redacted] said [redacted] informed the White House that NARA was not able to reconstruct the responsive documents for EOP2, as Mr. Berger was provided original documents. [redacted] said [redacted] would never know what if any original documents were missing from Mr. Berger's visits on May 30, 2002, and July 18, 2003.

b2, b6, b7c

The OI, with assistance from [redacted], reviewed the documents Mr. Berger reviewed in an attempt to identify if it could be determined if additional documents were missing. It was not apparent that Mr. Berger removed an entire NSC numbered package or a SMOF file folder, however, the contents of these documents could not be verified. Due to complications, the emails Mr. Berger reviewed could not be readily reconstructed.

b2, b6, b7c

[redacted] said on October 8, 2003, [redacted] reported to [redacted] what had transpired at the meeting with the NSC. [redacted] stated the [redacted] [redacted] said [redacted] then conducted a careful review of the statutes. [redacted] said [redacted] wanted to consult with other senior NARA officials to get their sense of the matter as they have knowledge, wisdom, and input on what to do in these matters. [redacted] said a meeting of these officials could not be facilitated until October 10, 2003.

b2, b5, b6, b7c

Case Title: Samuel R. Berger [redacted] b2	Case Number: [redacted] b2
---	-------------------------------

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General
National Archives and Records Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

██████████ said on October 10, 2003, ██████████ met with ██████████, ██████████, and ██████████, ██████████ said ██████████ shared potentially applicable statutes and executive orders at this meeting. ██████████ said at this meeting they concurred this could be a criminal matter and decided to report this to the OIG instead of going directly to the DOJ.

b2, b6, b7C

The Inspector General (IG) was briefed on this matter on Friday, October 10, 2003. This same date, OI investigators along with ██████████, retrieved documents from Mr. Berger, at his residence, at the request of Mr. Berger's attorney. ██████████ said the documents appeared to be Mr. Berger's hand written notes. These documents were secured ██████████.

b2, b6, b7C

██████████ was on travel over the holiday weekend. On Tuesday, October 14, 2003, the OI gathered information. On this date, an attorney representing ██████████ contacted NARA stating ██████████ had documents to turn over to NARA. These documents, notes taken concerning documents reviewed, were received by the OI and ██████████ and secured ██████████.

b2, b6, b7C

On October 15 and 16, 2003, the IG briefed DOJ attorneys and the FBI on this matter. The DOJ accepted the criminal referral concerning Mr. Berger's actions. The FBI requested the OI stop all interviews of cleared ██████████ and any NARA employees with knowledge of the incident involving Mr. Berger. The OI obliged and at their request assisted the FBI in collecting evidence for the criminal investigation.

b6, b7C

On April 9, 2004, NARA's IG and the DOJ's IG met with the Assistant Attorney General, Criminal Division, and the DOJ attorneys to discuss reporting this matter to the 9/11 Commission. A decision was made that the DOJ would notify the 9/11 Commission.

On April 14, 2004, DOJ officials advised the OI they could conduct an investigation of NARA procedures as they related to Mr. Berger's visits, with requested limitations.

On April 1, 2005, Mr. Berger pled guilty to Unauthorized Removal and Retention of Classified Material. On September 8, 2005, Mr. Berger was sentenced to two years of probation, subsequent to pleading guilty. The Court ordered a \$25.00 special assessment, a fine of \$50,000, 100 hours of community service, and no access to any classified material for 3 years.

Case Title:
Samuel R. Berger ██████████

b2

Case Number:

b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General
National Archives and Records Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

Exhibit Number	Description
1	Interviews of [REDACTED] b6, b7C
2	Memo to clarify discrepancies in the preparation for review of documents
3	Interview of [REDACTED] b2
4	Director of Central Intelligence Directive 6/9
5	Interview of [REDACTED] b6, b7C
6	[REDACTED] b2
7	Interview of Samuel Berger, dated July 8, 2005
8	Interview of [REDACTED] b6, b7C
9	[REDACTED], dated September 2, 2003 b6, b7C
10	Interview of [REDACTED] b6, b7C
11	Interview of [REDACTED] b6, b7C
12	Interview of [REDACTED] b6, b7C
13	Interview of [REDACTED] b6, b7C
14	[REDACTED] b2
15	Interview of [REDACTED] b6, b7C
16	Interview of [REDACTED] b6, b7C
17	Memorandum of Verification, dated June 2005

Case Number: [REDACTED] b2	Case Title: Samuel R. Berger [REDACTED] b2
-------------------------------	---

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

EXHIBIT #1

NOTE TO FOIA REQUESTERS

Exhibit #1 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(1)

MEMORANDUM OF INTERVIEW OR ACTIVITY

Type of Activity: <input checked="" type="checkbox"/> Personal Interview <input type="checkbox"/> Telephone Interview <input type="checkbox"/> Records Review <input type="checkbox"/> Other	Date and Time: May 31 – June 2, 2005
[REDACTED] <i>b6, b7C</i> [REDACTED] [REDACTED] - to clarify discrepancies in the preparation for review of documents by Sandy Berger	Conducted by: [REDACTED] <i>b6, b7C</i> Location of Interview/Activity: Archives I, Washington, DC

Subject Matter/Remarks

[REDACTED] were interviewed together to get a complete understanding of how the documents were identified, pulled and prepared for review by Samuel R. Berger. This information was gathered after final interviews of [REDACTED]. Therefore, this information is deemed more accurate. The following information was deemed unclassified by the National Security Council. *b6, b7C*

The Clinton Presidential "W" files consisted of [REDACTED] federal record center boxes (another one was added sometime after October 2, 2003.) The materials in these boxes were either National Security Council (NSC) numbered documents or Staff Member Office Files (SMOFs), which were segregated. A box usually belonged to one person or a directorate. [REDACTED] *b2, b6, b7C*

[REDACTED] These were the only files contained in the boxes with the exception of "overflow" files that came over from the administration as they were cleaning areas after the change of administrations. These files would be filled in folders but did not belong to an individual. [REDACTED]

The requested materials for all of Mr. Berger's reviews were narrowed by date, nothing prior to 1998, and subject matter, the Middle East. The best [REDACTED] could estimate, since [REDACTED] was not involved in the May 2002 search for materials, was that about [REDACTED] boxes from the universe of "W" files were searched. Of those, about one third were NSC numbered documents and the other two thirds were SMOFs. *b2, b6, b7C*

Mr. Berger was provided [REDACTED] material on all his visits to NARA. *b2*

Case Number: [REDACTED] <i>b2</i>	Case Title: Samuel R. Berger [REDACTED] <i>b2</i>
--------------------------------------	--

ENCLOSURE(2)

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

The [redacted] is an electronic system used during the Clinton administration by the NSC to manage their records. The [redacted] was used as a finding aid as it indexed NSC numbered documents. The White House transferred data from the [redacted] system to NARA, via a flat file. NARA put this data on a Window based system.

b2

Basic information, an overview or brief synopsis of the document, was entered into [redacted] and assigned a seven-digit number. A search engine was used and a key word search was performed on the system in response to EOP 2. A list of search terms was not provided to [redacted] was allowed to and ran searches and received hits in preparation for this visit. [redacted] printed the abstract and provided this information to [redacted]. The numbered documents had a cover sheet with the document number; however, one document may contain several pages. [redacted] searched [redacted] index for documents responsive to EOP 2. The NSC numbered documents were located at [redacted]. The system does not identify which documents are at which location. [redacted] system only allows the index sheet to be marked as [redacted]. All the NSC numbered documents may not be available. Some may have been destroyed while others might be misfiled. Twenty to thirty percent of the time, NSC numbered documents were not found where they were supposed to be.

b2, b6, b7C

[redacted] dealt mostly with NSC numbered documents. NSC numbered documents may have been printed on heavy paper stock, [redacted]. Copies of NSC numbered documents could be recognized as all were copied on 8" by 11" paper and were in black and white.

b2, b6, b7C

The NSC numbered documents have a cover sheet. Normally the first page is printed on bond paper. The classification is usually stamped in red ink. [redacted]

b2

Because these documents were numbered, someone could determine if a numbered document was missing. However, there could be several pages of one NSC numbered document and the pages may or may not have been individually numbered in consecutive order. Emails could also be included in the document. The NSC referred to one NSC numbered document as a package. Finalized NSC packages reflected a watermark.

b6, b7C

The NSC numbered documents were numbered on their face, but individual pages were not numbered. All NSC numbered documents have a cover sheet and are bound in some manner, either by staple, binder clip or appropriate means. [redacted] staff removed the staples or binding and made photocopies for the production to the White House. Any loose paper pieces would probably be gone. They were not bound together upon return to the box.

Staff Member Office Files (SMOFs) contained the papers an individual filed in a particular folder. This could include draft NSC numbered documents, memos, emails, notes, etc. Some of these documents were copies of the originals. Archivists consider everything in a SMOF folder to be an original as it was sent for preservation. It is not a copy until an archivist makes a copy.

The NSC also sent over electronic files to include an electronic email system that included unclassified [redacted] emails. These are not designated as the "W" files. [redacted]

b2

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

[REDACTED] was the primary reviewer of the emails. NARA had received an email system at the end of the Clinton administration. This system, known as [REDACTED] contained emails the NSC designated as "records." [REDACTED]

[REDACTED] printed and prepared the emails responsive to EOP 3. EOP3 had two paragraphs explaining what emails the 9/11 commission was requesting. They were emails from Mr. Berger to the Transnational Threats Staff ([REDACTED]) and the converse. They determined Mr. Berger and [REDACTED] did not always directly handle their email so they queried about eight people on their staff. [REDACTED] recalled the search was done by name and subject fields. NARA consulted with the White House on the search string(s) (words) they were using to query the current administrations emails and tried to use the same ones.

Once [REDACTED] received "hits," [REDACTED] reviewed the emails to determine if they were relevant to the request. [REDACTED] gave an example that an email might come up on the search having to do with Spain which would not have been responsive, so [REDACTED] would not have printed that email even though it came up in the initial search (terrorism). Once [REDACTED] believed the email was relevant, [REDACTED] printed a copy and wrote the file name [a number] on the back of each relevant email, in pen. The emails were grouped by classification then chronologically. This was done so the email could be segregated which would allow other reviewers with different security clearances to review the appropriate classified documents (i.e. [REDACTED]).

The documents for Mr. Berger's review were moved [REDACTED] to [REDACTED] office in Federal Records Center boxes. They were transported on a cart normally by two cleared individuals. This was done primarily to facilitate the cart being moved through the facility and over door jams. The boxes either had no descriptive words on them or if they did, the wording was covered with a clean sheet of paper. [REDACTED] believed if they covered the material in a closed box this was sufficient for transport in a government facility. [REDACTED] commented that classified information could be moved from one secure container to another secure container.

Mr. Berger's review in May 2002

The materials pulled for Mr. Berger's visit in May 2002 were kept segregated in case he wanted to return and review the documents again. These original materials filled five federal record center boxes. One box contained NSC numbered documents. Four boxes contained SMOF files. Of these four boxes; one was box W-049 which was brought forward for the entire review. These boxes became know as an artificial collection or the "Berger Request."

Box W-049 was [REDACTED] SMOF files. In that box were several NSC numbered documents. When they could not locate a NSC numbered document, they would go to box W-049.

[REDACTED] staff was more sensitive as this was the first access of Clinton Presidential records.

Case Number: [REDACTED] b2	Case Title: Samuel R. Berger [REDACTED] b2
-------------------------------	---

██████████ explained that at this time the ██████████ was not running. Because the ██████████ was not running, a keyword search of the ██████████ database was conducted by ██████████, from the incumbent President's database, and a hard copy list of results, in the form of NSC numbered document numbers was provided to ██████████ staff. ██████████

██████████ contained in the correspondence requesting Mr. Berger's access to the records. ██████████

██████████ could not find some of the NSC numbered documents so ██████████ faxed a list back to the NSC of the ones ██████████ could not locate. They told ██████████ they could be in other files.

██████████ said there was never an index of the SMOFs reviewed. ██████████ said ██████████ would not know if he removed originals during this visit.

██████████ explained there was no automated search for SMOFs. Each box of SMOF material contained a folder file or inventory list. These lists were copied and collated and provided by the NSC. ██████████ had to review the index of file folder lists in order to determine which folders might be responsive. SMOFs were searched by the file folder title using the keywords provided in the correspondence. This was a search where an archivist used their experience and intellect to decide what was responsive to the request. If documents in the SMOF were deemed non-responsive, by ██████████, they were put in an envelope in the back of the SMOF folder.

An "out card" was left in each box to mark the place where an NSC numbered document or SMOF was removed and indicated it was pulled for "Berger Request." These cards were blue and made by the ██████████ staff. This was because there were standard "out-cards" left in some files by Clinton staff.

██████████ could not recall if Mr. Berger was provided with any documents containing the Millennium Alert After Action Report (MAAAR) on his May 30, 2002, visit. [The subsequent physical review of the materials Mr. Berger reviewed did not indicate he was provided such.]

Some of the materials from the May 2002 review were assimilated into the materials responsive to EOP 2 and possibly additional EOP requests. In addition to the out cards left in the boxes from which the documents for Mr. Berger's May 2002 review were originally pulled, ██████████ left out cards referencing they were in the "Berger Request" if those documents were pulled and carried forward in response to EOP 2. In the instances when documents responsive to EOP 2 were still in their original box, an out card was left in the original box indicating the document(s) were withdrawn for "Terror Com" or "Terrorism."

Mr. Berger's review in July 2003

On July 18, 2003, Mr. Berger reviewed original textual documents, four boxes, in ██████████ office. One box contained NSC numbered documents and three boxes contained SMOF files. ██████████ had originally pulled 5 boxes worth of SMOF files. Documents deemed responsive were copied and placed in boxes for ██████████

Case Number: ██████████ b2	Case Title: Samuel R. Berger ██████████ b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

██████████ was running searches for NSC numbered documents in response to EOP2. ██████████ realized searches were running faster than ██████████ could pull the documents. ██████████ decided to create a table listing the NSC numbers that needed to be pulled. ██████████ put them in numerical order and divided which ones could be found at ██████████ and which ones were in ██████████ to make ██████████ job go quicker. (The NSC numbered documents ██████████ had initially pulled were not incorporated into ██████████ table.)

b2,
b6,
b7C

██████████ pulled the NSC numbered documents. ██████████ used the list ██████████ created and annotated the status of the document. If it was pulled from a box, the box number was annotated on the index. If the document was pulled from boxes set aside from Mr. Berger's May 2002 visit, the list was annotated that the document was pulled from the "Berger Box." ██████████ prepared a list of NSC numbered documents ██████████. ██████████ sent this list, of six digit numbers only, to ██████████. ██████████ made "out-cards" for the documents ██████████ pulled in response to the 9/11 commission's requests. If the document was pulled but deemed to be non-responsive, it was placed in a file labeled non-responsive as opposed to being re-filed. If ██████████ found them to be non-responsive, they were marked as non-responsive and either removed or put aside in a file designated as non-responsive to EOP 2. They were not sure if it was the same file or a different non-responsive file.

b2,
b6,
b7C

They narrowed NSC's results based on the subject file. The list was sent over in two batches.

██████████ believed the search runs may be with the materials and the keywords would be reflected at the top of the printout.

b6,
b7C

██████████ pulled SMOF files responsive to EOP 2. ██████████ recalled the NSC sent over copies of SMOF inventory sheets and highlighted the ones the NSC believed were responsive to EOP 2. ██████████ felt the NSC was not consistent and missed some of the relevant folders so ██████████ did a "second SMOF pull/search." The total became SMOF's responsive to EOP2. ██████████ believed ██████████ annotated the NSC inventories with ██████████ handwriting. This became a new artificial file. ██████████ probably still maintains the non-responsive file but these files were probably moved forward for subsequent requests.

b6,
b7C

If documents in the SMOF were deemed responsive, then a tab was placed around those documents, they were copied and provided ██████████.

b2

For the SMOF files, an out card was left to mark the place where a SMOF was removed and indicated it was pulled for "Terror Com" or "Terrorism." In addition, ██████████ wrote on the SMOF, in pencil, where the file came from. These documents have not been re-filed in the originating box.

b6,
b7C

In July 2003, ██████████ came in to assist Mr. Berger by reviewing documents ██████████. ██████████ reviewed the NSC numbered documents from ██████████, responsive to EOP 2.

b2,
b6,
b7C

In July, the textual document sent by facsimile from ██████████ was put in its own folder when received at ██████████. This document contained the MAAAR and is believed to have originated in

b2

Case Number: ██████████ b2	Case Title: Samuel R. Berger ██████████ b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

SMOF [redacted] At some point, either before or after Mr. Berger's visit in October, an [redacted] staff member looked in the folder labeled [redacted] and saw there was a document in the folder. However, it was later determine it did not contain the right document. The original document remains at the [redacted].

b2, b1
b7c

If Mr. Berger or [redacted] with Mr. Berger deemed any NSC numbered documents non-responsive, they were not sure if they were placed in the non-responsive box or put back with the materials.

b6, b7c

For the July production, the NSC sent copies of the file folder lists (inventories), per box, highlighting the SMOF files which they thought were responsive. [redacted] made a note if [redacted] pulled the document or if [redacted] thought it was non-responsive. [redacted] made a new copy of the inventories and determined which [redacted] thought was responsive.

b6, b7c

The production to the White House for EOP2 was done in two deliveries. The first delivery was from what was deemed responsive by [redacted] after Mr. Berger's review. The White House sent a copy of what was not forwarded to the 911 commission to [redacted].

b6, b7c

The second delivery was from what was deemed responsive after [redacted] review. [redacted] sent up documents which were reviewed by [redacted]. Some of these records were deemed non-responsive to EOP 2 while being reviewed by [redacted] and [redacted]. The documents deemed responsive were sent to the White House.

b2, b5, b6, b7c

The White House sent a copy of what was forwarded to the 911 commission to [redacted].

[redacted] staff did not distinguish between the documents pulled for EOP2 and EOP3. The EOP2 request was more restrictive than EOP3. When pulling EOP3, they went back to the production of EOP2. [redacted]

b5

[redacted] They did review the EOP2 documents which the White House did not forwarded to the 9/11 commission. Mr. Berger was provided these documents but they did not know if Mr. Berger reviewed these documents again as he had reviewed them for EOP2.

The White House staff was going to look at what they did not send to the 911 commission for EOP 2 to determine if it was responsive to EOP 3. [redacted] began to review the original files which were pulled for EOP 2 to determine if the documents deemed non-responsive for EOP 2 were responsive to EOP 3. This meant going in a SMOF file and reviewing any material that was not tabbed as responsive to EOP 2. If the tabs were white and had a checkmark on them, the document(s) were copied for EOP 2. NSC numbered documents would have been treated as a whole. [redacted] probably reviewed the documents [redacted] and [redacted] deemed non-responsive for EOP 2 to see if they were responsive to EOP 3. Staff at the [redacted] did a similar search for these materials and sent a copy of documents responsive to EOP 3 to [redacted].

b2, b6, b7c

Mr. Berger's review in September 2003

Mr. Berger was served copies from the [redacted] deemed responsive to EOP3. Mr. Berger was served two SMOF folders from the [redacted] and one SMOF folder from [redacted]. He was served one redwell folder containing NSC numbered documents from [redacted]. He

b2, b6, b7

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

7

was also given all the emails but only had time to review a portion of them. [redacted] marked the emails Mr. Berger reviewed. b6, b7C

[redacted] searched the email system using the search terms which were responsive to EOP 3. b6, b7C

The copies of materials from the SMOFs had a cover sheet indicating where the documents originated. They believed there was only one box of materials provided to Mr. Berger. They could not be sure due to the volume of the emails.

Included in this production was a document sent from [redacted]. The document was placed in a folder someone created labeled [redacted]. Today, the [redacted] document is not in the folder, but two other documents are in this folder. b2

Mr. Berger came to do his review of these documents deemed responsive to EOP 3. This copy set was sent to the White House.

Then a second copy set was pulled and sent. [redacted] took their copy set of what they produced to the White House for EOP 2. This included the documents sent up by [redacted] and [redacted] tabbed the documents the White House sent forward to the 911 commission [redacted] from their copy set. [redacted] and [redacted] began reviewing those documents for responsiveness to EOP 3. [redacted] is unsure if they tabbed the documents which were provided to the White House from this set for EOP 3. b5, b6, b7C

Someone indicated the documents were reviewed after Mr. Berger's visit on September 2, 2003, to determine if anything was missing. [redacted] said there was no review of documents Mr. Berger saw on September 2, 2003, to ensure nothing was missing (not after he left). There was not a control set of documents so there was no way to determine if any documents were removed. Today, there could be an attempt to verify the NSC numbered documents and the SMOFs Mr. Berger was provided. However, the real "wildcard" would be the recreation of the emails Mr. Berger was provided. [redacted] used the search terms to query the email, then [redacted] reviewed those for responsiveness on-line and printed what [redacted] deemed as responsive. This was followed by [redacted] reviewing the documents for responsiveness. b6, b7C

After the September visit, the emails were divided in folders as [redacted], which were served to [redacted]. b2, b6, b7C

In preparation for Mr. Berger's review on October 2, 2003, [redacted] numbered the copies, in pencil, in the bottom left corner. The back page of the document was numbered but not the entire document. A document in this case might contain several pages stapled together. The numbers were assigned sequentially. There was a list of numbers that corresponded to a record type. Then they were organized chronologically and numbered. Most of these documents were emails. [redacted] has a recollection that either [redacted] double-checked the numbering. Neither [redacted] had a recollection of doing this. The documents were placed in folders, b6, b7C

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

separated by responsiveness to paragraphs two and three in the EOP requests. They were also then sorted chronologically. There were about five folders. The numbering sequence was written on the folder. About 25 documents were from SMOF files.

██████████ numbered most of the copies. ██████████ became tired or it was late and ██████████ did not finish numbering the documents. ██████████ provided a note that ██████████ left ██████████ asking ██████████ to complete the numbering the morning of October 2, 2003. ██████████ numbered the remaining documents.

b6,
b7C

Mr. Berger's review in October 2003

On October 2, 2003, Mr. Berger was served one box of textual material and one box of emails. [They removed the emails Berger had reviewed in September. Then they put the emails in order (see list).] These were numbered and placed in folders. The folders were not numbered, only the documents inside. The folders were not served in numerical order. They had been divided by classification and which paragraph they addressed in the EOP request before they were numbered. The folders were in large accordion folders.

Mr. Berger reviewed his and ██████████ notes first. Really, they were the first items in the box. ██████████ could recall the order documents were served as they were not in the room, with the exception of ██████████. Then, Mr. Berger was provided one folder at a time for review.

b6,
b7C

██████████ reviewed folders given to him by ██████████ at his desk to determine if any numbers were missing. They had not thought through what would be done if a document was found to be missing.

b6,
b7C

██████████ was reviewing the folders at someone's desk, outside ██████████ office, when ██████████ discovered #217 missing. ██████████ believed he verified it was missing.

b6, b7C

██████████ gave ██████████ the date of the document before the missing email and the date of the document after the missing email, from email #216 and #218. This was the time frame in which ██████████ searched the emails, using the same search terms which were responsive to the EOP request. The staff was able to verify there was an email that should have been printed and produced to Mr. Berger in that time frame. ██████████ located the missing email. ██████████ then left for the day, before printing the missing email ██████████ called back to the office to ensure ██████████ knew what to look for on the email system in order to find the email in question. ██████████ told ██████████ another copy of this email was printed, ██████████ wrote #217 on the back, and provided to ██████████.

b6,
b7C

██████████ took the email (#217) into Mr. Berger. Shortly after that, ██████████ left ██████████ office. The sofa phone light was lit but then went off. ██████████ went back in ██████████ office and Mr. Berger left abruptly.

b6,
b7C

██████████ commented to ██████████ staff that ██████████ may have not filed #217 (the second copy) in the right place.

Case Number: ██████████ b2	Case Title: Samuel R. Berger ██████████ b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

After determining four documents were missing, on October 3, 2003, [redacted] assisted in running a quick search and reprinted the missing numbered emails. These were differentiated from the originally marked copies by adding the date and time on the back of each.

b6, b7c

The staff noticed [redacted]. However, the date and content was different from the email the sticky was on now (#156).

b5

After picking-up documents from Mr. Berger office, on October 5, 2003, [redacted] spoke to [redacted] and told [redacted] one document was the textural document sent up from Little Rock and the other was #323.

b6, b7c

Additional Notes:

b6, b7c

[redacted] recalled [redacted] instructing Mr. Berger he could take notes but the notes would have to stay at NARA during at least one of his visits, possibly more.

All documents, even copies, were treated as originals. All documents had classification markings on them. [redacted] did not add cover sheets as these were raw unprocessed presidential records. Photocopies were made [redacted] with the designated photocopying machine. All documents provided from the [redacted] were copies.

b2, b6, b7c

[redacted] was involved in the verification of NSC numbered documents NARA still held. [redacted] took the list(s) [redacted] used to pull files for Mr. Berger's visits reflecting the NSC numbered documents. [redacted] compared the NSC numbered documents segregated for Mr. Berger's reviews with the list of the files [redacted] pulled for his visits. [redacted] determined no NSC numbered documents were missing. This is not to say pages could not be missing from those documents. [redacted] was not sure if anyone had determined if the NSC numbered documents Mr. Berger reviewed in May 2002 had been verified.

b6, b7c

[redacted] was asked to verify the documents sent up by the [redacted] which were responsive to EOP 2 and EOP 3. [redacted] recalled that the [redacted] sent up copies of their cover sheets, which were placed on top of the documents they forwarded to [redacted]. The cover sheets had written on them the number of pages the package contained. [redacted] added these up and compared that number to the number of copies [redacted] still had. They matched. [redacted] was able to locate the cover sheets and can locate the documents which were sent to the White House and probably can locate the documents from this pull deemed non-responsive.

b2, b6, b7c

Neither [redacted], nor [redacted] ever wrote up anything concerning this incident or verification. [redacted] was never asked to and did not prepare a statement of facts. However, [redacted] asked [redacted] to prepare a flow chart, which is actually more of a time line. The flow chart is with the administrative files [redacted]. [redacted] provided the drafts of flow charts.

b2, b6, b7c

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

All inventory lists are kept with the series of records. There is not a centralized inventory. If the records are unprocessed the inventory list provided with the documents is used.

[redacted] has a courier card. [redacted] received the card in the mail and was never briefed by NAS and did not sign any receipt or other forms. However, [redacted] received informal training on the transmittal of classified information through ISOO several years ago.

b6, b7C

The original MAAAR was never served to Mr. Berger. It did not come up on any of the search terms. [redacted] staff later searched by the word "Millennium" or the NSC number and provided a copy of the original MAAAR to the White House.

b6, b7C

After Mr. Berger's review, non-responsive documents were normally placed in a separate area. These documents would be reviewed in subsequent requests.

Tabs were being removed for reviewing and copying for several months as the EOP requests extended beyond EOP3. [redacted] staff said there was much room for human error on the exact documents the tabs were placed around. Some of the tabs had notes on them and some were written over. There were two tabs in the bottom of a box, not attached to anything.

b6, b7C

If an NSC numbered document had already been provided in EOP 2 (original), a copy of the NSC numbered document was moved forward to the EOP 3 production. Out cards were only placed in the box when an original was removed. All photocopies of documents provided to Mr. Berger had a cover sheet indicating where the copy originated. Mr. Berger did review documents from [redacted] in response to EOP 3.

b2

The other copies provided to Mr. Berger had a cover sheet on them indicating their origin. Some copies even reflected the NARA "slug."

The staff ensured all emails identified as removed by Mr. Berger were produced. On October 10, 2003, they confirmed everything they expected to have they had and had annotated if they could not find a document during the original search.

Copies of the materials provided to the NSC responsive to the EOP requests are maintained [redacted]

b2

Each collection [redacted] has an inventory. These are kept in folders [redacted]. [redacted] does not create a new inventory but kept the one that came with the boxes from the White House. Each box from the Clinton administration records, the "W" files, stored in the [redacted] is numbered sequentially and has an inventory sheet contained within. A copy of each inventory sheet is kept in a Hollinger box [redacted]. The NSC passed these over as a set.

b2, b6, b7C

[redacted] indicated that copies of classified material were marked with the same classification as the original by virtue of the fact the classification marking on the original carried over to the copy. Furthermore, emails included the classification [redacted] in the metadata that served as the "cover" for the emails.

b2, b6, b7C

Case Number:

[redacted]

b2

Case Title:

Samuel R. Berger [redacted]

b2

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

11

About a month ago, the [redacted] staff went through the documents Mr. Berger reviewed and tracked them down from their final destination [pulled for additional EOP requests] to their originating box.

b6, b7c

[redacted] staff maintains the inventories sent over from the White House. A very few of these inventories are maintained in an electronic finding aid, [redacted].

b2, b6, b7c

The Millennium Alert After Action Review (MAAAR) was 13 pages long.

#150 – has no email content, subject line only, just attachment

#217 – has 3 lines in the email with the attachment

#323 – has a short email, 3 paragraphs, with the attachment

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

EXHIBIT #3

NOTE TO FOIA REQUESTERS

Exhibit #3 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(3)



PDF Version

MS Word Version

(DCID 6/9) — MANUAL

Physical Security Standards for Sensitive Compartmented Information Facilities

(Effective 18 November 2002)

TABLE OF CONTENTS

PREFACE.

1. POLICY AND CONCEPT

1.1 Policy Statement

1.2 Concept

1.3 American Disabilities Act (ADA) Review

2. GENERAL ADMINISTRATIVE

2.1 SCI Facilities (SCIFs)

2.2 Physical Security Preconstruction Review and Approval

2.3 Accreditation

2.4 Co-Utilization

2.5 Personnel Controls

2.6 Control of Combinations

2.7 Entry/Exit Inspections

2.8 Control of Electronic Devices and Other Items

3. PHYSICAL SECURITY CONSTRUCTION POLICY FOR SCIFs

3.1 Construction Policy for SCI Facilities

3.2 Temporary Secure Working Area (TSWA).

3.3 Requirements Common To All SCIFs; Within The US and Overseas

4. CONSTRUCTION SPECIFICATIONS

4.1 Vault Construction Criteria

4.2 SCIF Criteria For Permanent Dry Wall Construction

4.3 SCIF Construction Criteria For Steel Plate

4.4 SCIF Construction Criteria For Expanded Metal.

4.5 General.

5. GLOSSARY

ANNEX A - SCIF Accreditation Checklist

ANNEX B - Intrusion Detection Systems (IDS)

ANNEX C - Tactical Operations/Field Training

PART I - Ground Operation.

PART II - Aircraft/Airborne Operation.

PART III - Shipboard Operation.

ENCLOSURE(9)

EXHIBIT #5

NOTE TO FOIA REQUESTERS

Exhibit #5 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(5)

EXHIBIT #6

NOTE TO FOIA REQUESTERS

Exhibit #6 to this report is redacted in its entirety pursuant to FOIA exemption (b)(2).

ENCLOSURE(6)

MEMORANDUM OF INTERVIEW OR ACTIVITY

Type of Activity: <input checked="" type="checkbox"/> Personal Interview <input type="checkbox"/> Telephone Interview <input type="checkbox"/> Records Review <input type="checkbox"/> Other	Date and Time: July 8, 2005 9:30 a.m.
Activity or Interview of: Samuel R. Berger	Conducted by: <div style="background-color: black; width: 150px; height: 15px; margin-bottom: 5px;"></div> b6, b7C
	Location of Interview/Activity: Washington, DC

Subject Matter/Remarks

On July 8, 2005, [REDACTED] interviewed Samuel "Sandy" R. Berger, former National Security Advisor (NSA) to President William J. Clinton, at the Bond Building, 1400 New York Avenue, Washington, DC. Mr. Berger participated as part of his plea agreement. b6, b7C

Also present were [REDACTED] b6, b7C

Mr. Berger described his personality as intense and a uni-tasker. He did not believe anyone would describe him as arrogant. He did not feel he was overbearing and did not seek to intimidate anyone while at the Archives. Mr. Berger provided the following information:

Mr. Berger visited the Archives, Washington, DC, to review documents requested from the Clinton Presidential materials. Mr. Berger did not have a vivid recollection of visiting the Archives on May 30, 2002, to review documents in preparation for his testimony before the Graham-Goss / Joint Intelligence Committee. Mr. Berger did recall his visits to the Archives to review documents to determine if Executive Privilege needed to be exerted prior to documents being provided to the National Commission on Terrorist Attacks Upon the United States (hereafter, the 9/11 Commission).

On every visit to the Archives, Mr. Berger came in the Pennsylvania Avenue entrance of the Archives, proceeded through the magnetometer, and signed a log book at the security desk. Someone from security called [REDACTED], office and someone from [REDACTED] office would escort Mr. Berger to [REDACTED] office. Mr. Berger always left late in the b6, b7C

Case Number: <div style="background-color: black; width: 80px; height: 15px; margin-bottom: 5px;"></div> b2	Case Title: Samuel R. Berger [REDACTED] b2
--	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

evening, around 7 p.m. There were no guards in the lobby at that time. Therefore, no one ever checked his belongings on his way out.

██████████ was very professional and courteous. However, ██████ was not warm and "fuzzy" with Mr. Berger. ██████ told Mr. Berger he could take notes while he was at the Archives but ██████ made it clear he could not remove them. He did not understand the documents could have been sent to the National Security Council (NSC) for review and classification. [Mr. Berger did ask that his notes from his May 2002 review be sent to the NSC for review. The NSC returned his notes as classified.] He did understand the notes would remain at the Archives for him to use on subsequent visits.

b6,
b7C

All document reviews by Mr. Berger were conducted in ██████ office. Mr. Berger sat at a small table in ██████ office. ██████ did not brief Mr. Berger on security procedures. ██████ must have assumed a briefing was not required due to his previous positions as the NSA. ██████ did not advise Mr. Berger on what he could and could not bring into the Archives. ██████ did not provide Mr. Berger paper. On every visit, Mr. Berger brought his leather portfolio with a note pad inside. It was his practice to wear a suit but he did not recall if he wore a coat to the Archives.

b6,
b7C

Mr. Berger did not believe he received preferential treatment until after his visits when he learned ██████ office was not an appropriate facility to view classified material. Mr. Berger believed he was afforded the opportunity to review documents in a more comfortable environment after someone described the ██████ accommodations to him. At the time of his review, Mr. Berger did not know nor did he consider the nature of ██████ office and whether ██████. He believed he was in a suitable location to review the documents. Mr. Berger did not consider asking that the documents be sent to another location for review as he was not aware of another convenient location to conduct the review.

b2,
b6,
b7C

Mr. Berger stated ██████ of the protocol in reviewing these records ██████ his notes had to remain at the Archives and the Archives would send them to the NSC for classification.

b6,
b7C

Mr. Berger made a general statement that he went to the restroom on an average of every thirty minutes to one hour to use the facilities and stretch his legs. This was the only room he went to besides ██████ office.

b6,
b7C

Mr. Berger explained that after 9/11, the Clinton Administration was inundated with calls on their response to this terrorist attack. It was obvious he was going to have to testify on their actions. Mr. Berger put in over 100 hours of his time, unpaid, in order to be responsive. Everyone else stepped back from the questions but Mr. Berger felt responsible.

Mr. Berger reviewed the documents at the Archives not only for privilege but also to refresh his recollection for his testimony and assisting in preparing others ██████ for their testimony. ██████ only had tangential contact with the records. Mr. Berger had unique knowledge of the records and the appropriate clearances.

b5, b6
b7C

Case Number: ██████████ b2	Case Title: Samuel R. Berger ██████ b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Sumner Watson, Inc.

In May or June 2003, [redacted] called Mr. Berger to say [redacted] received a request from the 9/11 Commission. [redacted] acted as the liaison between the Clinton Administration and the Archives. [redacted] asked Mr. Berger to go to the Archives to review records in response to the Executive Office of the President's (EOP) requests.

3
b6,
b7c

On July 18, 2003, Mr. Berger reviewed material in response to EOP 2. The boxes of materials were on a cart in [redacted] office between Mr. Berger's seat and the coffee table, or off to his side. [redacted] handed Mr. Berger "bunches" of folders. Once he completed the review, [redacted] would hand him another bunch. If [redacted] was not sitting with Mr. Berger, [redacted] was working at [redacted] desk, usually on the computer at an angle to him where he could see [redacted] over his right shoulder.

b6,
b7c

The documents were not organized chronologically. Mr. Berger would read the documents, trying to save all his questions instead of interrupting [redacted] work. He was trying to be sensitive to [redacted] work responsibilities. [redacted] and Mr. Berger would read over the documents on which he had questions. [redacted] ruled on responsiveness to the 9/11 Commission.

b6,
b7c

There were more questions to be answered in July 2003, as this was the first EOP request he was involved with. Some of the questions included what constitutes a document, does the 9/11 Commission want duplicate copies of the same information, do they want copies of the same document that contained additional notes, etc. There were two or three calls to [redacted] on these issues during Mr. Berger's review.

b6,
b7c

Mr. Berger started his own company, Stonebridge, in 2001. [redacted] had [redacted] phone number from setting up appointments for Mr. Berger's visits. He told his secretary not to call him at the Archives unless there was a time sensitive issue. His secretary probably called him at [redacted] number about a half dozen times on this visit. Mr. Berger told [redacted] he was happy to go outside [redacted] office to take the calls. [redacted] asked Mr. Berger if he needed privacy to which he said "yes." [redacted] said instead that [redacted] would go outside [redacted] office while he was on the phone, which [redacted] did. Once this pattern was established, he thought the offer for [redacted] to leave [redacted] office was "standing." [redacted]. Mr. Berger had no intent to order [redacted] out of [redacted] office. While Mr. Berger was on the phone, he was left alone in [redacted] office. He used the phone closest to the couch. It was a hard line and he wanted that privacy with his clients. Mr. Berger did not use his cell phone and never told [redacted] it was not working.

b6,
b7c

Mr. Berger could not recall specifically if [redacted] left [redacted] office when [redacted] made phone calls. The only other time [redacted] left [redacted] office during his reviews was maybe to step out to get more boxes or consult with [redacted] staff. He did not recall if any of [redacted] staff stepped in the office with him when [redacted] stepped for these moments. Mr. Berger did not take any breaks to leave the building during this visit.

b6,
b7c

[redacted]. At some point, Mr. Berger took notes. He realized he was not going to be able to reconstruct in detail all the documents he had reviewed, so he needed to take his notes with him, about ten to twenty pages.

b6,
b7c

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

At the end of the day, Mr. Berger tri-folded his notes and put them in his suit pocket. He took the opportunity to do this when [REDACTED] was out of [REDACTED] office due to him being on a private phone call. Mr. Berger said he did not recall being hesitant to remove his suit jacket during this visit. However, at some point, him not removing his jacket could have been related to the fact he placed the notes in his jacket. Mr. Berger knew he had to leave some notes behind so it would not be obvious he removed notes. He had been making notes and if he did not leave any behind it would have been noticeable. [Mr. Berger was surprised to learn he left only two pages of notes at the Archives.]

b6
b7C

The notes he removed were torn from the top of the note pad. Mr. Berger did not have time to sort through and determine which pages he wanted to take and which to leave. He said this was the scenario on all three occasions when he removed notes from the Archives. He was aware he would not have a complete set but some notes were better than none.

b6, b7C

Mr. Berger did not recall asking [REDACTED] to have the documents arranged chronologically on his next visit. However, he might have mentioned they were not arranged chronologically.

The Millennium Alert After Action Review (MAAR) should have been with the documents Mr. Berger was reviewing on this visit, but he does not recall seeing it. The Principals meeting was in June 2000 and invariably before these meetings a memo reflecting what they were going to talk about would have been circulated. The Principals consisted of the [REDACTED] and others.

b6
b7C

Mr. Berger did not remove any documents on this visit.

[REDACTED] came to the Archives in July 2003, to review documents in response to EOP 2. Mr. Berger did not ask [REDACTED] to look for the MAAR or any other specific documents.

b6
b7C

On **September 2, 2003**, Mr. Berger came to the Archives to review documents in response to EOP 3. Again, the boxes of materials were on a cart in [REDACTED] office between Mr. Berger's seat and the coffee table, or off to his side. [REDACTED] was working with Mr. Berger in the review of the documents. [REDACTED] spent about the same amount of time with Mr. Berger as [REDACTED] had on his visit in July 2003. Mr. Berger could not estimate a percentage on the amount of time. His recollection was that the documents were Xerox copies.

b6
b7C

Again, [REDACTED] always stepped out of [REDACTED] office when Mr. Berger made or received phone calls. [REDACTED] may have also stepped out to consult with [REDACTED] staff, for a minute, but he has no recollection of whether [REDACTED] staff would step in when [REDACTED] was out.

b6
b7C

Mr. Berger was not told anything about the process of the documents after his review and their presentation to the 9/11 Commission. It never occurred to Mr. Berger that by removing the MAAR from the Archives, it would not be provided to the 9/11 Commission. It was his assumption the box of documents he was reviewing at the Archives, or a copy of them, was going from the Archives to the

Case Number: [REDACTED] b2	Case Title: Samuel R. Berger [REDACTED] b2
-------------------------------	---

White House. He did not assume that his removal of documents kept them from going forward to the 9/11 Commission. Mr. Berger knew he was not reviewing originals.

In late November and early December 1999, there were five to fifteen [terrorist] attacks. During this time, the Principals met every day for about an hour. They were operating more like a working group to get through the millennium. During this time, Ahmed Ressay was caught in Washington State with explosives to be used at the Los Angeles International Airport.

b6, b7C

After the millennium, Mr. Berger asked [REDACTED], to prepare the MAAR to determine where they were exposed and the vulnerabilities. There were fights over the jurisdiction of the funding. In March 2001, the Principals approved the recommendations and they were funded. After 9/11, the MAAR was widely discussed in the press. Mr. Berger commented the MAAR was not the most sensitive document he reviewed at the Archives.

Mr. Berger believed the MAAR was widely distributed among the FBI, the CIA, and the Department of State, for a total of about fifteen people. The MAAR was circulated three to four times to four or five people at each agency. All these agencies were subject to the EOP requests. [REDACTED] was going to testify concerning the MAAR.

b6, b7C

Mr. Berger read through the MAAR and took notes. There were twenty-nine topics for recommendations under four categories. He thought the 9/11 Commission would want to know what the Clinton Administration did to "fill in the holes." He was trying to move quickly through the document review. [REDACTED] had told him he still had three more days' worth of documents to review. Mr. Berger now says it was a foolish decision to take the MAAR and the notes out of the Archives.

b6, b7C

Mr. Berger believed this MAAR to be the final report. However, this would have been more likely if this version had a cover page/sheet. Mr. Berger did not return the MAAR to the pile that was returned to [REDACTED]. He did not have a recollection of putting other documents in this folder but he did have the intent to take the document. [There were two documents in what had been an empty folder after he removed the MAAR. [REDACTED] archivists did not move any documents into this folder.] He did not put any intentional markings on the documents. Mr. Berger did not recall receiving this folder separately from other folders. He did not recall seeing any other versions of the MAAR on this visit.

b6, b7C

During this visit, Mr. Berger received more calls as there were two op-ed articles out. One article stated Sudan offered Osama Bin Laden to the United States in 1996 but the Clinton Administration did not take the offer. Mr. Berger referred to this as an urban legend. The other article was by former Secretary of Defense Casper Weinberger who said the Clinton Administration was responsible for the attacks on September 11, 2001. These articles initiated a "flurry" of activities.

Mr. Berger took the first opportunity when [REDACTED] was out of [REDACTED] office to remove the document. He most likely put it in his jacket pocket, after folding it, but he does not have a precise recollection of where he put the document. It is perceivable he put it in his pants pocket. It was also possible he placed it in his portfolio and took it out. The document was twelve to thirteen pages. The notes were folded and put in his pocket. He would have put the notes on his person at the end of the day.

b6, b7C

Case Number:

[REDACTED]

b2

Case Title:

Samuel R. Berger [REDACTED]

b2

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

5
b6
b7c

Mr. Berger did not believe [redacted] personnel were suspicious that he was removing documents. They did not give him any indications of this.

Mr. Berger denied removing any documents in his socks. [He asked us to describe what the potential witness saw, which we did.] He stated his shoes frequently come untied [To which [redacted] said he was a witness.] and his socks frequently fall down. [At that point, Mr. Berger lifted his pant leg to reveal a sock falling down his ankle and pale skin.] Besides, it would have fallen out of his sock. He said this story was absurd and embarrassing.

b6
b7c

After leaving the Archives for the day, Mr. Berger went back to his office and put the document in an envelope on his desk.

On September 2, 2003, Mr. Berger called someone who was helping him review materials. He told them they should be prepared to answer the 9/11 Commission's questions concerning the MAAR.

It was asked that [redacted], former Clinton staffer, be cleared to review these documents. Mr. Berger had not worked on a document search in thirty years. If he was working at the NSC, this is certainly something someone on his staff would have done for him. [redacted] was able to [redacted] cleared for [redacted] material but the [redacted] clearance.

b2
b6
b7c

On **October 2, 2003**, Mr. Berger was reviewing documents at the Archives. The documents were in accordion files. [redacted] had the documents in a box, on the floor, by [redacted] desk. The time [redacted] spent with him in reviewing the documents did not change. He did not recall NARA staff being more or less restrictive with the documents than on other visits.

b6
b7c

[redacted] first provided Mr. Berger the documents marked for review by [redacted]. A version of the MAAR was with these documents, marked [redacted]. Mr. Berger did not know why it was classified differently than the version he removed in September which was [redacted]. It was obvious to him this was a different version of the MAAR. Mr. Berger wanted to know how it was edited to now be classified as [redacted]. He needed to compare the two versions of the MAAR. [redacted] had mentioned the MAAR went through several iterations but the changes were over money not substantive. Mr. Berger placed this version under his portfolio while [redacted] assistant was in the office. He then returned the folder to [redacted] assistant. Mr. Berger has no recollection of post-it notes on this document or moving them to another document. The assistant was standing in the area by [redacted] desk where the files were.

b2
b6
b7c

Next, [redacted] provided him all but two documents the White House had sent back from the documents he reviewed for EOP 2. [The White House sent those two documents on to the 9/11 Commission.]

b5
b1
b7c

[Large redacted block]

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Then they turned to the documents of the day. This time, the emails were organized. He recalled being handed the documents individually, not in a folder. About mid-day, Mr. Berger came across another version of the MAAR. In October, Mr. Berger saw a version of the MAAR and now had doubts that what he removed in September was the final report. At this point, he wanted to track the evolution of the MAAR. He slid the document under his portfolio.

██████████ told Mr. Berger there was a missing document, one that ██████████ could not find. Mr. Berger said at this point "the bomb should have burst in the air, but obviously it did not." However, Mr. Berger did apprehend the consequences of what ██████████ said. Mr. Berger disassembled first, then he asked ██████████ if the document could have been misfiled. ██████████ said "No." Mr. Berger asked if they had not produced this document already. ██████████ said it was a different version.

b6,
b7C

██████████ gave him another copy of the document. Mr. Berger slid this document under his portfolio also. ██████████ did not ask for it back. If ██████████ had asked for it back, it would have "triggered" a decision for him to give the documents back.

b6,
b7C

In total, he removed four documents, all versions of the MAAR. Mr. Berger does not recall if he placed all the documents on his person at once or at different times. He did not put the documents on his person until he was alone. He removed the notes, about fifteen pages, towards the end of the day.

Mr. Berger had a long day and wanted to go home around 6 p.m. ██████████ wanted him to finish the review and said they only had about an hours worth of work left. He understood ██████████ was getting pressure from the White House to provide a response so he agreed. ██████████ suggested he take a walk and come back and finish up. Mr. Berger left the building with all the documents he put in his pockets. He was aware of the risk he was taking, but he also knew ██████████.

b2,
b6, b7C

Mr. Berger exited the Archives on to Pennsylvania Avenue, the north entrance. It was dark. He did not want to run the risk of bringing the documents back in the building risking the possibility ██████████ might notice something unusual. He headed towards a construction area on Ninth Street. Mr. Berger looked up and down the street, up into the windows of the Archives and the DOJ, and did not see anyone. He removed the documents from his pockets, folded the notes in a "V" shape and inserted the documents in the center. He walked inside the construction fence and slid the documents under a trailer.

b6,
b7C

Mr. Berger came back into the building without fearing the documents might slip out of his pockets or that ██████████ and ██████████ staff would notice that his pockets were bulging. ██████████

b2,
b6, b7C

If Mr. Berger had been aware ██████████ staff was tracking the documents he was provided, he would not have removed them. He also said that if staff had escorted him out of the building for his walk, he would have felt less confident that no one was in the area and someone might be watching his actions.

b6,
b7C

Case Number: ██████████ b2	Case Title: Samuel R. Berger ██████████ b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Mr. Berger does not recall reviewing his notes or [redacted] notes on this visit. b6, b7C

It is possible that [redacted], stopped by to introduce [redacted] but Mr. Berger did not have a vivid memory of this. b6, b7C

Mr. Berger was trying to balance his review carefully but was also trying to be expeditious. He skipped meals and drank diet cokes. He did go to the restroom, possibly with documents in his pockets, but did not discard documents there or rearrange them on his person. b6, b7C

On this visit, [redacted].

[redacted] did not tell Mr. Berger that [redacted] had numbered the documents or that [redacted] had a way of tracking these records. Mr. Berger said he would have "picked-up" on that comment. He said "I may be stupid, but I am not self destructive." As he left for the day between 7 and 7:30 p.m., [redacted] asked Mr. Berger [redacted]. He totally missed that signal later realizing it was [redacted] subtle way to ask him if he removed documents. Mr. Berger believed no one knew he removed documents. b6, b7C

Mr. Berger left the building, retrieved the documents and notes from the construction area, and returned to his office.

On **October 4, 2003**, late in the afternoon, [redacted] called Mr. Berger to tell him [redacted] called from the Archives. Mr. Berger was aware [redacted] was the [redacted]. [redacted] said documents were missing after Mr. Berger's visit on October 2, 2003. Mr. Berger panicked because he realized he was caught. Mr. Berger lied to [redacted] telling [redacted] he did not take the documents. b6, b7C

Mr. Berger remembers next calling [redacted] at [redacted] office. He knew it was not a good sign [redacted] was there on a Saturday. [redacted] described the documents stating there were four copies of three documents missing. Mr. Berger asked [redacted] if the four documents they were missing were copies of the MAAR. He told [redacted] he would see if he accidentally took them. Mr. Berger was agitated because he realized he was caught. b6, b7C

[redacted] called Mr. Berger and said "I hope you can find them because if not, we have to refer this to the NSC's [redacted]." [redacted] did not say what would be done if Mr. Berger returned the documents. When asked again, Mr. Berger became unsure whether [redacted] said this to him. However, he was sure the source of the statement was [redacted] asked Mr. Berger to go to his office to see if he could find the documents. b5, b6, b7C

Mr. Berger drove to his office late that afternoon. On the night of October 2, 2003, he had destroyed, cut into small pieces, three of the four documents. These were put in the trash. By Saturday, the trash had been picked-up. He tried to find the trash collector but had no luck. Neither [redacted] nor [redacted] offered to help him look through the trash. b6, b7C

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc.

9
b6,
b7c

About 7 p.m., Mr. Berger called [redacted] and said "I think I solved the mystery." [redacted] said [redacted] was going into [redacted] and would call as soon as it was over. About 11:30 p.m., Mr. [redacted] called Mr. Berger. Mr. Berger told [redacted], "I found two documents but not the other two." [redacted] told him to get the documents from his office and lock them in the safe in his home. [redacted] was glad he found two but three were still missing.

Mr. Berger did not recall [redacted], unless [redacted] picked-up the documents.

b6, b7c

On **October 5, 2003**, Mr. Berger recalled NARA staff picking up the two documents at his home. He understands that NARA staff recalled picking up the documents at his office. Mr. Berger was willing to accept that NARA staff came to his office.

There were additional conference calls. [redacted] was surprised when Mr. Berger returned the documents he removed in September. He knew he was caught, so he purported he must have removed the documents accidentally or inadvertently by sweeping them up with his documents. Later, Mr. Berger made a decision, on his own, to tell the truth. He said "I realized I was giving a benign explanation for what was not benign." Mr. Berger wanted to return everything he had taken. He realized he was returning documents he removed in September. He did not realize he returned more than they knew he removed. Mr. Berger was aware of the consequences but he knew returning the documents was the right thing to do.

b6, b7c

Mr. Berger called [redacted] told [redacted] what happened, and asked what he should do. [redacted] told Mr. Berger to get a lawyer. Mr. Berger and [redacted] did not discuss this issue any further as they were [redacted] and knew it was better not to talk about this.

b6,
b7c

Mr. Berger specifically recalled returning his notes to NARA staff at his home. He had flown in from New York, spent about an hour at his home, then flew back to New York to continue his travel. NARA staff never mentioned his notes. Mr. Berger believed if he had not returned them, they would never have known he removed his notes.

Mr. Berger does not know [redacted], nor did he have any contact with [redacted]. Mr. Berger had not met [redacted] prior to these visits to the Archives. Additionally, he did not contact the NSC on this matter.

b6,
b7c

There were not any handwritten notes on the documents Mr. Berger removed from the Archives. Mr. Berger did not believe there was unique information in the three documents he destroyed. Mr. Berger never made any copies of these documents.

Mr. Berger said as a general point, he has dealt with classified information for twelve years. Some documents are sensitive and some are not super sensitive. This may not have anything to do with the documents classification. Other documents he reviewed had more sensitive information in them such as the Presidential Findings. He had seen most of the information in the MAAR disclosed in the press. He substituted his sense of sensitivity instead of thinking of classification. The MAAR did not involve sources and methods. It was a policy document.

Case Number: [redacted] v2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Obtained via FOIA by Judicial Watch, Inc

Some of the notes he removed did have information about the Presidential Findings. This was the authority from the President for actions to be taken.

██████████ had no reason to believe he was not acting in an appropriate manner. Mr. Berger said if there was always someone with him, he would not have taken any documents. After learning he was given special treatment by viewing the documents in ██████████ office, he suggested no exceptions to the rules should be given to former National Security Advisors or others. The Archives should thoroughly check people when they enter and exit the building. *b6, b7c*

Mr. Berger received enough phone calls which gave him the opportunity to remove the documents. He never sent ██████████ out of the room for the sole purpose of removing the documents. *b6, b7c*

The DOJ asked Mr. Berger if he removed any other documents from the Archives that we were not aware of to which Mr. Berger replied no.

Case Number: ██████████ <i>b2</i>	Case Title: Samuel R. Berger ██████████ <i>b2</i>
--------------------------------------	--

EXHIBIT #8

NOTE TO FOIA REQUESTERS

Exhibit #8 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE (8)

b6, b7C

He walked out the door and into the hallway. The door closed. Shortly after it closed, started down the hall, he was stooped over right outside the doorway. He was fiddling with something white which looked to be a piece of paper or multiple pieces of paper. It appeared to be rolled around his ankle and underneath his pant leg, with a portion of the paper sticking out underneath.

ENCLOSURE(9)

EXHIBIT #10

NOTE TO FOIA REQUESTERS

Exhibit #10 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE (c)

EXHIBIT #11

NOTE TO FOIA REQUESTERS

Exhibit #11 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(1)

EXHIBIT #12

NOTE TO FOIA REQUESTERS

Exhibit #12 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(12)

EXHIBIT #13

NOTE TO FOIA REQUESTERS

Exhibit #13 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE (3)

EXHIBIT #14

NOTE TO FOIA REQUESTERS

Exhibit #14 to this report is redacted in its entirety pursuant to FOIA exemption (b)(2).

ENCLOSURE(14)

EXHIBIT #15

NOTE TO FOIA REQUESTERS

Exhibit #15 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(S)

EXHIBIT #16

NOTE TO FOIA REQUESTERS

Exhibit #16 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(16)

MEMORANDUM OF INTERVIEW OR ACTIVITY

Type of Activity: <input type="checkbox"/> Personal Interview <input type="checkbox"/> Telephone Interview <input checked="" type="checkbox"/> Records Review <input type="checkbox"/> Other	Date and Time: June 2005
Activity or Interview of: Verification of Documents	Conducted by: <div style="background-color: black; width: 100px; height: 15px; margin-bottom: 5px;"></div> b6, b7C
	Location of Interview/Activity: Archives I, Washington, DC

Subject Matter/Remarks

This verification was done in [redacted] by [redacted]. This verification was done with the assistance of [redacted] and [redacted], in June 2005. Spreadsheets were generated in this verification process. They show the files identified as served on each visit and detailed notes.

b2,
b6,
b7C

First, we went through all the [redacted] boxes [redacted] and recorded the information from all the "out cards" placed in those boxes. (If the box was sealed we interpreted that to be indicative it had not been opened since it arrived.) The out-cards were different colors to distinguish between the out-cards left behind from the Clinton Administration.

b2,
b6, b7C

Next we went to the boxes which were provided to Sandy Berger on May 30, 2002. We verified each National Security Council (NSC) numbered package he was provided was still available as a package. We cannot verify each page is intact. The originals were unassembled, photo copied, and then reassembled in the same order by [redacted]. (This negated the need to look for torn corners still remaining in the packages.) Each package may contain multiple documents which may or may not be numbered sequentially. Some pages contain changes and only those pages are attached, not the full document.

b6, b7C

We verified each SMOF folder was still at NARA. We cannot verify the content of each folder. (We know documents had been removed from the folder titled [redacted] and others placed in the folder.) [redacted] has a file folder list but not a document level inventory. (Box 49 is the exception because the folder titles do not match the contents list.) The file folder lists reflecting the titles were with [redacted].

b2,
b6, b7C

For the documents Mr. Berger was served in May 2002, we verified all the NSC numbered packages and the Staff Member Office Files (SMOF) folders [redacted]. (Whole SMOF files were

b2,
b6, b7C

Case Number: <div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> b2	Case Title: Samuel R. Berger [redacted] b2
--	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

2

provided to Mr. Berger but we believe [redacted] placed the documents [redacted] deemed non-responsive in an envelope in the back of the SMOF file.) For the May 2002 visit, no one reviewed documents pulled [redacted]. Mr. Berger took notes and left them with [redacted] to send to the NSC for classification. These were classified [redacted] [Note: Mr. Berger's notes reflected he reviewed a document similar to Millennium Alert After Action Report but not a copy of it. This document is believed to still be at NARA.]

b2,
b6,
b7C

For the documents Mr. Berger was served in July 2003 [EOP 2], we verified all NSC numbered packages and SMOF folders [redacted]. We did not verify any page counts as Mr. Berger was provided with original NSC numbered packages and original SMOF folders (with the responsive documents tabbed).

b2, b6,
b7C

Mr. Berger took notes on a notepad he brought to NARA. Mr. Berger stated he removed notes when [redacted] left [redacted] office. He later provided these notes to [redacted]. Two pages of notes were turned over by [redacted] with an annotation indicating the notes were from Mr. Berger's July 2003 review. Two pages of notes remain [redacted] from this visit.

b2,
b6, b7C

For July 2003 [EOP 2], [redacted] reviewed the documents pulled at [redacted] and sent to [redacted]. Mr. Berger did not review these documents at this time.

b6,
b7C

For the documents Mr. Berger was served in September 2003 [EOP 3], we verified all the NSC numbered packages and SMOF folders [redacted]. The SMOF files were reviewed and responsive materials were tabbed. Copies were made of the tabbed materials and served to Mr. Berger. We compared the items served to Mr. Berger and the tabbed documents from the SMOF files to verify page counts. The NSC numbered documents were not verified for page count as originals were served.

b2, b6,
b7C

[redacted] had sent up copies of documents responsive to EOP 3 which Mr. Berger reviewed. At one point, after it was discovered Mr. Berger removed documents, [redacted] requested [redacted] send up the cover sheet of each document along with the page count of the document. [redacted] verified the page count provided by [redacted] was the same as the copy set provided to Mr. Berger. This was verified again during this review.

b6,
b7C

In September 2003, emails were provided to Mr. Berger (see notes under ADDITIONAL CLARIFICATION).

Mr. Berger said he removed notes on the September visit.

For the documents Mr. Berger was served in October 2003 [EOP 3], we verified the page count of the copies of the NSC numbered documents provided to Mr. Berger with the page count of the original NSC numbered documents. (Keep in mind there is no way to verify all the pages of the original NSC numbered documents were accurate as Mr. Berger had access to some or all of these originals in May 2002; and July and September 2003.)

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

The documents were not in chronological order. Email #150 was placed at the front of the file so Mr. Berger would readily see it.

The SMOF files were reviewed and responsive materials were tabbed. Copies were made of the tabbed materials and served to Mr. Berger. For some reason (possibly the 9/11 commissions review) the tabs were removed. Instead, we compared the items served to Mr. Berger with the tabbed documents from the files to verify page counts.

This accounted for items numbered by [redacted] as 339 – 379. Items 1 – 338 are emails (see notes below).

b2

ADDITIONAL CLARIFICATION:

The original recovered documents are [redacted] at NARA. The original recovered notes are at the FBI.

b2

It was determined that it would be unrealistic to take Mr. Berger's notes and try to match them to each review. This is problematic as Mr. Berger's notes are not dated. His notes do not reference a document number or SMOF title, only a date. The boxes of what was produced on each visit do not exist as they did and it would take a considerable effort to recreate those. Also, Mr. Berger may have annotated in his words or from his recollection instead of taking exact notes off a document.

When pulling emails for EOP3, [redacted] used the search string provided by the NSC. [redacted] also searched by individual names and additional terms. [redacted] sat at the computer and reviewed the emails. If [redacted] thought they were non-responsive, they were never printed. [redacted] wrote the file number on the back of each email. After [redacted] printed the email, they were reviewed again for responsiveness, possibly by [redacted].

b6,

b7C

To re-create this search for the email, [redacted] would have to determine the search terms and then filter out what [redacted] believed to be non-responsive. The remaining emails could be printed and compared to the emails provided to Mr. Berger for EOP3. Any emails for which there was not a duplicate copy could be reviewed again for responsiveness. This might give you emails which might be missing. This review would involve looking at a couple thousand emails. Currently, there is a problem with the email server and it is not accessible.

b6,

b7C

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY

Type of Activity: <input checked="" type="checkbox"/> Personal Interview <input type="checkbox"/> Telephone Interview <input type="checkbox"/> Records Review <input type="checkbox"/> Other	Date and Time: July 8, 2005 9:30 a.m.
Activity or Interview of: Samuel R. Berger	Conducted by: SA Kelly Maltagliati
	Location of Interview/Activity: Washington, DC

Subject Matter/Remarks

On July 8, 2005, Special Agent (SA) Kelly Maltagliati and Assistant Inspector General for Investigations Tracy Burnett interviewed Samuel "Sandy" R. Berger, former National Security Advisor (NSA) to President William J. Clinton, at the Bond Building, 1400 New York Avenue, Washington, DC. Mr. Berger participated as part of his plea agreement.

Also present were Paul Brachfeld, National Archives and Records Administration (NARA), Inspector General; Noel Hillman, Department of Justice (DOJ), Public Integrity Section (PIS), Chief; Dan Petalas, DOJ, PIS, Trial Attorney; Thomas Reilly, DOJ, Counterespionage Section (CES); Greg Leylegian, Federal Bureau of Investigation, CES; Lanny Breuer, Attorney at Law; and David Fagan, Attorney at Law.

Mr. Berger described his personality as intense and a uni-tasker. He did not believe anyone would describe him as arrogant. He did not feel he was overbearing and did not seek to intimidate anyone while at the Archives. Mr. Berger provided the following information:

Mr. Berger visited the Archives, Washington, DC, to review documents requested from the Clinton Presidential materials. Mr. Berger did not have a vivid recollection of visiting the Archives on May 30, 2002, to review documents in preparation for his testimony before the Graham-Goss / Joint Intelligence Committee. Mr. Berger did recall his visits to the Archives to review documents to determine if Executive Privilege needed to be exerted prior to documents being provided to the National Commission on Terrorist Attacks Upon the United States (hereafter, the 9/11 Commission).

On every visit to the Archives, Mr. Berger came in the Pennsylvania Avenue entrance of the Archives, proceeded through the magnetometer, and signed a log book at the security desk. Someone from security called Nancy Smith's, Director, Presidential Materials Staff (NLMS), office and someone from Ms. Smith's office would escort Mr. Berger to Ms. Smith's office. Mr. Berger always left late in the

Case Number: 04-001-GC	Case Title: Samuel R. Berger, et al.
---------------------------	---

evening, around 7 p.m. There were no guards in the lobby at that time. Therefore, no one ever checked his belongings on his way out.

Ms. Smith was very professional and courteous. However, she was not warm and "fuzzy" with Mr. Berger. Ms. Smith told Mr. Berger he could take notes while he was at the Archives but she made it clear he could not remove them. He did not understand the documents could have been sent to the National Security Council (NSC) for review and classification. [Mr. Berger did ask that his notes from his May 2002 review be sent to the NSC for review. The NSC returned his notes as classified.] He did understand the notes would remain at the Archives for him to use on subsequent visits.

All document reviews by Mr. Berger were conducted in Ms. Smith's office. Mr. Berger sat at a small table in her office. Ms. Smith did not brief Mr. Berger on security procedures. She must have assumed a briefing was not required due to his previous positions as the NSA. Ms. Smith did not advise Mr. Berger on what he could and could not bring into the Archives. Ms. Smith did not provide Mr. Berger paper. On every visit, Mr. Berger brought his leather portfolio with a note pad inside. It was his practice to wear a suit but he did not recall if he wore a coat to the Archives.

Mr. Berger did not believe he received preferential treatment until after his visits when he learned Ms. Smith's office was not an appropriate facility to view classified material. Mr. Berger believed he was afforded the opportunity to review documents in a more comfortable environment after someone described the Special Compartmentalized Information Facility (SCIF) accommodations to him. At the time of his review, Mr. Berger did not know nor did he consider the nature of Ms. Smith's office and whether it was a SCIF. He believed he was in a suitable location to review the documents. Mr. Berger did not consider asking that the documents be sent to another location for review as he was not aware of another convenient location to conduct the review.

Mr. Berger stated Bruce Lindsey, President Clinton's representative, did not inform him of the protocol in reviewing these records or that his notes had to remain at the Archives and the Archives would send them to the NSC for classification.

Mr. Berger made a general statement that he went to the restroom on an average of every thirty minutes to one hour to use the facilities and stretch his legs. This was the only room he went to besides Ms. Smith's office.

Mr. Berger explained that after 9/11, the Clinton Administration was inundated with calls on their response to this terrorist attack. It was obvious he was going to have to testify on their actions. Mr. Berger put in over 100 hours of his time, unpaid, in order to be responsive. Everyone else stepped back from the questions but Mr. Berger felt responsible.

Mr. Berger reviewed the documents at the Archives not only for privilege but also to refresh his recollection for his testimony and assisting in preparing others (President Clinton, Vice President Gore, Secretary of State Madeline Albright, etc.) for their testimony. Nancy Soderberg, former Clinton staffer, only had tangential contact with the records. Mr. Berger had unique knowledge of the records and the appropriate clearances.

Case Number: 04-001-GC	Case Title: Samuel R. Berger, et al.
---------------------------	---

In May or June 2003, Mr. Lindsey called Mr. Berger to say he received a request from the 9/11 Commission. Mr. Lindsey acted as the liaison between the Clinton Administration and the Archives. Mr. Lindsey asked Mr. Berger to go to the Archives to review records in response to the Executive Office of the President's (EOP) requests.

On **July 18, 2003**, Mr. Berger reviewed material in response to EOP 2. The boxes of materials were on a cart in Ms. Smith's office between Mr. Berger's seat and the coffee table, or off to his side. Ms. Smith handed Mr. Berger "bunches" of folders. Once he completed the review, she would hand him another bunch. If she was not sitting with Mr. Berger, Ms. Smith was working at her desk, usually on the computer at an angle to him where he could see her over his right shoulder.

The documents were not organized chronologically. Mr. Berger would read the documents, trying to save all his questions instead of interrupting Ms. Smith's work. He was trying to be sensitive to her work responsibilities. Ms. Smith and Mr. Berger would read over the documents on which he had questions. Ms. Smith ruled on responsiveness to the 9/11 Commission.

There were more questions to be answered in July 2003, as this was the first EOP request he was involved with. Some of the questions included what constitutes a document, does the 9/11 Commission want duplicate copies of the same information, do they want copies of the same document that contained additional notes, etc. There were two or three calls to Mr. Lindsey on these issues during Mr. Berger's review.

Mr. Berger started his own company, Stonebridge, in 2001. His secretary, Jane Cushman, had Ms. Smith's phone number from setting up appointments for Mr. Berger's visits. He told his secretary not to call him at the Archives unless there was a time sensitive issue. His secretary probably called him at Ms. Smith's number about a half dozen times on this visit. Mr. Berger told Ms. Smith he was happy to go outside her office to take the calls. Ms. Smith asked Mr. Berger if he needed privacy to which he said "yes." Ms. Smith said instead that she would go outside her office while he was on the phone, which she did. Once this pattern was established, he thought the offer for her to leave her office was "standing." Ms. Smith never appeared to be upset about leaving her office. Mr. Berger had no intent to order her out of her office. While Mr. Berger was on the phone, he was left alone in Ms. Smith's office. He used the phone closest to the couch. It was a hard line and he wanted that privacy with his clients. Mr. Berger did not use his cell phone and never told Ms. Smith it was not working.

Mr. Berger could not recall specifically if Ms. Smith left her office when she made phone calls. The only other time Ms. Smith left her office during his reviews was maybe to step out to get more boxes or consult with her staff. He did not recall if any of Ms. Smith's staff stepped in the office with him when she stepped for these moments. Mr. Berger did not take any breaks to leave the building during this visit.

Ms. Smith did not appear to be upset about the manner in which he was viewing the documents. She never requested that he keep the documents in their original order. At some point, Mr. Berger took notes. He realized he was not going to be able to reconstruct in detail all the documents he had reviewed, so he needed to take his notes with him, about ten to twenty pages.

Case Number:
04-001-GC

Case Title:
Samuel R. Berger, et al.

At the end of the day, Mr. Berger tri-folded his notes and put them in his suit pocket. He took the opportunity to do this when Ms. Smith was out of her office due to him being on a private phone call. Mr. Berger said he did not recall being hesitant to remove his suit jacket during this visit. However, at some point, him not removing his jacket could have been related to the fact he placed the notes in his jacket. Mr. Berger knew he had to leave some notes behind so it would not be obvious he removed notes. He had been making notes and if he did not leave any behind it would have been noticeable. [Mr. Berger was surprised to learn he left only two pages of notes at the Archives.]

The notes he removed were torn from the top of the note pad. Mr. Berger did not have time to sort through and determine which pages he wanted to take and which to leave. He said this was the scenario on all three occasions when he removed notes from the Archives. He was aware he would not have a complete set but some notes were better than none.

Mr. Berger did not recall asking Ms. Smith to have the documents arranged chronologically on his next visit. However, he might have mentioned they were not arranged chronologically.

The Millennium Alert After Action Review (MAAR) should have been with the documents Mr. Berger was reviewing on this visit, but he does not recall seeing it. The Principals meeting was in June 2000 and invariably before these meetings a memo reflecting what they were going to talk about would have been circulated. The Principals consisted of the Attorney General, the Secretary of State, the Deputy Director of the Federal Bureau of Investigation (FBI), the Director of the Central Intelligence Agency (CIA), the National Security Advisor for the vice president, and others.

Mr. Berger did not remove any documents on this visit.

Ms. Soderberg came to the Archives in July 2003, to review documents in response to EOP 2. Mr. Berger did not ask Ms. Soderberg to look for the MAAR or any other specific documents.

On **September 2, 2003**, Mr. Berger came to the Archives to review documents in response to EOP 3. Again, the boxes of materials were on a cart in Ms. Smith's office between Mr. Berger's seat and the coffee table, or off to his side. Ms. Smith was working with Mr. Berger in the review of the documents. Ms. Smith spent about the same amount of time with Mr. Berger as she had on his visit in July 2003. Mr. Berger could not estimate a percentage on the amount of time. His recollection was that the documents were Xerox copies.

Again, Ms. Smith always stepped out of her office when Mr. Berger made or received phone calls. She may have also stepped out to consult with her staff, for a minute, but he has no recollection of whether her staff would step in when she was out.

Mr. Berger was not told anything about the process of the documents after his review and their presentation to the 9/11 Commission. It never occurred to Mr. Berger that by removing the MAAR from the Archives, it would not be provided to the 9/11 Commission. It was his assumption the box of documents he was reviewing at the Archives, or a copy of them, was going from the Archives to the

Case Number:
04-001-GC

Case Title:
Samuel R. Berger, et al.

White House. He did not assume that his removal of documents kept them from going forward to the 9/11 Commission. Mr. Berger knew he was not reviewing originals.

In late November and early December 1999, there were five to fifteen [terrorist] attacks. During this time, the Principals met every day for about an hour. They were operating more like a working group to get through the millennium. During this time, Ahmed Ressam was caught in Washington State with explosives to be used at the Los Angeles International Airport.

After the millennium, Mr. Berger asked Richard Clarke, White House terrorism adviser, to prepare the MAAR to determine where they were exposed and the vulnerabilities. There were fights over the jurisdiction of the funding. In March 2001, the Principals approved the recommendations and they were funded. After 9/11, the MAAR was widely discussed in the press. Mr. Berger commented the MAAR was not the most sensitive document he reviewed at the Archives.

Mr. Berger believed the MAAR was widely distributed among the FBI, the CIA, and the Department of State, for a total of about fifteen people. The MAAR was circulated three to four times to four or five people at each agency. All these agencies were subject to the EOP requests. Mr. Clarke was going to testify concerning the MAAR.

Mr. Berger read through the MAAR and took notes. There were twenty-nine topics for recommendations under four categories. He thought the 9/11 Commission would want to know what the Clinton Administration did to "fill in the holes." He was trying to move quickly through the document review. Ms. Smith had told him he still had three more days' worth of documents to review. Mr. Berger now says it was a foolish decision to take the MAAR and the notes out of the Archives.

Mr. Berger believed this MAAR to be the final report. However, this would have been more likely if this version had a cover page/sheet. Mr. Berger did not return the MAAR to the pile that was returned to Ms. Smith. He did not have a recollection of putting other documents in this folder but he did have the intent to take the document. [There were two documents in what had been an empty folder after he removed the MAAR. NLMS archivists did not move any documents into this folder.] He did not put any intentional markings on the documents. Mr. Berger did not recall receiving this folder separately from other folders. He did not recall seeing any other versions of the MAAR on this visit.

During this visit, Mr. Berger received more calls as there were two op-ed articles out. One article stated Sudan offered Osama Bin Laden to the United States in 1996 but the Clinton Administration did not take the offer. Mr. Berger referred to this as an urban legend. The other article was by former Secretary of Defense Casper Weinberger who said the Clinton Administration was responsible for the attacks on September 11, 2001. These articles initiated a "flurry" of activities.

Mr. Berger took the first opportunity when Ms. Smith was out of her office to remove the document. He most likely put it in his jacket pocket, after folding it, but he does not have a precise recollection of where he put the document. It is perceivable he put it in his pants pocket. It was also possible he placed it in his portfolio and took it out. The document was twelve to thirteen pages. The notes were folded and put in his pocket. He would have put the notes on his person at the end of the day.

Case Number: 04-001-GC	Case Title: Samuel R. Berger, et al.
---------------------------	---

Mr. Berger did not believe NLMS personnel were suspicious that he was removing documents. They did not give him any indications of this.

Mr. Berger denied removing any documents in his socks. [He asked us to describe what the potential witness saw, which we did.] He stated his shoes frequently come untied [To which Mr. Breuer said he was a witness.] and his socks frequently fall down. [At that point, Mr. Berger lifted his pant leg to reveal a sock falling down his ankle and pale skin.] Besides, it would have fallen out of his sock. He said this story was absurd and embarrassing.

After leaving the Archives for the day, Mr. Berger went back to his office and put the document in an envelope on his desk.

On September 2, 2003, Mr. Berger called someone who was helping him review materials. He told them they should be prepared to answer the 9/11 Commission's questions concerning the MAAR.

It was asked that Steve Naplan, former Clinton staffer, be cleared to review these documents. Mr. Berger had not worked on a document search in thirty years. If he was working at the NSC, this is certainly something someone on his staff would have done for him. Ms. Smith was able to get Mr. Naplan cleared for TOP SECRET material but the CIA would not pay for his [Sensitive Compartmented Information] clearance.

On **October 2, 2003**, Mr. Berger was reviewing documents at the Archives. The documents were in accordion files. Ms. Smith had the documents in a box, on the floor, by her desk. The time Ms. Smith spent with him in reviewing the documents did not change. He did not recall NARA staff being more or less restrictive with the documents than on other visits.

Ms. Smith first provided Mr. Berger the documents marked for review by Mr. Naplan. A version of the MAAR was with these documents, marked SECRET. Mr. Berger did not know why it was classified differently than the version he removed in September which was TOP SECRET CODEWORD. It was obvious to him this was a different version of the MAAR. Mr. Berger wanted to know how it was edited to now be classified as SECRET. He needed to compare the two versions of the MAAR. Mr. Clarke had mentioned the MAAR went through several iterations but the changes were over money not substantive. Mr. Berger placed this version under his portfolio while Ms. Smith's assistant was in the office. He then returned the folder to Ms. Smith's assistant. Mr. Berger has no recollection of post-it notes on this document or moving them to another document. The assistant was standing in the area by Ms. Smith's desk where the files were.

Next, Ms. Smith provided him all but two documents the White House had sent back from the documents he reviewed for EOP 2. [The White House sent those two documents on to the 9/11 Commission.] Ms. Smith told him the White House was taking a narrower view of the production than the Archives. They discussed that the White House had not produced sixty percent of what they deemed responsive. Ms. Smith asked Mr. Berger if he wanted to again go through the documents the White House sent back from his EOP 2 review. He was annoyed. Mr. Berger said "No, I do not need to go through them, I think they are all producible." "Resubmit them all, they are all relevant."

Case Number:
04-001-GC

Case Title:
Samuel R. Berger, et al.

Then they turned to the documents of the day. This time, the emails were organized. He recalled being handed the documents individually, not in a folder. About mid-day, Mr. Berger came across another version of the MAAR. In October, Mr. Berger saw a version of the MAAR and now had doubts that what he removed in September was the final report. At this point, he wanted to track the evolution of the MAAR. He slid the document under his portfolio.

Ms. Smith told Mr. Berger there was a missing document, one that she could not find. Mr. Berger said at this point "the bomb should have burst in the air, but obviously it did not." However, Mr. Berger did apprehend the consequences of what she said. Mr. Berger disassembled first, then he asked her if the document could have been misfiled. Ms. Smith said "No." Mr. Berger asked if they had not produced this document already. Ms. Smith said it was a different version.

Ms. Smith gave him another copy of the document. Mr. Berger slid this document under his portfolio also. Ms. Smith did not ask for it back. If she had asked for it back, it would have "triggered" a decision for him to give the documents back.

In total, he removed four documents, all versions of the MAAR. Mr. Berger does not recall if he placed all the documents on his person at once or at different times. He did not put the documents on his person until he was alone. He removed the notes, about fifteen pages, towards the end of the day.

Mr. Berger had a long day and wanted to go home around 6 p.m. Ms. Smith wanted him to finish the review and said they only had about an hours worth of work left. He understood she was getting pressure from the White House to provide a response so he agreed. Ms. Smith suggested he take a walk and come back and finish up. Mr. Berger left the building with all the documents he put in his pockets. He was aware of the risk he was taking, but he also knew the guards were not there in the evening.

Mr. Berger exited the Archives on to Pennsylvania Avenue, the north entrance. It was dark. He did not want to run the risk of bringing the documents back in the building risking the possibility Ms. Smith might notice something unusual. He headed towards a construction area on Ninth Street. Mr. Berger looked up and down the street, up into the windows of the Archives and the DOJ, and did not see anyone. He removed the documents from his pockets, folded the notes in a "V" shape and inserted the documents in the center. He walked inside the construction fence and slid the documents under a trailer.

Mr. Berger came back into the building without fearing the documents might slip out of his pockets or that Ms. Smith and her staff would notice that his pockets were bulging. He did not recall a security guard in the lobby.

If Mr. Berger had been aware Ms. Smith's staff was tracking the documents he was provided, he would not have removed them. He also said that if staff had escorted him out of the building for his walk, he would have felt less confident that no one was in the area and someone might be watching his actions.

Case Number: 04-001-GC	Case Title: Samuel R. Berger, et al.
---------------------------	---

Mr. Berger does not recall reviewing his notes or Mr. Naplan's notes on this visit.

It is possible that Gary Stern, NARA General Counsel, stopped by to introduce himself but Mr. Berger did not have a vivid memory of this.

Mr. Berger was trying to balance his review carefully but was also trying to be expeditious. He skipped meals and drank diet cokes. He did go to the restroom, possibly with documents in his pockets, but did not discard documents there or rearrange them on his person.

On this visit, Ms. Smith did not advise Mr. Berger that she was not leaving her office for him to take personal calls, as this was not protocol.

Ms. Smith did not tell Mr. Berger that she had numbered the documents or that she had a way of tracking these records. Mr. Berger said he would have "picked-up" on that comment. He said "I may be stupid, but I am not self destructive." As he left for the day between 7 and 7:30 p.m., Ms. Smith asked Mr. Berger in a matter of fact way "Is there anything you want to tell me?" He totally missed that signal later realizing it was her subtle way to ask him if he removed documents. Mr. Berger believed no one knew he removed documents.

Mr. Berger left the building, retrieved the documents and notes from the construction area, and returned to his office.

On **October 4, 2003**, late in the afternoon, Mr. Lindsey called Mr. Berger to tell him Mr. Stern called from the Archives. Mr. Berger was aware Mr. Stern was the General Counsel of the Archives. Mr. Stern said documents were missing after Mr. Berger's visit on October 2, 2003. Mr. Berger panicked because he realized he was caught. Mr. Berger lied to Mr. Lindsey telling him he did not take the documents.

Mr. Berger remembers next calling Ms. Smith at her office. He knew it was not a good sign she was there on a Saturday. She described the documents stating there were four copies of three documents missing. Mr. Berger asked her if the four documents they were missing were copies of the MAAR. He told Ms. Smith he would see if he accidentally took them. Mr. Berger was agitated because he realized he was caught.

Mr. Stern called Mr. Berger and said "I hope you can find them because if not, we have to refer this to the NSC's General Counsel." Mr. Stern did not say what would be done if Mr. Berger returned the documents. When asked again, Mr. Berger became unsure whether Mr. Stern or Mr. Lindsey said this to him. However, he was sure the source of the statement was Mr. Stern. Mr. Stern asked Mr. Berger to go to his office to see if he could find the documents.

Mr. Berger drove to his office late that afternoon. On the night of October 2, 2003, he had destroyed, cut into small pieces, three of the four documents. These were put in the trash. By Saturday, the trash had been picked-up. He tried to find the trash collector but had no luck. Neither Mr. Stern nor Ms. Smith offered to help him look through the trash.

Case Number: 04-001-GC	Case Title: Samuel R. Berger, et al.
---------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

About 7 p.m., Mr. Berger called Mr. Stern and said "I think I solved the mystery." Mr. Stern said he was going into a play and would call as soon as it was over. About 11:30 p.m., Mr. Stern called Mr. Berger. Mr. Berger told him, "I found two documents but not the other two." Mr. Stern told him to get the documents from his office and lock them in the safe in his home. Mr. Stern was glad he found two but three were still missing.

Mr. Berger did not recall Stephen Hannestad, unless he picked-up the documents.

On **October 5, 2003**, Mr. Berger recalled NARA staff picking up the two documents at his home. He understands that NARA staff recalled picking up the documents at his office. Mr. Berger was willing to accept that NARA staff came to his office.

There were additional conference calls. Ms. Smith was surprised when Mr. Berger returned the documents he removed in September. He knew he was caught, so he purported he must have removed the documents accidentally or inadvertently by sweeping them up with his documents. Later, Mr. Berger made a decision, on his own, to tell the truth. He said "I realized I was giving a benign explanation for what was not benign." Mr. Berger wanted to return everything he had taken. He realized he was returning documents he removed in September. He did not realize he returned more than they knew he removed. Mr. Berger was aware of the consequences but he knew returning the documents was the right thing to do.

Mr. Berger called Mr. Lindsey, told him what happened, and asked what he should do. Mr. Lindsey told Mr. Berger to get a lawyer. Mr. Berger and Mr. Lindsey did not discuss this issue any further as they were both lawyers and knew it was better not to talk about this.

Mr. Berger specifically recalled returning his notes to NARA staff at his home. He had flown in from New York, spent about an hour at his home, then flew back to New York to continue his travel. NARA staff never mentioned his notes. Mr. Berger believed if he had not returned them, they would never have known he removed his notes.

Mr. Berger does not know John Carlin, former Archivist of the United States, nor did he have any contact with him. Mr. Berger had not met Ms. Smith prior to these visits to the Archives. Additionally, he did not contact the NSC on this matter.

There were not any handwritten notes on the documents Mr. Berger removed from the Archives. Mr. Berger did not believe there was unique information in the three documents he destroyed. Mr. Berger never made any copies of these documents.

Mr. Berger said as a general point, he has dealt with classified information for twelve years. Some documents are sensitive and some are not super sensitive. This may not have anything to do with the documents classification. Other documents he reviewed had more sensitive information in them such as the Presidential Findings. He had seen most of the information in the MAAR disclosed in the press. He substituted his sense of sensitivity instead of thinking of classification. The MAAR did not involve sources and methods. It was a policy document.

Case Number: 04-001-GC	Case Title: Samuel R. Berger, et al.
---------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Some of the notes he removed did have information about the Presidential Findings. This was the authority from the President for actions to be taken.

Obtained via FOIA by Judicial Watch, Inc.

Ms. Smith had no reason to believe he was not acting in an appropriate manner. Mr. Berger said if there was always someone with him, he would not have taken any documents. After learning he was given special treatment by viewing the documents in Ms. Smith's office, he suggested no exceptions to the rules should be given to former National Security Advisors or others. The Archives should thoroughly check people when they enter and exit the building.

Mr. Berger received enough phone calls which gave him the opportunity to remove the documents. He never sent Ms. Smith out of the room for the sole purpose of removing the documents.

The DOJ asked Mr. Berger if he removed any other documents from the Archives that we were not aware of to which Mr. Berger replied no.

Case Number: 04-001-GC	Case Title: Samuel R. Berger, et al.
---------------------------	---



REPORT OF INVESTIGATION

Title (Name and address): Samuel R. Berger [redacted] b2		Type of Investigation: Criminal	Type of Report: <input checked="" type="checkbox"/> Final <input type="checkbox"/> Supplemental
Social Security Number: NA		<input type="checkbox"/> Employee	<input checked="" type="checkbox"/> Non-employee <input type="checkbox"/> Former Employee
Date of Birth: NA	Date Entered on Duty: NA	Position and Grade: NA	
Post of Duty: NA		Organization and Office: NA	
Period of Investigation: October 2003 to October 2005			

BASIS FOR INVESTIGATION

The Office of Investigations (OI), Office of Inspector General (OIG), received information that Samuel R. Berger, former National Security Advisor, removed classified documents from the National Archives and Records Administration (NARA), constituting a violation of criminal law. The investigation pertaining to Mr. Berger's actions was referred to the Department of Justice (DOJ) per the Inspector General (IG) Act (as amended) and 18 U.S.C. § 402a – Coordination of counterintelligence activities. The DOJ and Federal Bureau of Investigation (FBI), with the assistance of the OIG, conducted the criminal investigation involving Mr. Berger.

The NARA OI investigated and is reporting on the activities addressing NARA's responsibilities concerning Presidential records and Mr. Berger's access to those records.

ALLEGED VIOLATIONS

1. [redacted]
2. [redacted] b6, b7c
3. [redacted]

Distribution	No.	Case Number:	Signature of Special Agent Making Report:
Office of Inspector General	1	[redacted] b2	
National Archives and Records Administration	2	Signature of Person Examining Report:	
Assistant U.S. Attorney	1		
Other (Specify):		Title: Assistant Inspector General for Investigations	Office(City): College Park, MD
		Division Office: Headquarters	Date of Report: 11/4/05

OFFICIAL USE ONLY

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

- 4. [REDACTED]
 - 5. [REDACTED]
 - 6. [REDACTED]
- b6, b7C

RESULTS OF INVESTIGATION

The investigation substantiated that Mr. Berger unlawfully removed and retained classified documents from NARA. On September 8, 2005, Mr. Berger was sentenced to two years of probation, subsequent to pleading guilty to Unauthorized Removal and Retention of Classified Material, a misdemeanor. The court ordered a \$25.00 special assessment, a fine of \$50,000, 100 hours of community service, and no access to any classified material for 3 years.

This investigation substantiated that [REDACTED] facilitated access to [REDACTED] on at least five occasions. [REDACTED] documents were provided to Mr. Berger on four occasions. [REDACTED] documents were provided to [REDACTED], on one occasion.

b2, b5, b6, b7C

[REDACTED]

b2, b6, b7C

On September 2, 2003, there was a suspicion Mr. Berger may have removed classified material from the Archives. Neither [REDACTED] nor [REDACTED] reported this suspicion to any law enforcement entity. [REDACTED]

b6, b7C

On October 3, 2003, [REDACTED] verified Mr. Berger removed classified material from NARA. Neither [REDACTED] nor [REDACTED] reported this incident to any law enforcement entity before conducting an investigation of the incident.

b6, b7C

[REDACTED] conducted an investigation, including contacting the subject of the investigation, [REDACTED].

b6, b7C

Case Title: Samuel R. Berger [REDACTED] b2	Case Number: [REDACTED] b2
---	-------------------------------

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained Via FOIA by Judicial Watch, Inc.

[REDACTED] Archives employees contend Mr. Berger did not remove documents to disburse their contents and/or commit espionage. [REDACTED]

b2, b5, b6, b7C

INVESTIGATIVE SUMMARY

EXHIBIT

The Presidential Records Act (PRA) of 1978 and Executive Order 13233 govern the official records of Presidents and Vice Presidents created or received after January 20, 1981. Upon the conclusion of a President's term of office, or if a President serves consecutive terms upon the conclusion of the last term, the Archivist of the United States shall assume responsibility for the custody, control, and preservation of, and access to, the Presidential records of that President. The Archivist shall deposit all such Presidential records in a Presidential archival depository or another archival facility operated by the United States.

The William J. Clinton Presidential material was transferred to the legal custody of NARA at the end of President Clinton's administration. The [REDACTED] at NARA is responsible for Presidential records. [REDACTED]

b6, b7C

[REDACTED]. The majority of the Clinton Presidential records were sent to the Clinton Project [now the William J. Clinton Presidential Library] in Little Rock, AR. [REDACTED]

b2, b5

[REDACTED]. These documents designated as the "W" intelligence files, contain classified information [REDACTED] material.

On April 12, 2002, President Clinton signed a letter designating Mr. Berger and [REDACTED] as agents on his behalf to review relevant NSC documents regarding Osama Bin Laden/Al Qaeda, Sudan, and Presidential correspondence from or to Omar Bashir, contained in the Clinton Presidential records. This request was made to facilitate Mr. Berger's testimony to the Joint Intelligence Committee (Graham-Goss Commission). This request was forwarded by [REDACTED], [REDACTED] in a letter dated April 15, 2002.

b6, b7C

The NSC's [REDACTED] sent a letter to [REDACTED], dated May 14, 2002, designating the guidelines for access to these highly sensitive records. The letter stated Mr. Berger was the only person from the Clinton administration who had been designated and had all clearances required for access

b6, b7C

Case Title: Samuel R. Berger [REDACTED] b2 Case Number: [REDACTED] b2

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

to the most sensitive "W" files. [redacted] said [redacted] repeatedly briefed Mr. Berger that he was not allowed to remove any documentation from NARA. The letter also stated notes may be taken but must be retained by NARA staff and forwarded to the NSC for a classification review and appropriate marking. [redacted] said the NSC told [redacted] Mr. Berger was made aware of this requirement.

b6, b7C

[redacted]

b2, b5

On May 30, 2002, Mr. Berger reviewed Clinton Presidential materials at Archives I (Washington, DC) for the purpose of preparing his testimony to the Graham-Goss Commission. Additionally, in response to requests from the National Commission on Terrorist Attacks Upon the United States (hereinafter the 9/11 Commission), Mr. Berger conducted a constitutional Presidential Privilege review of Clinton Presidential materials at Archives I on three occasions: July, September, and October 2003. On all of these visits, Mr. Berger reviewed documents including [redacted] material.

b2, b6, b7C

Under the PRA the Congressional committee agreed the incumbent President would request the records and turn them over to the 9/11 Commission. This was facilitated through Executive Office of the President (EOP) requests. According to [redacted], the established protocol was for NARA to conduct a review, at Archives I and at the Clinton Project, and determine which Clinton Presidential records were responsive to the EOP requests, with [redacted] making the final call on responsiveness for NARA. Clinton representatives reviewed the documents for privilege and discussed responsiveness with [redacted]. After the reviews, copies were sent to the NSC for the representative of the incumbent President to review before forwarding to the 9/11 Commission.

b2, b6, b7C

On all four visits to Archives I, Mr. Berger signed in as a visitor and was escorted to [redacted] office, room [redacted], where he conducted his review of documents including [redacted] material. Mr. Berger was allowed to bring personal items into the room including his portfolio and cell phone. [redacted]

b2, b6, b7C

[redacted]

pursuant to DCID 6/9: Physical Security

Case Title: Samuel R. Berger [redacted] b2

Case Number: [redacted] b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General National Archives and Records Administration

OFFICIAL USE ONLY

Standards for Sensitive Compartmented Information Facilities, Section 2.3.2.

[REDACTED]

b2, b6, b7C

Some NARA employees believed room [REDACTED] was "cleared" as it contained [REDACTED]

[REDACTED] acknowledged [REDACTED] received a [REDACTED] classified document from Little Rock, AR, [REDACTED], in response to an EOP request.

b2, b5, b6, b7C

[REDACTED]. According to NARA documentation, [REDACTED] since about 1993. During this investigation, this [REDACTED].

The Director of the CIA is the overall authority [REDACTED]. [REDACTED] material is governed by the DCIDs. According to CIA officials, NARA can make agency specific regulations requiring additional security measures as long as they exceed the requirements of the DCIDs. [REDACTED]

b2, b6, b7C

[REDACTED] CIA Office of Security, advised that the CIA Director delegates their authority to the Senior Official of the Intelligence Community (SOIC). While some agencies have a designated SOIC, NARA does not. Therefore, NARA falls under the Director of Security, CIA, SOIC. Waivers to DCIDs have to be signed by the SOIC.

On May 30, 2002, Mr. Berger was provided original NSC numbered documents and original Staff Member Office Files (SMOFs). [REDACTED] indicated Mr. Berger did not have many questions for [REDACTED] as this review was in preparation for his testimony. [REDACTED] said Mr. Berger left his notes at NARA, and requested these notes be sent to the NSC for classification review.

b2, b6, b7C

On July 18, 2003, Mr. Berger was provided original NSC numbered documents and original SMOFs. [REDACTED] and Mr. Berger were sitting at the table in [REDACTED] office going over the documents during most of this visit. They were discussing responsiveness to the EOP2 request. Mr. Berger said he took several phone calls on this visit where [REDACTED] stepped out of [REDACTED] office.

b2, b6, b7C

Mr. Berger said he realized he was not going to be able to reconstruct in detail all the documents he had reviewed, so he needed to take his notes with him, about ten to

b2, b6, b7C

Case Title: Samuel R. Berger [REDACTED] b2

Case Number: [REDACTED] b2

OFFICIAL USE ONLY

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

twenty pages. Mr. Berger said at the end of the day, he folded his notes and put them in his suit pocket. Mr. Berger said he took the opportunity to do this when [redacted] was out of [redacted] office.

b6, b7C

[redacted] came to Archives I in July 2003 to assist Mr. Berger by reviewing Presidential records sent to Archives I from the Clinton Project in response to EOP2. [redacted] visit was separate from Mr. Berger's visit in July. [redacted] verified [redacted] reviewed documents classified to the [redacted] in [redacted] office.

b2, b6, b7C

[redacted] said Mr. Berger's handling of the documents on July 18, 2003, caused archival concerns in maintaining provenance. [redacted] said [redacted] and Mr. Berger [redacted] and Mr. Berger would pull out other documents. [redacted], therefore the documents became disorganized. [redacted] said Mr. Berger requested that on his next visit he preferred to see the documents in chronological order. [redacted] suggested to the [redacted] that on Mr. Berger's next visit they provide him with copies to allow for placement of the documents in chronological order.

b2, b6, b7C

On September 2, 2003, Mr. Berger was provided original NSC numbered documents and copies of SMOFs for review in response to EOP3. [redacted] said Mr. Berger was also provided a document faxed from the Clinton Project to Archives I on July 22, 2003.

b2, b6, b7C

[redacted] said [redacted] did not spend as much direct time with Mr. Berger as [redacted] had on the previous visit. According to [redacted], during this visit, Mr. Berger asked [redacted] to leave [redacted] office several times so he could talk privately on the phone. [redacted] said [redacted] left as [redacted] trusted Mr. Berger and was aware that Mr. Berger, as National Security Advisor, had generated most of the documents [redacted] was reviewing. However, [redacted] said [redacted] did not like leaving [redacted] office because [redacted] works with sensitive items [redacted] and did not feel comfortable leaving Mr. Berger alone with this material. [redacted] said [redacted] knew of no statutory authority that allowed [redacted] to refuse to leave the room.

b2, b5, b6, b7C

Mr. Berger said he would say: "Sorry, I have to make a private phone call," and [redacted] would take this as [redacted] cue to leave. Mr. Berger said he told [redacted] he was happy to go outside [redacted] office to take the calls. Mr. Berger said instead [redacted] offered to leave [redacted] office while he was on the phone. Mr. Berger said once this pattern was established, he thought the offer for [redacted] to leave [redacted] office was "standing." [redacted] denied there was any such agreement.

b2, b6, b7C

Case Title: Samuel R. Berger [redacted] b2

Case Number: [redacted] b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General

National Archives and Records Administration

OFFICIAL USE ONLY

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

asked staff member to buy a soda for Mr. Berger. said Mr. Berger stepped out of office, out of the suite, and into the hallway headed for the men's room. said came out of the suite and had to "side step" Mr. Berger. said saw Mr. Berger bent down, fiddling with something white, which could have been paper, around his ankle. said continued to the basement to buy the soda. said attempted to call but could not recall extension. said returned to the suite and asked to step out. said briefly explained to what had witnessed. According to, asked to write the information down. said sent an email to, before Mr. Berger left for the day.

b2, b6, b7C

said read the email. According to, when Mr. Berger stepped out to the men's room, discussed with if was sure enough of what saw to confront Mr. Berger. said that did not believe there was enough information to confront someone of Mr. Berger's stature. said did not mention the email to or discuss this matter until after Mr. Berger left.

b2, b5, b6, b7C

Mr. Berger said he took the first opportunity when was out of office to remove a document (a facsimile sent from in July). He said he folded the notes and put them in his pocket at the end of the day. Mr. Berger denied removing any documents in his socks. He stated his shoes frequently come untied and his socks frequently fall down.

b2, b6, b7C

On either September 2, 2003, or September 3, 2003, contacted, and advised of what occurred. According to, said "we have a problem." said said was worried Mr. Berger might be taking documents out of Archives I and that and staff were going to watch Mr. Berger closely on his next visit. When asked, said did not make these statements to

b2, b6, b7C

stated mentioned the incident to supervisor, nor provided further guidance to. said does not recall having a conversation with about this incident in preparation for Mr. Berger's visit on October 2, 2003. However, stated approved a more aggressive action to be taken by and the when Mr. Berger returned but did not give specific direction.

b2, b6, b7C

Case Title: Samuel R. Berger b2 Case Number: b2

OFFICIAL USE ONLY

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

On September 4, 5, and 8, 2003, [redacted], formerly of President Clinton's National Security staff, reviewed classified documents responsive to EOP3 [redacted]. [redacted] said [redacted] inquired as to why [redacted] was not allowed to conduct the review in [redacted] office. [redacted] said [redacted] advised [redacted] [redacted] had other matters to attend to and that [redacted] staff would assist him.

b2, b6, b7C

Next, [redacted] prepared for Mr. Berger's return. According to [redacted], the incident on September 2, 2003, in which [redacted] thought [redacted] witnessed Mr. Berger with something in his sock was in [redacted] thoughts as [redacted] prepared for Mr. Berger's next visit. [redacted] said they decided to hand number the documents provided to Mr. Berger on the back of each document as a means of controlling the documents. [redacted] said they numbered documents to feel secure that Mr. Berger was not removing documents. [redacted] said they numbered these documents themselves, without consultation with NARA General Counsel, Security, management, the OIG, or law enforcement. However, [redacted] said [redacted] told [redacted] of their intention to number the documents (by September 28th at the latest). [redacted] said [redacted] thought it was a good idea.

b2, b6, b7C

Mr. Berger next came to Archives I on October 2, 2003. He reviewed copies of NSC numbered documents, copies of SMOFs, and hard copies of emails, including those which [redacted] had reviewed, in response to EOP3. [redacted] said [redacted] told Mr. Berger [redacted] was not leaving [redacted] office for him to take private calls. [redacted] said [redacted] was working at [redacted] desk while Mr. Berger reviewed the documents. [redacted] also recounted that Mr. Berger made numerous visits to the men's room.

b2, b6, b7C

[redacted] said on this visit Mr. Berger was provided one file folder of documents at a time. Once Mr. Berger finished reviewing a file folder, [redacted] said they reviewed the hand numbering to ensure all the documents were returned. [redacted] said in the afternoon [redacted] was returning a file folder to a [redacted] member during one of Mr. Berger's many visit's to the men's room. The [redacted] member said they discovered a numbered document (#217) was missing from a file folder Mr. Berger had reviewed. [redacted] said they printed another copy of the document which was missing. [redacted] said [redacted] gave this second copy (#217) to Mr. Berger. [redacted] said [redacted] told Mr. Berger [redacted] had a way of "legally controlling" the emails. [redacted] said [redacted] emphasized to Mr. Berger that the document was numbered and apparently when he was provided the emails he had not been provided this one. [redacted] said Mr. Berger indicated he was sure he had seen this email and asked [redacted] if [redacted] remembered seeing this email. [redacted] said [redacted] told Mr. Berger [redacted] had seen similar information but that this unique email number was missing.

b2, b6, b7C

Mr. Berger said he saw a version of the Millennium Alert After Action Review

Case Title: Samuel R. Berger [redacted] b2

Case Number: [redacted] b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General

National Archives and Records Administration

OFFICIAL USE ONLY

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

(MAAAR) and now had doubts that what he removed from Archives I in September was the final report. He said at this point, he wanted to track the evolution of the MAAAR. Mr. Berger said he slid the document (#217) under his portfolio.

b2, b6, b7C

Mr. Berger said that when [redacted] told him there was a missing document "the bomb should have burst in the air, but obviously it did not." Mr. Berger said when [redacted] gave him another copy of the document (#217), he slid this document under his portfolio also. Mr. Berger said [redacted] did not ask for it back. Mr. Berger said if [redacted] had asked for the document back, it would have "triggered" a decision for him to give the documents back.

b2, b6, b7C

According to [redacted], about five minutes later, Mr. Berger told [redacted] he had to make a private phone call and [redacted] had to leave [redacted] office. [redacted] said [redacted] was uncomfortable with this request but left [redacted] office. [redacted] said [redacted] stepped over to the desk outside [redacted] office that had a phone on it with [redacted] line accessible. [redacted] said [redacted] noticed [redacted] phone line was not lit. According to [redacted], [redacted] opened [redacted] office door at which point Mr. Berger "mowed" [redacted] down on the way to the men's room, a location from which he had recently returned.

b2, b6, b7C

Later that evening, Mr. Berger took a break to go outside. No one escorted him out of Archives I. In total, during this visit he removed four documents, all versions of the MAAAR. Mr. Berger said he left the building with all four documents (#150, #323, and two copies of #217) in his pockets.

b2, b6, b7C

[redacted] Mr. Berger said if [redacted] had escorted him out of the building, he would have felt less confident that no one was in the area and more concerned someone might be watching his actions.

Mr. Berger said he did not want to take the risk of bringing the documents back in the building and the possibility [redacted] might notice something unusual. Mr. Berger said he placed the documents under a trailer in an accessible construction area outside Archives I. He returned to [redacted] office to finish his review. He said he removed the notes, about fifteen pages, near the end of the day. Mr. Berger said he then left Archives I, retrieved the documents from the construction area, and returned to his office.

b2, b6, b7C

[redacted] was working on other projects, therefore, all the documents were not checked before Mr. Berger left. Also, the folders were only given to staff when Mr. Berger went to the men's room. After Mr. Berger left, [redacted] said [redacted] and [redacted] returned the documents [redacted]. [redacted] said the folders were not checked at this time to determine if any additional hand numbered documents were missing as it was late, other staff had already left for the day, and they had no reason

b2, b6, b7C

Case Title: Samuel R. Berger [redacted] b2

Case Number: [redacted] b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General National Archives and Records Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained Via FOIA by Judicial Watch, Inc.

to believe Mr. Berger removed documents. At that time, [redacted] said they believed the email (#217) might not have been provided to Mr. Berger initially.

The first thing the next morning, Friday, October 3, 2003, the [redacted] said they began verifying that all documents provided to Mr. Berger on October 2, 2003, were present. [redacted] stated four numbered, classified, emails were missing from those provided to Mr. Berger on October 2, 2003. According to [redacted], all the missing documents had the MAAAR as an attachment.

b2, b6, b7C

[redacted]

b2, b6, b7C

Upon discovery that classified documents were missing, [redacted] contacted [redacted] as [redacted] supervisor, [redacted] was on travel. [redacted] had also been working with the [redacted] on the production of the EOP requests. [redacted] traveled to Archives I where [redacted] and [redacted] discussed what action should be taken. [redacted] said [redacted] stated the normal reporting process would be notification of the NSC as the equity holder and [redacted] may have raised the issue of who in the agency should be notified, mentioning the Archivist of the United States, NARA security, and the Inspector General. [redacted] said [redacted] called [redacted] to report the matter and seek guidance on how to proceed but [redacted] was on travel. [redacted] said [redacted] asked [redacted] if [redacted] contacted [redacted] boss, [redacted]. [redacted] said [redacted] told [redacted] had tried but [redacted] was not available.

b2, b6, b7C

The next day, Saturday, October 4, 2003, [redacted] said [redacted] talked with [redacted] who asked that [redacted] and [redacted] come up with a plan to handle this matter and report back to [redacted]. [redacted] said [redacted] received a call from [redacted] asking [redacted] to contact [redacted]. [redacted] said they were treating this incident as an unauthorized removal of classified documents, a breach of National Security Information. According to [redacted], it was [redacted] job to handle security violations. [redacted] said [redacted] was acting at [redacted] direction and if [redacted] had asked [redacted] to work with the OIG [redacted] would have. [redacted] stated NARA personnel conducted an inquiry per the NARA ISM.

b2, b6, b7C

[redacted] stated [redacted] led the investigation [redacted] expanded that [redacted]

b2, b6, b7C

Case Title: Samuel R. Berger [redacted]
NARA - OIG Form OI 212 (Rev 04/2005)

b2

Case Number: [redacted]

b2

Office of Inspector General
National Archives and Records Administration

OFFICIAL USE ONLY

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

was on [redacted] leadership team, [redacted] had expertise in Archives' matters, and [redacted] was the [redacted]. [redacted] said [redacted] was told Mr. Berger removed only copies of documents. [redacted] said this did not effect [redacted] belief this was a serious matter.

b6, b7C

[redacted] said [redacted] told [redacted] [redacted] asked [redacted] to head up this investigation. It was clear to [redacted] and [redacted] that [redacted] was not in charge.

b2, b6, b7C

[redacted] considered [redacted] to be in charge of the incident even though [redacted] was a [redacted] and [redacted] was [redacted]. [redacted] believed [redacted] was only in charge until [redacted] was briefed. [redacted] said that [redacted], [redacted], and [redacted] all provided input on how to proceed.

b2, b6, b7C

[redacted] said [redacted] stated [redacted] was stepping away from the decision making in this matter. [redacted] said [redacted] kept the lead and decisions on this matter separate from [redacted] because [redacted] was a [redacted]. [redacted] said [redacted] made this clear to [redacted] and [redacted]; and they indicated they agreed with [redacted] decision. [redacted] believed this was clear to [redacted] because [redacted] never said [redacted] had to run their ideas by [redacted]. [redacted] said, in [redacted] view, [redacted] was leading the inquiry [redacted].

b2, b6, b7C

[redacted] said [redacted] considered this incident to be a potential crime and the unauthorized removal of classified documents should be reported to the FBI. [redacted] said [redacted] believed the FBI might want to look into this matter due to the level of classified materials involved. [redacted] said either [redacted] or [redacted] suggested the FBI be contacted. However, [redacted] said [redacted] never contacted the FBI and could not explain why the FBI was never contacted. [redacted] said [redacted] recalled [redacted] mentioning something about the FBI. [redacted] said [redacted] did not recall anyone mentioning contacting the FBI.

b2, b6, b7C

That afternoon, [redacted], [redacted], and [redacted] met at Archives I. [redacted] said [redacted] advised them the normal procedures were to recover the documents as quickly as possible and to report the incident to the equity holder. [redacted], [redacted], and [redacted] decided to contact Mr. Berger and ask [redacted] to return the documents. [redacted] said they ran the idea of calling Mr. Berger by [redacted] and [redacted] authorized the contact. [redacted] said [redacted] indicated [redacted] just wanted to do what was right and deferred to [redacted]. [redacted] said while [redacted] was not in charge, [redacted] wanted to be informed on how this matter was proceeding.

b2, b6, b7C

[redacted] said

Case Title: Samuel R. Berger [redacted] b2 Case Number: [redacted] b2

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

they decided to contact [redacted] as Mr. Berger would be more responsive to [redacted]. [redacted] said [redacted], and [redacted] called [redacted], on speaker phone, and told [redacted] copies of emails were missing from the material Mr. Berger reviewed. They asked [redacted] to call Mr. Berger. [redacted] said at some point during the day, they explained how they had numbered the documents and now they were missing. [redacted] said they told [redacted] if Mr. Berger took the documents by mistake then gave them back it would be reported as an inadvertent removal. [redacted] said it was clear to [redacted] NARA intended on reporting this incident regardless.

[redacted]
b2, b6, b7C

[redacted] said [redacted] called Mr. Berger who told [redacted] that he did not think he had any documents. [redacted] said [redacted] called [redacted] (others were possibly on the line) and told [redacted] Mr. Berger's response. [redacted] said [redacted] was instructed to ask Mr. Berger a specific question. [redacted] said [redacted] suggested they contact Mr. Berger directly as asking a question through [redacted] was not efficient.

b2, b6, b7C
[redacted]

[redacted] said [redacted] called Mr. Berger and advised him NARA was treating this matter as a security infraction and [redacted] was going to report this to the NSC. According to [redacted], Mr. Berger said they were mistaken and that he gave the documents back to [redacted] assistant. [redacted] said they asked Mr. Berger to see if he could find any documents.

b2, b6, b7C
[redacted]

That evening, after [redacted] left Archives I, [redacted] said [redacted] took a call from Mr. Berger. According to [redacted], Mr. Berger asked if one of the misplaced emails was the one [redacted] had mentioned was missing and had given to him individually; and if the document that was missing contained information that was in several emails. [redacted] confirmed all the emails that were missing contained similar information.

b2, b6, b7C
[redacted]

[redacted] said around 8:00 p.m., Mr. Berger called [redacted] cell phone and asked if [redacted] could talk, as he wanted to explain something. [redacted] said [redacted] was at [redacted] and could not speak then but agreed to call him later that night.

b2, b6, b7C
[redacted]

Near midnight, [redacted] called Mr. Berger who said he found two documents. [redacted] advised Mr. Berger NARA would make arrangements to pick the documents up in the morning.

b2, b6, b7C
[redacted]

On Sunday, October 5, 2003, [redacted] said [redacted] informed [redacted] of the developments and [redacted] recommended [redacted] ask Mr. Berger to search his office again. [redacted] said [redacted] called Mr. Berger and asked him to search his office. [redacted] said Mr. Berger called back to say he was unable to locate any additional documents and it was possible that documents could have been disposed of in his

b2, b6, b7C
[redacted]

Case Title: Samuel R. Berger [redacted] b2 Case Number: [redacted] b2

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO THE OFFICE OF INSPECTOR GENERAL, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

office trash. [redacted] said [redacted] recommended to Mr. Berger he search his trash.

Later that morning, [redacted] and [redacted] picked-up documents from Mr. Berger. [redacted] said one document was an email which they had numbered by hand (#323) and the other was a facsimile of a textual document sent [redacted]. [redacted] identified the document from [redacted] as one Mr. Berger would have reviewed on September 2, 2003, not October 2, 2003, as thought. [redacted] said this was another copy of the MAAAR. [redacted] said they realized the implications that Mr. Berger took copies of documents on two separate visits (September 2, 2003 and October 2, 2003) and that the missing items all included the MAAAR.

b2, b6, b7C

[redacted] said that afternoon [redacted] and [redacted] called [redacted] and told [redacted] what Mr. Berger had provided and the significance of the dates Mr. Berger reviewed the documents. [redacted] said [redacted] told [redacted] had to talk to Mr. Berger. [redacted] said [redacted] and [redacted] spoke with Mr. Berger to explain that one of the documents he returned was from his visit on September 2, 2003, and that documents removed on October 2, 2003, were still missing.

b2, b6, b7C

According to [redacted], later that day, [redacted] called and told [redacted] Mr. Berger called [redacted] and said he [Mr. Berger] may have been incorrect and took the textual document on September 2, 2003.

b2, b6, b7C

[redacted] said that evening, after talking with [redacted] and [redacted], a decision was made to contact the NSC. [redacted] said later that evening [redacted] spoke with the NSC's [redacted]. [redacted] gave him a short briefing and they set up a meeting for Monday, October 6, 2003. [redacted] said [redacted] also called [redacted], and gave [redacted] a short briefing and asked [redacted] to inform [redacted].

b2, b5, b6, b7C

According to [redacted], on October 6, 2003, the NSC's [redacted] met with [redacted] and [redacted] and advised [redacted] should formally report this to [redacted]. [redacted] said on October 6, 2003, [redacted] briefed [redacted]. [redacted] said that on October 6, 2003, [redacted] removed [redacted] by delegating [redacted] to handle this matter.

b2, b6, b7C

[redacted] said [redacted] recounted what [redacted] knew of the matter and stressed that [redacted] wanted [redacted] to manage the situation so that [redacted] was not directly involved. [redacted] said [redacted] asked [redacted] to review NARA policies to ensure this did not happen again. [redacted] said [redacted] was now in charge of an issue [redacted] saw as two fold. One issue being the change in procedures that was required concerning

b2, b6, b7C

Case Title: Samuel R. Berger [redacted] b2

Case Number: [redacted] b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General National Archives and Records Administration

OFFICIAL USE ONLY

REPORT OF INVESTIGATION
Obtained Via FOIA by Judicial Watch, Inc.

the prevention of such an incident in the future. The other issue was the leak of national security information.

█ stated █ believed it was NARA's responsibility to recover the documents and report to the NSC. █ said on October 7, 2003, █ and █ met with NSC officials. █ said █ assumed once they reported this to the NSC that the NSC would take over the investigation.

█
b2, b5, b6, b7C

█
█

and █ said the NSC wanted to ensure all documents responsive to EOP3 were provided to the White House so the NSC could then assure the 9/11 Commission that all documents were provided. █ said NARA had to be sure that no responsive records were removed by Mr. Berger and therefore not provided to the NSC.

█ said the █ reconstructed computer searches for the NSC numbered documents and SMOF files; and were confident to the best of their ability that all documents deemed responsive to EOP3 were provided to the White House. █ said █ informed the White House that NARA was not able to reconstruct the responsive documents for EOP2, as Mr. Berger was provided original documents. █ said █ would never know what if any original documents were missing from Mr. Berger's visits on May 30, 2002, and July 18, 2003.

b2, b6, b7C

The OI, with assistance from █, reviewed the documents Mr. Berger reviewed in an attempt to identify if it could be determined if additional documents were missing. It was not apparent that Mr. Berger removed an entire NSC numbered package or a SMOF file folder, however, the contents of these documents could not be verified. Due to complications, the emails Mr. Berger reviewed could not be readily reconstructed.

b2, b6, b7C

█ said on October 8, 2003, █ reported to █ what had transpired at the meeting with the NSC. █ stated the █ said █ then conducted a careful review of the statutes. █ said █ wanted to consult with other senior NARA officials to get their sense of the matter as they have knowledge, wisdom, and input on what to do in these matters. █ said a meeting of these officials could not be facilitated until October 10, 2003.

b2, b5, b6, b7C

Case Title: Samuel R. Berger █ b2	Case Number: █ b2
-----------------------------------	-------------------

NARA - OIG Form OI 212 (Rev 04/2005) Office of Inspector General National Archives and Records Administration

OFFICIAL USE ONLY

REPORT OF INVESTIGATION

Obtained via FOIA by Judicial Watch, Inc.

██████████ said on October 10, 2003, ██████████ met with ██████████, ██████████, ██████████, and ██████████, ██████████ said ██████████ shared potentially applicable statutes and executive orders at this meeting. ██████████ said at this meeting they concurred this could be a criminal matter and decided to report this to the OIG instead of going directly to the DOJ.

b2, b6, b7C

The Inspector General (IG) was briefed on this matter on Friday, October 10, 2003. This same date, OI investigators along with ██████████, retrieved documents from Mr. Berger, at his residence, at the request of Mr. Berger's attorney. ██████████ said the documents appeared to be Mr. Berger's hand written notes. These documents were secured ██████████.

b2, b6, b7C

██████████ was on travel over the holiday weekend. On Tuesday, October 14, 2003, the OI gathered information. On this date, an attorney representing ██████████ contacted NARA stating ██████████ had documents to turn over to NARA. These documents, notes taken concerning documents reviewed, were received by the OI and ██████████ and secured ██████████.

b2, b6, b7C

On October 15 and 16, 2003, the IG briefed DOJ attorneys and the FBI on this matter. The DOJ accepted the criminal referral concerning Mr. Berger's actions. The FBI requested the OI stop all interviews of cleared ██████████ and any NARA employees with knowledge of the incident involving Mr. Berger. The OI obliged and at their request assisted the FBI in collecting evidence for the criminal investigation.

b6, b7C

On April 9, 2004, NARA's IG and the DOJ's IG met with the Assistant Attorney General, Criminal Division, and the DOJ attorneys to discuss reporting this matter to the 9/11 Commission. A decision was made that the DOJ would notify the 9/11 Commission.

On April 14, 2004, DOJ officials advised the OI they could conduct an investigation of NARA procedures as they related to Mr. Berger's visits, with requested limitations.

On April 1, 2005, Mr. Berger pled guilty to Unauthorized Removal and Retention of Classified Material. On September 8, 2005, Mr. Berger was sentenced to two years of probation, subsequent to pleading guilty. The Court ordered a \$25.00 special assessment, a fine of \$50,000, 100 hours of community service, and no access to any classified material for 3 years.

Case Title:
Samuel R. Berger ██████████

b2

Case Number:

b2

NARA - OIG Form OI 212 (Rev 04/2005)

Office of Inspector General
National Archives and Records Administration

OFFICIAL USE ONLY

Exhibit Number	Description
1	Interviews of [REDACTED] b6, b7C
2	Memo to clarify discrepancies in the preparation for review of documents
3	Interview of [REDACTED] b2
4	Director of Central Intelligence Directive 6/9
5	Interview of [REDACTED] b6, b7C
6	[REDACTED] b2
7	Interview of Samuel Berger, dated July 8, 2005
8	Interview of [REDACTED] b6, b7C
9	[REDACTED], dated September 2, 2003 b6, b7C
10	Interview of [REDACTED] b6, b7C
11	Interview of [REDACTED] b6, b7C
12	Interview of [REDACTED] b6, b7C
13	Interview of [REDACTED] b6, b7C
14	[REDACTED] b2
15	Interview of [REDACTED] b6, b7C
16	Interview of [REDACTED] b6, b7C
17	Memorandum of Verification, dated June 2005

Case Number: [REDACTED] b2	Case Title: Samuel R. Berger [REDACTED] b2
----------------------------	--

EXHIBIT #1

NOTE TO FOIA REQUESTERS

Exhibit #1 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(1)

MEMORANDUM OF INTERVIEW OR ACTIVITY

Type of Activity: <input checked="" type="checkbox"/> Personal Interview <input type="checkbox"/> Telephone Interview <input type="checkbox"/> Records Review <input type="checkbox"/> Other	Date and Time: May 31 – June 2, 2005
[REDACTED] b6, b7C [REDACTED] [REDACTED] - to clarify discrepancies in the preparation for review of documents by Sandy Berger	Conducted by: [REDACTED] b6, b7C Location of Interview/Activity: Archives I, Washington, DC

Subject Matter/Remarks

[REDACTED] were interviewed together to get a complete understanding of how the documents were identified, pulled and prepared for review by Samuel R. Berger. This information was gathered after final interviews of [REDACTED]. Therefore, this information is deemed more accurate. The following information was deemed unclassified by the National Security Council. b6, b7C

The Clinton Presidential "W" files consisted of [REDACTED] federal record center boxes (another one was added sometime after October 2, 2003.) The materials in these boxes were either National Security Council (NSC) numbered documents or Staff Member Office Files (SMOFs), which were segregated. A box usually belonged to one person or a directorate. [REDACTED] b2, b6, b7C

[REDACTED] These were the only files contained in the boxes with the exception of "overflow" files that came over from the administration as they were cleaning areas after the change of administrations. These files would be filled in folders but did not belong to an individual. [REDACTED]

The requested materials for all of Mr. Berger's reviews were narrowed by date, nothing prior to 1998, and subject matter, the Middle East. The best [REDACTED] could estimate, since [REDACTED] was not involved in the May 2002 search for materials, was that about [REDACTED] boxes from the universe of "W" files were searched. Of those, about one third were NSC numbered documents and the other two thirds were SMOFs. b2, b6, b7C

Mr. Berger was provided [REDACTED] material on all his visits to NARA. b2

Case Number: [REDACTED] b2	Case Title: Samuel R. Berger [REDACTED] b2
--	--

ENCLOSURE(2)

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

The [redacted] is an electronic system used during the Clinton administration by the NSC to manage their records. The [redacted] was used as a finding aid as it indexed NSC numbered documents. The White House transferred data from the [redacted] system to NARA, via a flat file. NARA put this data on a Window based system.

b2

Basic information, an overview or brief synopsis of the document, was entered into [redacted] and assigned a seven-digit number. A search engine was used and a key word search was performed on the system in response to EOP 2. A list of search terms was not provided to [redacted] was allowed to and ran searches and received hits in preparation for this visit. [redacted] printed the abstract and provided this information to [redacted]. The numbered documents had a cover sheet with the document number; however, one document may contain several pages. [redacted] searched [redacted] index for documents responsive to EOP 2. The NSC numbered documents were located at [redacted]. The system does not identify which documents are at which location. [redacted] system only allows the index sheet to be marked as [redacted]. All the NSC numbered documents may not be available. Some may have been destroyed while others might be misfiled. Twenty to thirty percent of the time, NSC numbered documents were not found where they were supposed to be.

b2, b6, b7C

[redacted] dealt mostly with NSC numbered documents. NSC numbered documents may have been printed on heavy paper stock, [redacted]. Copies of NSC numbered documents could be recognized as all were copied on 8" by 11" paper and were in black and white.

b2, b6, b7C

The NSC numbered documents have a cover sheet. Normally the first page is printed on bond paper. The classification is usually stamped in red ink. [redacted]

b2

Because these documents were numbered, someone could determine if a numbered document was missing. However, there could be several pages of one NSC numbered document and the pages may or may not have been individually numbered in consecutive order. Emails could also be included in the document. The NSC referred to one NSC numbered document as a package. Finalized NSC packages reflected a watermark.

b6, b7C

The NSC numbered documents were numbered on their face, but individual pages were not numbered. All NSC numbered documents have a cover sheet and are bound in some manner, either by staple, binder clip or appropriate means. [redacted] staff removed the staples or binding and made photocopies for the production to the White House. Any loose paper pieces would probably be gone. They were not bound together upon return to the box.

Staff Member Office Files (SMOFs) contained the papers an individual filed in a particular folder. This could include draft NSC numbered documents, memos, emails, notes, etc. Some of these documents were copies of the originals. Archivists consider everything in a SMOF folder to be an original as it was sent for preservation. It is not a copy until an archivist makes a copy.

The NSC also sent over electronic files to include an electronic email system that included unclassified [redacted] emails. These are not designated as the "W" files. [redacted]

b2

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

[Redacted]

[Redacted] was the primary reviewer of the emails. NARA had received an email system at the end of the Clinton administration. This system, known as [Redacted] contained emails the NSC designated as "records." [Redacted]

b2, b6, b7C

[Redacted] printed and prepared the emails responsive to EOP 3. EOP3 had two paragraphs explaining what emails the 9/11 commission was requesting. They were emails from Mr. Berger to the Transnational Threats Staff ([Redacted]) and the converse. They determined Mr. Berger and [Redacted] did not always directly handle their email so they queried about eight people on their staff. [Redacted] recalled the search was done by name and subject fields. NARA consulted with the White House on the search string(s) (words) they were using to query the current administrations emails and tried to use the same ones.

b6, b7C

Once [Redacted] received "hits," [Redacted] reviewed the emails to determine if they were relevant to the request. [Redacted] gave an example that an email might come up on the search having to do with Spain which would not have been responsive, so [Redacted] would not have printed that email even though it came up in the initial search (terrorism). Once [Redacted] believed the email was relevant, [Redacted] printed a copy and wrote the file name [a number] on the back of each relevant email, in pen. The emails were grouped by classification then chronologically. This was done so the email could be segregated which would allow other reviewers with different security clearances to review the appropriate classified documents (i.e. [Redacted]).

b6, b7C

The documents for Mr. Berger's review were moved [Redacted] to [Redacted] office in Federal Records Center boxes. They were transported on a cart normally by two cleared individuals. This was done primarily to facilitate the cart being moved through the facility and over door jams. The boxes either had no descriptive words on them or if they did, the wording was covered with a clean sheet of paper. [Redacted] believed if they covered the material in a closed box this was sufficient for transport in a government facility. [Redacted] commented that classified information could be moved from one secure container to another secure container.

b2, b6, b7C

Mr. Berger's review in May 2002

The materials pulled for Mr. Berger's visit in May 2002 were kept segregated in case he wanted to return and review the documents again. These original materials filled five federal record center boxes. One box contained NSC numbered documents. Four boxes contained SMOF files. Of these four boxes; one was box W-049 which was brought forward for the entire review. These boxes became know as an artificial collection or the "Berger Request."

Box W-049 was [Redacted] SMOF files. In that box were several NSC numbered documents. When they could not locate a NSC numbered document, they would go to box W-049.

b6, b7C

[Redacted] staff was more sensitive as this was the first access of Clinton Presidential records. [Redacted]

b6, b7C

Case Number: [Redacted] b2	Case Title: Samuel R. Berger [Redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

██████████ explained that at this time the ██████████ was not running. Because the ██████████ was not running, a keyword search of the ██████████ database was conducted by ██████████, from the incumbent President's database, and a hard copy list of results, in the form of NSC numbered document numbers was provided to ██████████ staff.

b2,
b5, b6
b7c

██████████ contained in the correspondence requesting Mr. Berger's access to the records. ██████████

██████████ could not find some of the NSC numbered documents so ██████████ faxed a list back to the NSC of the ones ██████████ could not locate. They told ██████████ they could be in other files.

b6, b7

██████████ said there was never an index of the SMOFs reviewed. ██████████ said ██████████ would not know if he removed originals during this visit.

b6, b7c

██████████ explained there was no automated search for SMOFs. Each box of SMOF material contained a folder file or inventory list. These lists were copied and collated and provided by the NSC. ██████████ had to review the index of file folder lists in order to determine which folders might be responsive. SMOFs were searched by the file folder title using the keywords provided in the correspondence. This was a search where an archivist used their experience and intellect to decide what was responsive to the request. If documents in the SMOF were deemed non-responsive, by ██████████, they were put in an envelope in the back of the SMOF folder.

b6,
b7c

An "out card" was left in each box to mark the place where an NSC numbered document or SMOF was removed and indicated it was pulled for "Berger Request." These cards were blue and made by the ██████████ staff. This was because there were standard "out-cards" left in some files by Clinton staff.

b6,
b7c

██████████ could not recall if Mr. Berger was provided with any documents containing the Millennium Alert After Action Report (MAAAR) on his May 30, 2002, visit. [The subsequent physical review of the materials Mr. Berger reviewed did not indicate he was provided such.]

b6,
b7c

Some of the materials from the May 2002 review were assimilated into the materials responsive to EOP 2 and possibly additional EOP requests. In addition to the out cards left in the boxes from which the documents for Mr. Berger's May 2002 review were originally pulled, ██████████ left out cards referencing they were in the "Berger Request" if those documents were pulled and carried forward in response to EOP 2. In the instances when documents responsive to EOP 2 were still in their original box, an out card was left in the original box indicating the document(s) were withdrawn for "Terror Com" or "Terrorism."

b6, b7

Mr. Berger's review in July 2003

On July 18, 2003, Mr. Berger reviewed original textual documents, four boxes, in ██████████ office. One box contained NSC numbered documents and three boxes contained SMOF files. ██████████ had originally pulled 5 boxes worth of SMOF files. Documents deemed responsive were copied and placed in boxes for ██████████

b2,
b6, b7

Case Number: ██████████ b2	Case Title: Samuel R. Berger ██████████ b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

5

██████████ was running searches for NSC numbered documents in response to EOP2. ██████████ realized ██████████ searches were running faster than ██████████ could pull the documents. ██████████ decided to create a table listing the NSC numbers that needed to be pulled. ██████████ put them in numerical order and divided which ones could be found at ██████████ and which ones were in ██████████ to make ██████████ job go quicker. (The NSC numbered documents ██████████ had initially pulled were not incorporated into ██████████ table.)

b2,
b6,
b7C

██████████ pulled the NSC numbered documents. ██████████ used the list ██████████ created and annotated the status of the document. If it was pulled from a box, the box number was annotated on the index. If the document was pulled from boxes set aside from Mr. Berger's May 2002 visit, the list was annotated that the document was pulled from the "Berger Box." ██████████ prepared a list of NSC numbered documents ██████████. ██████████ sent this list, of six digit numbers only, to ██████████. ██████████ made "out-cards" for the documents ██████████ pulled in response to the 9/11 commission's requests. If the document was pulled but deemed to be non-responsive, it was placed in a file labeled non-responsive as opposed to being re-filed. If ██████████ found them to be non-responsive, they were marked as non-responsive and either removed or put aside in a file designated as non-responsive to EOP 2. They were not sure if it was the same file or a different non-responsive file.

b2,
b6,
b7C

They narrowed NSC's results based on the subject file. The list was sent over in two batches.

██████████ believed the search runs may be with the materials and the keywords would be reflected at the top of the printout.

b6,
b7C

██████████ pulled SMOF files responsive to EOP 2. ██████████ recalled the NSC sent over copies of SMOF inventory sheets and highlighted the ones the NSC believed were responsive to EOP 2. ██████████ felt the NSC was not consistent and missed some of the relevant folders so ██████████ did a "second SMOF pull/search." The total became SMOF's responsive to EOP2. ██████████ believed ██████████ annotated the NSC inventories with ██████████ handwriting. This became a new artificial file. ██████████ probably still maintains the non-responsive file but these files were probably moved forward for subsequent requests.

b6,
b7C

If documents in the SMOF were deemed responsive, then a tab was placed around those documents, they were copied and provided ██████████.

b2

For the SMOF files, an out card was left to mark the place where a SMOF was removed and indicated it was pulled for "Terror Com" or "Terrorism." In addition, ██████████ wrote on the SMOF, in pencil, where the file came from. These documents have not been re-filed in the originating box.

b6,
b7

In July 2003, ██████████ came in to assist Mr. Berger by reviewing documents ██████████ ██████████ reviewed the NSC numbered documents from ██████████, responsive to EOP 2.

b2,
b6,
b7C

In July, the textual document sent by facsimile from ██████████ was put in its own folder when received at ██████████. This document contained the MAAAR and is believed to have originated in ██████████.

b2

Case Number: ██████████ b2	Case Title: Samuel R. Berger ██████████ b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

SMOF [redacted]. At some point, either before or after Mr. Berger's visit in October, an [redacted] staff member looked in the folder labeled [redacted] and saw there was a document in the folder. However, it was later determine it did not contain the right document. The original document remains at the [redacted].

b2, b1
b7c

If Mr. Berger or [redacted] with Mr. Berger deemed any NSC numbered documents non-responsive, they were not sure if they were placed in the non-responsive box or put back with the materials.

b6
b7c

For the July production, the NSC sent copies of the file folder lists (inventories), per box, highlighting the SMOF files which they thought were responsive. [redacted] made a note if [redacted] pulled the document or if [redacted] thought it was non-responsive. [redacted] made a new copy of the inventories and determined which [redacted] thought was responsive.

b6
b7c

The production to the White House for EOP2 was done in two deliveries. The first delivery was from what was deemed responsive by [redacted] after Mr. Berger's review. The White House sent a copy of what was not forwarded to the 911 commission to [redacted].

b6
b7c

The second delivery was from what was deemed responsive after [redacted] review. [redacted] sent up documents which were reviewed by [redacted]. Some of these records were deemed non-responsive to EOP 2 while being reviewed by [redacted] and [redacted]. The documents deemed responsive were sent to the White House.

b2
b5, b6
b7c

[redacted] The White House sent a copy of what was forwarded to the 911 commission to [redacted].

[redacted] staff did not distinguish between the documents pulled for EOP2 and EOP3. The EOP2 request was more restrictive than EOP3. When pulling EOP3, they went back to the production of EOP2. [redacted]

b5

[redacted] They did review the EOP2 documents which the White House did not forwarded to the 9/11 commission. Mr. Berger was provided these documents but they did not know if Mr. Berger reviewed these documents again as he had reviewed them for EOP2.

The White House staff was going to look at what they did not send to the 911 commission for EOP 2 to determine if it was responsive to EOP 3. [redacted] began to review the original files which were pulled for EOP 2 to determine if the documents deemed non-responsive for EOP 2 were responsive to EOP 3. This meant going in a SMOF file and reviewing any material that was not tabbed as responsive to EOP 2. If the tabs were white and had a checkmark on them, the document(s) were copied for EOP 2. NSC numbered documents would have been treated as a whole. [redacted] probably reviewed the documents [redacted] and [redacted] deemed non-responsive for EOP 2 to see if they were responsive to EOP 3. Staff at the [redacted] did a similar search for these materials and sent a copy of documents responsive to EOP 3 to [redacted].

b2
b6
b7c

Mr. Berger's review in September 2003

Mr. Berger was served copies from the [redacted] deemed responsive to EOP3. Mr. Berger was served two SMOF folders from the [redacted] and one SMOF folder from [redacted]. He was served one redwell folder containing NSC numbered documents from [redacted]. He

b2
b6, b7c

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

was also given all the emails but only had time to review a portion of them. [redacted] marked the 66, 57C emails Mr. Berger reviewed.

[redacted] searched the email system using the search terms which were responsive to EOP 3. 66, 67C

The copies of materials from the SMOFs had a cover sheet indicating where the documents originated. They believed there was only one box of materials provided to Mr. Berger. They could not be sure due to the volume of the emails.

Included in this production was a document sent from [redacted]. The document was placed in a folder someone created labeled [redacted]. Today, the [redacted] document is not in the folder, but two other documents are in this folder. 62

Mr. Berger came to do his review of these documents deemed responsive to EOP 3. This copy set was sent to the White House.

Then a second copy set was pulled and sent. [redacted] 65, [redacted] 66, [redacted] took their copy set of what they produced to the White House for EOP 2. This included the documents sent up by [redacted] and [redacted] tabbed the documents the White House sent forward to the 911 commission [redacted] 67C [redacted] from their copy set. [redacted] and [redacted] began reviewing those documents for responsiveness to EOP 3. [redacted] is unsure if they tabbed the documents which were provided to the White House from this set for EOP 3.

Someone indicated the documents were reviewed after Mr. Berger's visit on September 2, 2003, to determine if anything was missing. [redacted] said there was no review of documents Mr. Berger saw on September 2, 2003, to ensure nothing was missing (not after he left). There was not a control set of documents so there was no way to determine if any documents were removed. Today, there could be an attempt to verify the NSC numbered documents and the SMOFs Mr. Berger was provided. However, the real "wildcard" would be the recreation of the emails Mr. Berger was provided. [redacted] used the search terms to query the email, then [redacted] reviewed those for responsiveness on-line and printed what [redacted] deemed as responsive. This was followed by [redacted] reviewing the documents for responsiveness. 66, 67C

After the September visit, the emails were divided in folders as [redacted], which were served to [redacted]. 62, 66, 67C

In preparation for Mr. Berger's review on October 2, 2003, [redacted] numbered the copies, in pencil, in the bottom left corner. The back page of the document was numbered but not the entire document. A document in this case might contain several pages stapled together. The numbers were assigned sequentially. There was a list of numbers that corresponded to a record type. Then they were organized chronologically and numbered. Most of these documents were emails. [redacted] has a recollection that either [redacted] double-checked the numbering. Neither [redacted] had a recollection of doing this. The documents were placed in folders, 66, 67C

Case Number: [redacted] 62 Case Title: Samuel R. Berger [redacted] 62

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

8

separated by responsiveness to paragraphs two and three in the EOP requests. They were also then sorted chronologically. There were about five folders. The numbering sequence was written on the folder. About 25 documents were from SMOF files.

██████████ numbered most of the copies. ██████████ became tired or it was late and ██████████ did not finish numbering the documents. ██████████ provided a note that ██████████ left ██████████ asking ██████████ to complete the numbering the morning of October 2, 2003. ██████████ numbered the remaining documents. b6, b7C

Mr. Berger's review in October 2003

On October 2, 2003, Mr. Berger was served one box of textual material and one box of emails. [They removed the emails Berger had reviewed in September. Then they put the emails in order (see list).] These were numbered and placed in folders. The folders were not numbered, only the documents inside. The folders were not served in numerical order. They had been divided by classification and which paragraph they addressed in the EOP request before they were numbered. The folders were in large accordion folders.

Mr. Berger reviewed his and ██████████ notes first. Really, they were the first items in the box. ██████████ could recall the order documents were served as they were not in the room, with the exception of ██████████. Then, Mr. Berger was provided one folder at a time for review. b6, b7C

██████████ reviewed folders given to him by ██████████ at his desk to determine if any numbers were missing. They had not thought through what would be done if a document was found to be missing. b6, b7C

██████████ was reviewing the folders at someone's desk, outside ██████████ office, when ██████████ discovered #217 missing. ██████████ believed he verified it was missing. b6, b7C

██████████ gave ██████████ the date of the document before the missing email and the date of the document after the missing email, from email #216 and #218. This was the time frame in which ██████████ searched the emails, using the same search terms which were responsive to the EOP request. The staff was able to verify there was an email that should have been printed and produced to Mr. Berger in that time frame. ██████████ located the missing email. ██████████ then left for the day, before printing the missing email ██████████ called back to the office to ensure ██████████ knew what to look for on the email system in order to find the email in question. ██████████ told ██████████ another copy of this email was printed, ██████████ wrote #217 on the back, and provided to ██████████. b6, b7C

██████████ took the email (#217) into Mr. Berger. Shortly after that, ██████████ left ██████████ office. The sofa phone light was lit but then went off. ██████████ went back in ██████████ office and Mr. Berger left abruptly. b6, b7C

██████████ commented to ██████████ staff that ██████████ may have not filed #217 (the second copy) in the right place.

Case Number: ██████████ b2	Case Title: Samuel R. Berger ██████████ b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

After determining four documents were missing, on October 3, 2003, [redacted] assisted in running a quick search and reprinted the missing numbered emails. These were differentiated from the originally marked copies by adding the date and time on the back of each. b6, b7C

The staff noticed [redacted]. However, the date and content was different from the email the sticky was on now (#156). b5

After picking-up documents from Mr. Berger office, on October 5, 2003, [redacted] spoke to [redacted] and told [redacted] one document was the textual document sent up from Little Rock and the other was #323. b6, b7C

Additional Notes:

[redacted] recalled [redacted] instructing Mr. Berger he could take notes but the notes would have to stay at NARA during at least one of his visits, possibly more. b6, b7C

All documents, even copies, were treated as originals. All documents had classification markings on them. [redacted] did not add cover sheets as these were raw unprocessed presidential records. Photocopies were made [redacted] with the designated photocopying machine. All documents provided from the [redacted] were copies. b2, b6, b7C

[redacted] was involved in the verification of NSC numbered documents NARA still held. [redacted] took the list(s) [redacted] used to pull files for Mr. Berger's visits reflecting the NSC numbered documents. [redacted] compared the NSC numbered documents segregated for Mr. Berger's reviews with the list of the files [redacted] pulled for his visits. [redacted] determined no NSC numbered documents were missing. This is not to say pages could not be missing from those documents. [redacted] was not sure if anyone had determined if the NSC numbered documents Mr. Berger reviewed in May 2002 had been verified. b6, b7C

[redacted] was asked to verify the documents sent up by the [redacted] which were responsive to EOP 2 and EOP 3. [redacted] recalled that the [redacted] sent up copies of their cover sheets, which were placed on top of the documents they forwarded to [redacted]. The cover sheets had written on them the number of pages the package contained. [redacted] added these up and compared that number to the number of copies [redacted] still had. They matched. [redacted] was able to locate the cover sheets and can locate the documents which were sent to the White House and probably can locate the documents from this pull deemed non-responsive. b2, b6, b7C

Neither [redacted], nor [redacted] ever wrote up anything concerning this incident or verification. [redacted] was never asked to and did not prepare a statement of facts. However, [redacted] asked [redacted] to prepare a flow chart, which is actually more of a time line. The flow chart is with the administrative files [redacted]. [redacted] provided the drafts of flow charts. b2, b6, b7C

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

All inventory lists are kept with the series of records. There is not a centralized inventory. If the records are unprocessed the inventory list provided with the documents is used.

██████████ has a courier card. ██████ received the card in the mail and was never briefed by NAS and did not sign any receipt or other forms. However, ██████ received informal training on the transmittal of classified information through ISOO several years ago.

b6,
b7C

The original MAAAR was never served to Mr. Berger. It did not come up on any of the search terms. ██████ staff later searched by the word "Millennium" or the NSC number and provided a copy of the original MAAAR to the White House.

b6,
b7C

After Mr. Berger's review, non-responsive documents were normally placed in a separate area. These documents would be reviewed in subsequent requests.

Tabs were being removed for reviewing and copying for several months as the EOP requests extended beyond EOP3. ██████ staff said there was much room for human error on the exact documents the tabs were placed around. Some of the tabs had notes on them and some were written over. There were two tabs in the bottom of a box, not attached to anything.

b6, b7C

If an NSC numbered document had already been provided in EOP 2 (original), a copy of the NSC numbered document was moved forward to the EOP 3 production. Out cards were only placed in the box when an original was removed. All photocopies of documents provided to Mr. Berger had a cover sheet indicating where the copy originated. Mr. Berger did review documents from ██████ in response to EOP 3.

b2

The other copies provided to Mr. Berger had a cover sheet on them indicating their origin. Some copies even reflected the NARA "slug."

The staff ensured all emails identified as removed by Mr. Berger were produced. On October 10, 2003, they confirmed everything they expected to have they had and had annotated if they could not find a document during the original search.

Copies of the materials provided to the NSC responsive to the EOP requests are maintained ██████

b2

Each collection ██████ has an inventory. These are kept in folders ██████. ██████ does not create a new inventory but kept the one that came with the boxes from the White House. Each box from the Clinton administration records, the "W" files, stored in the ██████ is numbered sequentially and has in inventory sheet contained within. A copy of each inventory sheet is kept in a Hollinger box ██████. The NSC passed these over as a set.

b2,
b6,
b7C

██████████ indicated that copies of classified material were marked with the same classification as the original by virtue of the fact the classification marking on the original carried over to the copy. Furthermore, emails included the classification ██████ in the metadata that served as the "cover" for the emails.

b2,
b6,
b7C

Case Number: ██████████ b2	Case Title: Samuel R. Berger ██████ b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

About a month ago, the [redacted] staff went through the documents Mr. Berger reviewed and tracked them down from their final destination [pulled for additional EOP requests] to their originating box.

b6, b7c

[redacted] staff maintains the inventories sent over from the White House. A very few of these inventories are maintained in an electronic finding aid, [redacted].

b2, b6, b7c

The Millennium Alert After Action Review (MAAAR) was 13 pages long.

#150 – has no email content, subject line only, just attachment

#217 – has 3 lines in the email with the attachment

#323 – has a short email, 3 paragraphs, with the attachment

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

EXHIBIT #3

NOTE TO FOIA REQUESTERS

Exhibit #3 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(3)



PDF Version

MS Word Version

(DCID 6/9) — MANUAL

Physical Security Standards for Sensitive Compartmented Information Facilities

(Effective 18 November 2002)

TABLE OF CONTENTS

PREFACE.

1. POLICY AND CONCEPT

1.1 Policy Statement

1.2 Concept

1.3 American Disabilities Act (ADA) Review

2. GENERAL ADMINISTRATIVE

2.1 SCI Facilities (SCIFs)

2.2 Physical Security Preconstruction Review and Approval

2.3 Accreditation

2.4 Co-Utilization

2.5 Personnel Controls

2.6 Control of Combinations

2.7 Entry/Exit Inspections

2.8 Control of Electronic Devices and Other Items

3. PHYSICAL SECURITY CONSTRUCTION POLICY FOR SCIFs

3.1 Construction Policy for SCI Facilities

3.2 Temporary Secure Working Area (TSWA).

3.3 Requirements Common To All SCIFs; Within The US and

Overseas

4. CONSTRUCTION SPECIFICATIONS

4.1 Vault Construction Criteria

4.2 SCIF Criteria For Permanent Dry Wall Construction

4.3 SCIF Construction Criteria For Steel Plate

4.4 SCIF Construction Criteria For Expanded Metal.

4.5 General.

5. GLOSSARY

ANNEX A - SCIF Accreditation Checklist

ANNEX B - Intrusion Detection Systems (IDS)

ANNEX C - Tactical Operations/Field Training

PART I - Ground Operation.

PART II - Aircraft/Airborne Operation.

PART III - Shipboard Operation.

ENCLOSURE(4)

ANNEX D

PART I - Electronic Equipment in Sensitive Compartmented Facilities (SCIFs)

PART II - Disposal of Laser Toner Cartridges

ANNEX E - Acoustical Control and Sound Masking Techniques

ANNEX F - Personnel Access Controls

ANNEX G - Telecommunications Systems and Equipment

PREFACE:

DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs) was approved by the Director of Central Intelligence (DCI) on 30 January 1994.

A complete copy of DCID 6/9 consists of the basic DCID and annexes A through G. The annexes are as follows:

- Annex SCIF Checklist (approved 27 May 1994)
 - A -
 - Annex Intrusion Detection Systems (revised 18 November 2002)
 - B -
 - Annex Tactical Operations/Field Training (approved 27 May 1994)
 - C -
 - Part I - Ground Operation
 - Part II- Aircraft/Airborne Operation
 - Part III - Shipborne Operation
 - Annex Part I - Electronic Equipment in SCIFs (approved 30 January 1994)
 - D - Part II - Handling and Disposal of Laser Toner Cartridges (revised 5 June 1998)
 - Annex Acoustical control and Sound Masking Techniques (approved 30
 - E - January 1994)
 - Annex Personnel Access Controls (revised 18 November 2002)
 - F -
 - Annex Telephone Security (revised 18 November 2002)
 - G -
-

1. POLICY AND CONCEPT**1.1 Policy Statement**

1.1.1 Physical security standards are hereby established governing the construction and protection of facilities for storing, processing, and discussing Sensitive Compartmented Information (SCI) which requires extraordinary security safeguards. Compliance with this DCID 6/9 Implementing Manual (hereafter referred to as the "Manual") is mandatory for all Sensitive Compartmented Information Facilities (SCIFs) established after the effective date of this manual, including those that make substantial renovations to existing SCIFs. Those SCIFs approved prior to the effective date of this Manual will not require modification to meet these standards.

1.1.2 The physical security safeguards set forth in this Manual are the standards for the protection of SCI. Senior Officials of the Intelligence Community (SOICs), with DCI concurrence, may impose more stringent standards if they believe extraordinary conditions and circumstances warrant. SOICs may not delegate this authority. Additional cost resulting from more stringent

standards should be borne by the requiring Agency, Department, or relevant contract.

Obtained via FOIA by Judicial Watch, Inc.

1.1.3 In situations where conditions or unforeseen factors render full compliance to these standards unreasonable, the SOIC or designee may waive specific requirements in accordance with this Manual. However, this waiver must be in writing and specifically state what has been waived. The Cognizant Security Authority (CSA) must notify all co-utilizing agencies of any waivers it grants.

1.1.4 All SCIFs must be accredited by the SOIC or designee prior to conducting any SCI activities.

1.1.5 One person is now authorized to staff a SCIF, which eliminates the two-person rule (the staffing of a SCIF with two or more persons in such proximity to each other to deter unauthorized copying or removal of SCI).

1.2 Concept

1.2.1 SCIF design must balance threats and vulnerabilities against appropriate security measures in order to reach an acceptable level of risk. Each security concept or plan must be submitted to the CSA for approval. Protection against surreptitious entry, regardless of SCIF location, is always required. Security measures must be taken to deter technical surveillance of activities taking place within the SCIF. TEMPEST security measures must be considered if electronic processing of SCI is involved.

1.2.2 On military and civilian compounds, there may exist security controls such as identification checks, perimeter fences, police patrols, and other security measures. When considered together with the SCIF location and internal security systems, those controls may be sufficient to be used in lieu of certain physical security or construction requirements contained in this Manual.

1.2.3 Proper security planning for a SCIF is intended to deny foreign intelligence services and other unauthorized personnel the opportunity for undetected entry into those facilities and exploitation of sensitive activities. Faulty security planning and equipment installation not only jeopardizes security but wastes money. Adding redundant security features causes extra expense which could be used on other needed features. When security features are neglected during initial construction, retrofitting of existing facilities to comply with security requirements is necessary.

1.3 American Disabilities Act (ADA) Review

1.3.1 Nothing in this manual shall be construed to contradict or inhibit compliance with the law or building codes. CSAs shall work to meet appropriate security needs according to the intent of this Manual at acceptable cost.

2. GENERAL ADMINISTRATIVE

2.1 SCI Facilities (SCIFs)

A SCIF is an accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or electronically processed. SCIFs will be afforded personnel access control to preclude entry by unauthorized personnel. Non-SCI indoctrinated personnel entering a SCIF must be continuously escorted by an indoctrinated employee who is familiar with the security procedures of that SCIF. The physical security protection for a SCIF is intended to prevent as well as detect visual, acoustical, technical, and physical access by unauthorized persons. Physical

Obtained via FOIA by Judicial Watch, Inc.

security criteria are governed by whether the SCIF is in the United States or not, according to the following conditions: closed storage, open storage, continuous operations, secure working area.

2.2 Physical Security Preconstruction Review and Approval

CSAs shall review physical security preconstruction plans for SCIF construction, expansion or modification. All documentation pertaining to SCIF construction will be appropriately controlled and restricted on a need-to-know basis. The approval or disapproval of a physical security preconstruction plan shall be made a matter of record.

2.2.1 The requester shall submit a Fixed Facility Checklist (FFC, Annex A) to the respective CSA for review and approval.

2.2.2 The Checklist submission shall include floor plans, diagrams of electrical communications, heating, ventilation, air conditioning (HVAC) connections, security equipment layout (to include the location of intrusion detection equipment), etc. All diagrams or drawings must be submitted on legible and reproducible media.

2.2.3 The CSA shall be responsible for providing construction advice and assistance and pre-approving SCIF construction or modification.

2.3 Accreditation

The CSA will ensure SCIFs comply with DCID 6/9. The CSA is authorized to inspect any SCIF, direct action to correct any deficient situation, and withdraw SCIF accreditation. The procedures for establishment and accreditation of SCIFs are prescribed below:

2.3.1 The procedures for establishment and accreditation of SCIFs from conception through construction must be coordinated and approved by the SOIC or CSA.

2.3.2 SCI shall never be handled, processed, discussed, or stored in any facility other than a properly accredited SCIF unless written authorization is granted by the CSA.

2.3.3 An inspection of the SCIF shall be performed by the CSA or appointed representative prior to accreditation. Periodic reinspections shall be based on threat, physical modifications, sensitivity of programs, and past security performance. Inspections may occur at any time, announced or unannounced. The completed fixed facility checklist will be reviewed during the inspection to ensure continued compliance. TSCM evaluations may be required at the discretion of the CSA, as conditions warrant. Inspection reports shall be retained within the SCIF and by the CSA. All SCIFs shall maintain on site, current copies of the following documents:

- a. DCID 6/9 Fixed Facility Checklist
- b. Accreditation authorization documents (e.g., physical, TEMPEST, and AIS).
- c. Inspection reports, including TSCM reports, for the entire period of SCIF accreditation
- d. Operating procedures, Special Security Officer Contractor Special Security Officer (SSO/CSSO) appointment letters, Memoranda of Agreement (MOAs), Emergency Action Plans, etc.
- e. Copies of any waivers granted by the CSA.

2.3.4 Inspection: Authorized inspectors shall be admitted to a SCIF without delay or hindrance when inspection personnel are properly certified to have the appropriate level of security clearance and SCI indoctrination for the security level of the SCIF. Short notice or emergency conditions may warrant entry without regard to the normal SCIF duty hours. Government owned equipment needed to conduct SCIF inspections will be admitted into SCIF without delay.

2.3.5 Facilities which are presently accredited, under construction or in the approval process at the date of implementation of this Manual shall not require modification to conform to these standards.

2.3.5.1 Facilities undergoing major modification may be required to comply entirely with the provisions of this Manual. Approval for such modifications shall be requested through the CSA and received prior to any modifications taking place within the SCIF.

2.3.5.2 In the event a need arises to reopen a SCIF after the accreditation has been terminated, the CSA may approve the use of a previously accredited SCIF based upon a review of an updated facility accreditation package.

2.3.6 Withdrawal of Accreditation:

2.3.6.1 Termination of Accreditation: When it has been determined that a SCIF is no longer required, withdrawal of accreditation action will be initiated by the SSO/CSSO. Upon notification, the CSA will issue appropriate SCI withdrawal correspondence. The CSA or appointed representative will conduct a close out inspection of the facility to ensure that all SCI material has been removed.

2.3.6.2 Suspension or Revocation of Accreditation: When the CSA determines that there is a danger of classified information being compromised or that security conditions in a SCIF are unsatisfactory, SCI accreditation will be suspended or revoked. All appropriate authorities must be notified of such action immediately.

2.4 Co-Utilization

2.4.1 Agencies desiring to co-utilize a SCIF should accept the current accreditation and any waivers. Any security enhancements required by an agency or department requesting co-utilization should be funded by that organization, and must be approved by the SOIC with DCI concurrence prior to implementation. A co-utilization agreement must be established prior to occupancy.

2.4.2 Special Access Programs (SAP) co-located within a SCIF will meet the physical security requirements of this Manual and DCI Special Access Programs (SAP) Policy, January 4, 1989.

2.5 Personnel Controls

2.5.1 Access rosters listing all persons authorized access to the facility shall be maintained at the SCIF point of entry. Electronic systems, including coded security identification cards or badges may be used in lieu of security access rosters.

2.5.2 Visitor identification and control: Each SCIF shall have procedures for identification and control of visitors seeking access to the SCIF.

2.6 Control of Combinations

Obtained via FOIA by Judicial Watch, Inc.

2.6.1 Combinations to locks installed on security containers/safes, perimeter doors, windows and any other openings should be changed whenever:

- a. A combination lock is first installed or used;
- b. A combination has been subjected, or believed to have been subjected to compromise; and
- c. At other times when considered necessary by the CSA.

2.6.2 All combinations to SCIF entrance doors should be stored in another SCIF of equal or higher accreditation level. When this is not feasible, alternate arrangements will be made in coordination with the CSA.

2.7 Entry/Exit Inspections

The CSA shall prescribe procedures for inspecting persons, their property, and vehicles at the entry or exit points of SCIFs, or at other designated points of entry to the building, facility, or compound. The purpose of the inspection is to deter the unauthorized removal of classified material, and deter the introduction of prohibited items or contraband. This shall include determination of whether inspections are randomly conducted or mandatory for all, and whether they apply for visitors only or for the entire staff assigned. All personnel inspection procedures should be reviewed by the facility's legal counsel prior to promulgation.

2.8 Control of Electronic Devices and Other Items

2.8.1 The CSA shall ensure that procedures are instituted for control of electronic devices and other items introduced into or removed from the SCIF. See Annex D for guidance.

2.8.2 The prohibition against electronic equipment in SCIFs does not apply to those needed by the disabled or for medical or health reasons (e.g. motorized wheelchairs, hearing aids, heart pacemakers, amplified telephone headsets, teletypewriters for the hearing impaired). However, the SSO or CSSO shall establish procedures for notification that such equipment is being entered in to the SCIF.

2.8.3 Emergency and police personnel and their equipment, including devices carried by emergency medical personnel responding to a medical crisis within a SCIF, shall be admitted to the SCIF without regard to their security clearance status. Emergency personnel will be escorted to the degree practical. However, debriefing of emergency personnel will be accomplished as soon as possible, if appropriate.

2.8.4 Equipment for TEMPEST or Technical Surveillance Countermeasures (TSCM) testing shall be admitted to a SCIF as long as the personnel operating the equipment are certified to have the appropriate level of security clearance and SCI indoctrination.

3. PHYSICAL SECURITY CONSTRUCTION POLICY FOR SCIFs

3.1 Construction Policy for SCI Facilities

Physical security criteria is governed by whether the SCIF is located in the US or not, according to the following conditions: closed storage, open storage, continuous operations, secure working areas.

3.1.1 Closed Storage

3.1.1.1 Inside U.S.:

- a. The SCIF must meet the specifications in Chapter 4 Permanent Dry Wall Construction).
- b. The SCIF must be alarmed in accordance with Annex B to this manual.
- c. SCI must be stored in GSA approved security containers.
- d. There must be a response force capable of responding to an alarm within 15 minutes after annunciation and a reserve response force available to assist the responding force.
- e. The CSA may require any SCIF perimeter walls accessible from exterior building ground level to meet the equivalent protection afforded by Chapter 4 (Expanded Metal) construction requirement.

3.1.1.2 Outside U.S.:

- a. The SCIF must meet the construction specifications for SCIFs as set forth in Chapter 4 (Steel Plate or Expanded Metal). SCIFs within US Government controlled compounds ^[1][1], or equivalent, having armed immediate response forces may use specifications indicated in Chapter 4 (Permanent Dry Wall Construction) with prior approval of the CSA.
- b. The SCIF must be alarmed in accordance with Annex B.
- c. All SCI controlled material will be stored in GSA-approved containers having a rating for both forced and surreptitious entry equal to or exceeding that afforded by Class 5 containers.
- d. There must be a response force capable of responding to an alarm within 10 minutes and a reserve response force available to assist the responding force.

3.1.2 Open Storage

3.1.2.1 INSIDE US: When open storage is justified and approved by the CSA. the SCIF must:

- a. be alarmed in accordance with Annex B;
- b. have a response force capable of responding to an alarm within 5 minutes and a reserve response force available to assist the response force; and
- c. meet one of the following:
 1. SCIFs within a controlled US government compound or equivalent may use specifications indicated in Chapter 4 (Permanent Dry Wall Construction): or

Obtained via FOIA by Judicial Watch, Inc.

2. SCIFs within a controlled building with continuous personnel access control, may use specifications indicated in Chapter 4 (Permanent Dry Wall Construction). The CSA may require any SCIF perimeter walls accessible from exterior building ground level to meet the equivalent protection afforded by Chapter 4 (Expanded Metal) construction requirements; or
3. SCIFs which are not located in a controlled building or compound may use specifications indicated in Chapter 4 (expanded Metal) or (Vault) constructions requirements.

3.1.2.2 OUTSIDE US: Open storage of SCI material will be avoided. When open storage is justified as mission essential, vault construction is preferred. The SCIF must:

- a. be alarmed in accordance with Annex B;
- b. have a response force capable of responding to an alarm within 5 minutes and a reserve response force available to assist the responding force.
- c. have an adequate, tested plan to protect, evacuate, or destroy the material in the event of emergency or natural disaster; and
- d. meet one of the following:
 1. The construction specification for vaults set forth in Chapter 4 (Vaults); or
 2. With the approval of the CSA, SCIFs located on a controlled US government compound or equivalent having immediate response forces, may use expanded metal, steel plate, or GSA approved modular vaults in lieu of vault construction.

3.1.3 Continuous Operation

3.1.3.1 INSIDE THE US:

- a. The SCIF must meet the construction specifications as identified in Chapter 4 (Permanent Dry Wall Construction). An alert system and duress alarm may be required by the CSA, based on operational and threat conditions.
- b. Provisions should be made for storage of SCI in GSA approved containers. If the configuration of the material precludes this, there must be an adequate, tested plan to protect, evacuate, or destroy the material in the event of emergency, civil unrest or natural disaster.
- c. There must be a response force capable of responding to an alarm within 5 minutes and a reserve response force available to assist the responding force.

3.1.3.2 OUTSIDE THE US:

- a. The SCIF must meet the construction specifications for SCIFs as set forth in Chapter 4 (Expanded Metal). An alert system and duress alarm may be required by the CSA, based on operational and threat conditions. (b) The

capability must exist for storage of all SCI in GSA-approved security containers, or the SCIF must have an adequate, tested plan to protect, evacuate, or destroy the material in the event of emergency or natural disaster.

- b. SCIFs located within US Government controlled compounds, or equivalent, having immediate response forces, may use the secure area construction specifications as listed in Chapter 4 (Permanent Dry Wall Construction) with prior approval of the CSA
- c. There must be a response force capable of responding to an alarm within 5 minutes, and a reserve response force available to assist the responding force.

3.1.4 Secure Working Areas are accredited facilities used for handling, discussing, and/or processing SCI. but where SCI will not be stored.

3.1.4.1 INSIDE THE U.S.:

- a. The Secure Working Area SCIF must meet the specifications set forth in Chapter 4 (Permanent Dry Wall Construction).
- b. The Secure Working Area SCIF must be alarmed with a balanced magnetic switch on all perimeter entrance doors.
- c. No storage of SCI material is authorized.
- d. There must be a response force capable of responding to an alarm within 15 minutes after annunciation, and a reserve response force available to assist the responding force.

3.1.4.2 OUTSIDE THE U.S.:

- a. The Secure Working Area SCIF must meet the construction specifications indicated in Chapter 4 (Permanent Dry Wall Construction).
- b. The Secure Working Area SCIF must be equipped with an approved alarm system as set forth in Annex B.
- c. No storage of SCI material is authorized.
- d. There must be a response force capable of responding to an alarm within 10 minutes, and a reserve response force available to assist the responding force.

3.2 Temporary Secure Working Area (TSWA)

3.2.1 A Temporary Secure Working area is defined as a temporarily accredited facility that is used no more than 40 hours monthly for the handling, discussion, and/or processing of SCI, but where SCI should not be stored. with sufficient justification, the CSA may approve longer periods of usage and storage of SCI for no longer than 6 months.

3.2.2 During the entire period the TSWA is in use, the entrance will be controlled and access limited to persons having clearance for which the area has been approved. Approval for

Obtained via FOIA by Judicial Watch, Inc.

using such areas must be obtained from the CSA setting forth room number(s), building, location, purpose, and specific security measures employed during usage as well as during other periods. TSWAs should be covered by an alarm system. These areas should not be used for periods exceeding an average total of 40 hours per month. No special construction is required other than to meet sound attenuation requirements as set forth in Annex E, when applicable. If such a facility must also be used for the discussion of SCI, a Technical Surveillance Countermeasures (TSCM) evaluation may be required at the discretion of the CSA, as conditions warrant.

3.2.3 When not in use at the SCI level, the TSWA will be:

- a. Secured with a keylock or a combination lock approved by the CSA.
- b. Access will be limited to personnel possessing a US Secret clearance.

3.2.4 If such a facility is not alarmed or properly protected during periods of non-use, a TSCM inspection may be conducted prior to use for discussion at the SCI level.

3.3 Requirements Common To All SCIFs; Within The US and Overseas

3.3.1 CONSTRUCTION: The SCIF perimeter walls, floors and ceiling, will be permanently constructed and attached to each other. All construction must be done in such a manner as to provide visual evidence of unauthorized penetration.

3.3.2 SOUND ATTENUATION: The SCIF perimeter walls, doors, windows, floors and ceiling, including all openings, shall provide sufficient sound attenuation to preclude inadvertent disclosure of conversation. The requirement for sound attenuation are contained within Annex E.

3.3.3 ENTRANCE, EXIT, AND ACCESS DOORS:

3.3.3.1 Primary entrance doors to SCIFs shall be limited to one. If circumstances require more than one entrance door, this must be approved by the CSA. In some circumstances, an emergency exit door may be required. In cases where local fire regulations are more stringent, they will be complied with. All perimeter SCIF doors must be closed when not in use, with the exception of emergency circumstances. If a door must be left open for any length of time due to an emergency or other reasons, then it must be controlled in order to prevent unauthorized removal of SCI.

3.3.3.2 All SCIF perimeter doors must be plumbed in their frames and the frame firmly affixed to the surrounding wall. Door frames must be of sufficient strength to preclude distortion that could cause improper alignment of door alarm sensors, improper door closure or degradation of audio security.

3.3.3.3 All SCIF primary entrance doors must be equipped with an automatic door closer, a GSA-approved combination lock and an access control device with the following requirements:^[2]_[2]

- a. If doors are equipped with hinge pins located on the exterior side of the door where it opens into an uncontrolled area outside the SCIF, the hinges will be treated to prevent removal of the door (e.g., welded, set screws, etc.)
- b. If a SCIF entrance door is not used as an access control door and stands open in an uncontrolled area, the combination lock will be protected against

unauthorized access/tampering.

3.3.3.4 Control doors: The use of a vault door for controlling daytime access to a facility is not authorized. Such use will eventually weaken the locking mechanism, cause malfunctioning of the emergency escape device, and constitute a security and safety hazard. To preclude this, a second door will be installed and equipped with an automatic door closer and an access control device. (It is preferable that the access door be installed external to the vault door.)

3.3.3.5 SCIF emergency exit doors shall be constructed of material equivalent in strength and density to the main entrance door. The door will be secured with deadlocking panic hardware on the inside and have no exterior hardware. SCIF perimeter emergency exit doors should be equipped with a local enunciator in order to alert people working in the area that someone exited the facility due to some type of emergency condition.

3.3.3.6 Door Construction Types: Selections of entrance and emergency exit doors shall be consistent with SCIF perimeter wall construction. Specifications of doors, combination locks, access control devices and other related hardware may be obtained from the CSA. Some acceptable types of doors are:

- a. Solid wood core door, a minimum of 1 3/4 inches thick.
- b. Sixteen gauge metal cladding over wood or composition materials, a minimum of 1 3/4 inches thick. The metal cladding shall be continuous and cover the entire front and back surface of the door.
- c. Metal fire or acoustical protection doors, a minimum of 1 3/4 inches thick. A foreign manufactured equivalent may be used if approved by the CSA.
- d. A joined metal rolling door, minimum of 22 gauge, used as a loading dock or garage structure must be approved on a case-by-case basis.

3.3.4 PHYSICAL PROTECTION OF VENTS, DUCTS, AND PIPES:

3.3.4.1 All vents, ducts, and similar openings in excess of 96 square inches that enter or pass through a SCIF must be protected with either bars, or grills, or commercial metal duct sound baffles that meet appropriate sound attenuation class as specified in Annex E. Within the United States, bars or grills are not required if an IDS is used. If one dimension of the duct measures less than six inches, or duct is less than 96 square inches, bars are not required; however, all ducts must be treated to provide sufficient sound attenuation. If bars are used, they must be 1/2 inch diameter steel welded vertically and horizontally six (6) inches on center; if grills are used, they must be of 9-gauge expanded steel; if commercial sound baffles are used, the baffles or wave forms must be metal permanently installed and no farther apart than six (6) inches in one dimension. A deviation of 1/2 inch in vertical and/or horizontal spacing is permissible.

3.3.4.2 Based on the TEMPEST accreditation, it may be required that all vents, ducts, and pipes must have a non-conductive section (a piece of dissimilar material e.g., canvas, rubber) which is unable to carry electric current, installed at the interior perimeter of the SCIF.

3.3.4.3 An access port to allow visual inspection of the protection in the vent or duct should be installed inside the secure perimeter of the SCIF. If the inspection port must be installed outside the perimeter of the SCIF, it must be locked.

3.3.5 WINDOWS:

Obtained via FOIA by Judicial Watch, Inc.

3.3.5.1 All windows which might reasonably afford visual surveillance of personnel, documents, materials, or activities within the facility, shall be made opaque or equipped with blinds, drapes or other coverings to preclude such visual surveillance.

3.3.5.2 Windows at ground level ^[3][3] will be constructed from or covered with materials which will provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. SCIFs located within fenced and guarded government compounds or equivalent may eliminate this requirement if the windows are made inoperable by either permanently sealing them or equipping them on the inside with a locking mechanism.

3.3.5.3 All perimeter windows at ground level shall be covered by an IDS.

4. CONSTRUCTION SPECIFICATIONS.

4.1 Vault Construction Criteria

4.1.1 Reinforced Concrete Construction: Walls, floor, and ceiling will be a minimum thickness of eight inches of reinforced concrete. The concrete mixture will have a comprehensive strength rating of at least 2,500 psi. Reinforcing will be accomplished with steel reinforcing rods, a minimum of 5/8 inches in diameter, positioned centralized in the concrete pour and spaced horizontally and vertically six inches on center; rods will be tied or welded at the intersections. The reinforcing is to be anchored into the ceiling and floor to a minimum depth of one-half the thickness of the adjoining member.

4.1.2 GSA-approved modular vaults meeting Federal Specification FF-V-2737, may be used in lieu of a 4.1.1 above.

4.1.3 Steel-lined Construction: Where unique structural circumstances do not permit construction of a concrete vault, construction will be of steel alloy-type of 1/4" thick, having characteristics of high yield and tensile strength. The metal plates are to be continuously welded to load-bearing steel members of a thickness equal to that of the plates. If the load-bearing steel members are being placed in a continuous floor and ceiling of reinforced concrete, they must be firmly affixed to a depth of one-half the thickness of the floor and ceiling.

If the floor and/or ceiling construction is less than six inches of reinforced concrete, a steel liner is to be constructed the same as the walls to form the floor and ceiling of the vault. Seams where the steel plates meet horizontally and vertically are to be continuously welded together.

4.1.4 All vaults shall be equipped with a GSA-approved Class 5 or Class 8 vault door. Within the US, a Class 6 vault door is acceptable. Normally within the United States a vault will have only one door that serves as both entrance and exit from the SCIF in order to reduce costs.

4.2 SCIF Criteria For Permanent Dry Wall Construction

Walls, floor and ceiling will be permanently constructed and attached to each other. To provide visual evidence of attempted entry, all construction, to include above the false ceiling and below a raised floor, must be done in such a manner as to provide visual evidence of unauthorized Penetration.

4.3 SCIF Construction Criteria For Steel Plate

Obtained via FOIA by Judicial Watch, Inc.

Walls, ceiling and floors are to be reinforced on the inside with steel plate not less than 1/8" thick. The plates at all vertical joints are to be affixed to vertical steel members of a thickness not less than that of the plates. The vertical plates will be spot welded to the vertical members by applying a one-inch long weld every 12 inches; meeting of the plates in the horizontal plane will be continuously welded. Floor and ceiling reinforcements must be securely affixed to the walls with steel angles welded or bolted in place.

4.4 SCIF Construction Criteria For Expanded Metal

Walls are to be reinforced, slab-to-slab, with 9-gauge expanded metal. The expanded metal will be spot welded every 6 inches to vertical and horizontal metal supports of 16-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.

4.5 General

The use of materials having thickness or diameters larger than those specified above is permissible. The terms "anchored to and/or embedded into the floor and ceiling" may apply to the affixing of supporting members and reinforcing to true slab or the most solid surfaces; however, subfloors and false ceiling are not to be used for this purpose.

5. GLOSSARY

Access Control System: A system to identify and/or admit personnel with properly authorized access to a SCIF using physical, electronic, and/or human controls.

Accreditation: The formal approval of a specific place, referred to as a Sensitive Compartmented Information Facility (SCIF), that meets prescribed physical, technical, and personnel security standards.

Acoustic Security: Those security measures designed and used to deny aural access to classified information.

Astragal Strip: A narrow strip of material applied over the gap between a pair of doors for protection from unauthorized entry and sound attenuation.

Authorized Personnel: A person who is fully cleared and indoctrinated for SCI, has a valid need to know, and has been granted access to the SCIF.

Balanced Magnetic Switch (BMS): A type of IDS sensor which may be installed on any rigid, operable opening (i.e., doors, windows) through which access may be gained to the SCIF.

Break-Wire Detector: An IDS sensor used with screens and grids, open wiring, and grooved stripping in various arrays and configurations necessary to detect surreptitious and forcible penetrations of movable openings, floors, walls, ceilings, and skylights. An alarm is activated when the wire is broken.

Closed Storage: The storage of SCI material in properly secured GSA approved security containers within an accredited SCIF.

Computerized Telephone System (CTS): Also referred to as a hybrid key system, business communication system, or office communications system.

Cognizant Security Authority (CSA): The single principal designated by a SOIC (see definition

Obtained via FOIA by Judicial Watch, Inc.

of SOIC) to serve as the responsible official for all aspects of security program management with respect to the protection of intelligence sources and methods, under SOIC responsibility.

Continuous Operation: This condition exists when a SCIF is staffed 24 hours every day.

Controlled Area/Compound: Any area to which entry is subject to restrictions or control for security reasons.

Controlled Building: A building to which entry is subject to restrictions or control for security reasons.

Co-Utilization: Two or more organizations sharing the same SCIF

Dead Bolt: A lock bolt with no spring action. Activated by a key or turn knob and cannot be moved by end pressure.

Deadlocking Panic Hardware: A panic hardware with a deadlocking latch that has a device when in the closed position resists the latch from being retracted.

Decibel (db): A unit of sound measurement.

Document: Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, paintings, drawings, photos, engravings, sketches, working notes and papers, reproductions of such things by any means or process, and sound, voice, magnetic or electronic recordings in any form.

Dual Technology: PIR, microwave or ultrasonic IDS sensors which combine the features of more than one volumetric technology.

Expanded Steel: Also called EXPANDED METAL MESH. A lace work patterned material produced from sheet steel by making regular uniform cuts and then pulling it apart with uniform pressure.

Guard: A properly trained and equipped individual whose duties include the protection of a SCIF. Guards whose duties require direct access to a SCIF, or patrol within a SCIF, must meet the clearance criteria in Director of Central Intelligence Directive 6/4. CSA will determine if indoctrination is required.

Intelligence Community (and agencies within the (and agencies within the Community): Refers to the United States Government agencies and organizations identified in section 3.4(f) (1 through 7) of Executive Order 12333.

Intrusion Detection System: A security alarm system to detect unauthorized entry.

Isolator: A device or assembly of devices which isolates or disconnects a telephone or Computerized Telephone System (CTS) from all wires which exit the SCIF and which as been accepted as effective for security purposes by the Telephone Security Group (TSG approved).

Key Service Unit (KSU): An electromechanical switching device which controls routing and operation of an analog telephone system.

Line Supervision:

Obtained via FOIA by Judicial Watch, Inc.

Class I: Class I line security is achieved through the use of DES or an algorithm based on the cipher feedback or cipher block chaining mode of encryption. Certification by NIST or another independent testing laboratory is required.

Class II: Class II line supervision refers to systems in which the transmission is based on pseudo random generated or digital encoding using an interrogation and response scheme throughout the entire communication, or UL Class AA line supervision. The signal shall not repeat itself within a minimum six month period, Class II security shall be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

Motion Detection Sensor: An alarm sensor that detects movement.

Non-Conductive Section: Material (i.e. canvas, rubber, etc.) which is installed in ducts, vents, or pipes, and is unable to carry audio or RF emanations.

Non-Discussion Area: A clearly defined area within a SCIF where classified discussions are not authorized due to inadequate sound attenuation.

Open Storage: The storage of SCI material within a SCIF in any configuration other than within GSA approved security containers.

Response Force: Personnel (not including those on fixed security posts) appropriately equipped and trained, whose duties include initial or follow up response to situations which threaten the security of the SCIF. This includes local law enforcement support or other external forces as noted in agreements.

Secure Working Area: An accredited SCIF used for handling, discussing and/or processing of SCI, but where SCI will not be stored.

Senior Official of the Intelligence Community (SOIC): The head of an agency, of fine, bureau, or intelligence element identified in section 3.4(f) (1 through 6) of Executive Order 12333.

Sensitive Compartmented Information (SCI): SCI is classified information concerning or derived from intelligence sources, methods or analytical processes, which is required to be handled exclusively within formal control systems established by the Director of Central Intelligence.

Sensitive Compartmented Information Facility (SCIF): An accredited area, room, group of rooms, building, or installation where SCI may be stored, used, discussed and/or electronically processed.

Sound Group: Voice transmission attenuation groups established to satisfy acoustical requirements. Ratings measured in sound transmission class may be found in the Architectural Graphic Standards.

Sound Transmission Class (STC): The rating used in architectural considerations of sound transmission loss such as those involving walls, ceilings, and/or floors.

Special Access Program (SAP): Any approved program which imposes need-to-know or access controls beyond those normally required for access to CONFIDENTIAL, SECRET, or TOP SECRET information.

Surreptitious Entry: Unauthorized entry in a manner which leaves no readily discernible evidence.

Obtained via FOIA by Judicial Watch, Inc.

Tactical SCIF: An accredited area used for actual or simulated war operations for a specified period of time.

Technical Surveillance Countermeasures (TSCM) Surveys and Evaluations: A physical, electronic, and visual examination to detect technical surveillance devices, technical security hazards, and attempts at clandestine penetration.

Type Accepted Telephone: Any telephone whose design and construction conforms with the design standards for Telephone Security Group approved telephone sets. (TSG Standard #3, #4, or #5).

Vault: A room(s) used for the storing, handling, discussing, and/or processing of SCI and constructed to afford maximum protection against unauthorized entry.

Waiver: An exemption from a specific requirement of this document.

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) 6/9

ANNEX A - SCIF Accreditation Checklist

(Effective 27 May 1994)

Table of Contents

- Section A--General Information
- Section B--Peripheral Security
- Section C--SCIF Security
- Section D--Doors
- Section E--Intrusion Detection Systems
- Section F--Telephone System
- Section G--Acoustical Protection
- Section H--Administrative Security
- Attachments

DATE _____

FIXED FACILITY CHECKLIST

[] PRECONSTRUCTION [] NEW [] MODIFIED FACILITY

Section A -- General Information

1. SCIF Data: Organization/Company Name: _____
 SCIF Identification Number (if applicable): _____
 Organization subordinate to (If applicable): _____
 Contract Number & Expiration Date: _____
 CSA: _____
 Project Headquarter Security Office (if applicable): _____
2. SCIF Location: _____
 Street Address: _____

 Bldg Name/#: _____ Floor: _____
 Room(s) No: _____
 City: _____ State/Country: _____
 ZIP Code: _____
3. Responsible Security Personnel:
 Primary: _____ Alternate: _____
 Commercial Telephone: _____
 DSN Telephone: _____
 Secure Telephone: Type: _____
 Home Telephone: _____
 Fax No: (specify both classified and unclassified)
 Classified: _____ Unclassified: _____
 Other: _____
4. Accreditation Data:
 - a. Category of SCI Requested: _____
 Indicate the storage required:
 _____ Open Storage _____ Closed Storage _____ Continuous Operation
 _____ Secure Working Area _____ Temporary Secure Working Area
 - b. Existing Accreditation Information (If applicable):
 1. (1) Category of SCI:

 2. (2) Accreditation granted by:

 on _____
 - c. Last TEMPEST Accreditation (if applicable): Accreditation granted
 by: _____ on _____
 - d. If Automated Information Systems (AISs) are used, has an accreditation
 been granted? _____ YES _____ NO
 Accreditation granted by: _____ on _____
 - e. SAP co-located within SCIF? _____ YES _____ NO

Obtained via FOIA by Judicial Watch, Inc.

(If Yes, Classification: _____, and provide copy of Co-utilization Agreement for SAP operation in SCIF.)

f. Duty Hours: _____ hours to hours, _____ days per week.

g. Total square feet SCIF occupies: _____

5. Construction/modification: Is construction or modification complete?
_____ YES _____ NO _____ N/A (If NO, expected date of completion)

6. Inspections:

a. TSCM Service completed by _____ on _____
(Attach copy of report)
Were deficiencies corrected? _____ YES _____ NO _____ N/A
(If NO, explain:) _____

b. Last Physical Security Inspection by _____ on _____
(Attach copy of report)
Were deficiencies corrected? _____ YES _____ NO _____ N/A
(If NO, explain:) _____

c. Last Security Assistance visit by _____ on _____

7. REMARKS: _____

Section B -- Peripheral Security

8. Describe building exterior security:

a. Fence: _____

b. Fence Alarm: _____

c. Fence lighting: _____

d. Television (CCTV): _____

e. Guards: _____

f. Other: _____

9. Building:

1. Construction type: _____

2. Describe Access Controls: _____

(1) Continuous: _____ YES _____ NO

(2) If NO, during what hours? _____

10. Remarks: _____

Section C -- SCIF Security

Obtained via FOIA by Judicial Watch, Inc.

11. How is access to the SCIF controlled?

a. By Guard Force: YES NO Security Clearance Level: _____b. By Assigned Personnel: YES NOc. By Access Control Device: YES NO

If yes, Manufacturer _____ Model No _____

12. Does the SCIF have windows? YES NOa. How are they acoustically protected (If applicable) _____
_____b. How are they secured against opening? _____
_____c. How are they protected against visual surveillance? (If applicable) _____
_____13. Do ventilation ducts penetrate the SCIF perimeter? YES NOa. Number and size (Indicate on floor plan): _____

b. If over 96 square inches, type of protection used:

1. IDS: YES NO (Describe in Section E)2. Bars/Grills Metal Baffles: YES NO_____
OTHER - Explain: _____

c. Metal Duct Sound Baffles: Are ducts equipped with:

1. Metal Baffles: YES NO2. Noise Generator: YES NO3. Non-Conductive Joints: YES NO4. Inspection Ports: YES NO▪ If YES, are they within the SCIF? YES NO▪ If they are located outside of the SCIF, how are they secured?
_____d. If TEMPEST accreditation authority requires; are pipes, conduits, etc.,
penetrating the SCIF equipped
with non-conductive unions at the point they breach the SCIF perimeter? _____
YES _____ NOAre they provided acoustical protection? (if applicable) YES NO

14. Construction:

a. Perimeter walls:

1. Material & Thickness: _____

2. Do the walls extend from the true floor to the true ceiling?
_____ YES _____ NO

b. True ceiling (material and thickness): _____

c. False ceiling? _____ YES _____ NO If yes:

1. Type of ceiling material:

2. Distance between false and true ceiling:

d. True floor (material and thickness): _____

e. False Floor? _____ YES _____ NO If yes:

o Distance between false and true floor: _____

15. Remarks: _____

Section D -- Doors

16. Describe SCIF Primary Entrance Door (Indicate on floor plan): _____

Is an automatic door closer installed? _____ YES _____ NO

If NO, explain: _____

17. Describe number and type of doors used for SCIF emergency exits and other perimeter doors (Indicate on floor plan): _____

Is an automatic door closer installed? _____ YES _____ NO

If NO, explain: _____

18. Describe how the door hinges exterior to the SCIF are secured against removal (if in an uncontrolled area): _____

19. Locking devices:

a. Perimeter SCIF Entrance Door:

1. List manufacturer, model number and Group rating: _____

2. Does entrance door stand open into an uncontrolled area?
_____ YES _____ NO If YES, describe tamper protection: _____

b. Emergency Exits and Other Perimeter Doors:
Describe (locks, metal strip/bar, deadbolts, panic hardware): _____

c. Where are the door lock combinations filed? _____

20. Remarks: _____

Section E -- Intrusion Detection Systems

Give manufacturer and model numbers in response to following questions:

21. Method of Interior Motion Detection Protection:

a. Accessible Perimeter? _____
Storage Areas? _____

b. Motion Detection Sensors (Indicate on floor Plan): _____
Tamper protection: _____ YES _____ NO

c. Other (e.g. CCTV, etc.): _____

22. Door and Window Protection (Indicate on floor plan):

a. Balanced Magnetic Switch (BMS) on door?: _____
Tamper protection: _____ YES _____ NO

b. If SCIF has ground floor windows, how are they protected? _____

c. Other (e.g. CCTV, etc.): _____

23. Method of ventilation and duct work protection: _____

24. Space above false ceiling (only outside the United States, if required):

a. Motion Detection Sensors: _____
Tamper protection: _____ YES _____ NO

b. Other (e.g. CCTV): _____

25. Space below false floor only outside the United States, if required):

a. Motion Detection Sensors: _____
Tamper protection: _____ YES _____ NO

b. Other (e.g. CCTV): _____

26. IDS transmission line security protection:

a. Electronic line supervision (Manufacture and Model): _____

Obtained via FOIA by Judicial Watch, Inc.

If electronic line supervision. class of service: _____ I _____ II

b. Other: _____

27. Is emergency power available for the IDS? _____ YES _____ NO

TYPE: _____ Battery _____ Emergency Generator _____ Other

28. Where is the IDS control unit for the SCIF located (Indicated on floor plan)?

29. Where is the IDS Alarm enunciator panel located (Indicate on floor plan, Address)?

30. IDS Response Personnel: Describe: _____

Response Force Security Cleared: _____ YES _____ NO

a. Level: _____

b. Emergency Procedures documented? _____ YES _____ NO

c. Reserve Force available? _____ YES _____ NO

d. Response time required for alarm condition: _____ minutes.

e. Are response procedures tested and records maintained?

_____ YES _____ NO

If no, explain: _____

31. Is the IDS tested and records maintained? _____ YES _____ NO

If no, explain: _____

32. Remarks: _____

Section F -- Telephone System

33. Method of on-hook security provided:

a. TSG-2 Computerized Telephone System (CTS)? _____ YES _____ NO

1. Manufacturer/Model: _____

2. Location of the CTS: _____

3. Do the CTS installers and programmer have security clearances?

_____ If yes, at what access level (minimum established by CSA):

_____ If no, are escorts provided? _____

4. Is the CTS installed as per TSG-2 Configuration Requirements?

Obtained via FOIA by Judicial Watch, Inc.

 YES NO

- a. If no, provide make and model number of telephone equipment, explain your configuration, and attach a line drawing?

- b. Is access to the facility housing the switch controlled?
 YES NO

- c. Are all lines between the SCIF and the switch in controlled spaces?
 YES NO

5. Does the CTS use remote maintenance and diagnostic procedures or other remote access features? YES NO
If yes, explain those procedures: _____

- b. TSG-6 approved telephones?

1. Manufacturer/Model: _____

2. TSG number: _____

3. Ringer Protection (if required):

- c. TSG-6 approved disconnect devices?

1. Manufacturer/Model: _____

2. TSG number: _____

34. Methods of off-hook security provided:

- a. Is there a hold or mute feature? YES NO

1. If yes, which feature _____, and is it provided by the: _____
CTS?
or _____ Telephone?

2. If no, are approved push-to-operated handsets provided?
 YES NO
Describe:

35. Automatic telephone call answering:

- a. Is there an automatic call answering service for the telephones in the SCIF?
 YES NO

If yes, provide make and model number of the equipment, explain the configuration, and provide a line drawing.

Section G -- Acoustical Protection

- 40. Do all areas of the SCIF meet acoustical requirements? YES NO
If no, describe additional measures taken to provide minimum acoustical protection e.g. door, windows, etc) _____
- 41. Is the SCIF equipped with a public address, emergency/fire announcement or music system? YES NO
If yes, describe and explain how protected? _____
- 42. If any intercommunication system that is not part of the telephone system is used, describe and explain how protected: _____
- 43. Remarks: _____

Section H -- Administrative Security

- 45. Destruction Methods:
 - a. Describe method used for destruction of classified/sensitive material:
Manufacturer: _____ Model: _____
Manufacturer: _____ Model: _____
 - b. Describe location of destruction site(s) in relation to the secure facility: _____
 - c. Have provisions been made for the emergency destruction of classified/sensitive program material? (If required): YES NO
If YES, has the emergency destruction equipment and plan been coordinated with the CSA? YES NO
- 46. If reproduction of classified/sensitive material takes place outside the SCIF, describe equipment and security procedures used to reproduce documents: _____
- 47. Remarks: _____

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) 6/9

ANNEX B - Intrusion Detection Systems (IDS)^[4][4]

(Effective 18 November 2002)

This annex sets forth the requirements and establishes the Standard for Intrusion Detection Systems (IDS) and associated operations for Government and Government-Sponsored Sensitive Compartmented Information Facilities (SCIFs). Compliance with these requirements is mandatory for all SCIFs established after the effective date of this annex.

1.0 IDS Overview

The IDS shall detect attempted or actual unauthorized human entry into a SCIF. The IDS complements other physical security measures. The IDS shall consist of three distinct components: Intrusion Detection Equipment (IDE), Security and Response-Force Personnel, and Security Operation Procedures. IDS operations shall comprise four phases as described below:

1.1 Detection Phase. The detection phase begins when a sensor reacts to the stimuli for which the sensor was designed to detect.

1.2 Reporting Phase. The Premise Control Unit (PCU) receives signals from all associated sensors in the SCIF's alarmed zone and establishes the alarm status. The alarm status is immediately transmitted to the Monitoring Station. Within the Monitoring Station, a dedicated Alarm-Monitoring panel (or central processor) monitors incoming PCU signals. On receiving an alarm signal, a Monitoring Station's enunciator generates an audible and visible alarm for the monitoring personnel.

1.3 Assessment Phase. The assessment phase is the initial phase requiring human interaction. On receiving an audible or visible alarm, monitoring personnel immediately assess the situation and determine the appropriate response.

1.4 Response Phase. The response phase begins immediately after the operator has assessed the alarm condition. All alarms shall be immediately investigated. During the response phase, the precise nature of the alarm shall be determined and appropriate measures taken to safeguard the SCIF.

2.0 Definitions

2.1 Alarm. An alarm is a visual and audible indication that a sensor has detected the entry or attempted entry of an unauthorized person into a SCIF. Alarms also signify the malfunction of a sensor that normally causes such an alarm.

2.2 Alarm Zone. An alarm zone is a segregated or specified area under the control of a single Premise Control Unit (PCU).

2.3 Intrusion Detection Equipment (IDE). IDE is all the equipment, associated software/firmware, and communication lines included within the IDS.

2.4 Monitoring Station. The monitoring station is the central point for collecting alarm status from the PCUs handling the alarm zones under control of an IDS.

2.5 Premise Control Unit (PCU). A PCU is a device that receives changes of alarm status from IDS sensors, and transmits an alarm condition to the monitoring station.

2.6 Security in-depth. A determination by the Cognizant Security Authority (CSA) that a facility's security programs consist of layered and complementary controls sufficient to deter

Obtained via FOIA by Judicial Watch, Inc.

and detect unauthorized entry and movement within the areas adjacent to the SCIF.

2.7 Sensor. Sensors are devices that respond to a physical stimulus (as heat, light, sound, pressure, magnetism, or a particular motion) and transmits a resulting impulse.

2.8 United States. As used herein, the United States includes the 48 contiguous states, Alaska, Hawaii, as well as, protectorates, territories, and possessions under control of the United States (for example, Puerto Rico, Guam, Wake, Midway, American Samoa, US Virgin Islands, others). This definition does not include US-controlled installations (for example, military bases, embassies, leased space) located in foreign countries.

3.0 IDS Requirements

This section specifies the requirements for Intrusion Detection Systems (IDS) and associated operations for government and government-sponsored SCIFs and other associated areas.

3.1 General IDS Requirements. The following general requirements apply to all SCIFs and shall be met as a prerequisite for using a SCIF for government-classified operations.

3.1.1 SCIF Protection. All areas of a SCIF that reasonably afford access to the SCIF, or where SCI is stored, shall be protected by an IDS, unless continuously occupied. If the occupants of a continuously occupied SCIF cannot observe all potential entrances to the SCIF, the SCIF shall be equipped with a system to alert occupants of intrusions into the SCIF. This alerting system shall consist of Balance Magnetic Switches (BMS) (see paragraph 3.2.1.4) or other appropriate sensors. IDE and cabling associated with the alerting system shall not extend beyond the perimeter of the SCIF. Emergency exit doors shall be monitored 24 hours a day to provide quick identification and response to the appropriate door when there is an alarm indication (see paragraph 6.1.3).

3.1.2 Independent IDE and IDS. SCIFs shall be provided with IDE and alarm zones that are independent from systems safeguarding other protected sites. If a single monitoring station supervises several alarm zones, then the audible and visible annunciation for each such zone shall be distinguishable from other zones. The IDS's PCU, associated sensors, and cabling protecting the SCIF, shall be separate from and independent of fire, smoke, radon, water, and other such systems. (Note: If an access control system is integrated into an IDS, reports from the access control system shall be subordinate in priority to reports from intrusion alarms.)

3.1.3 Security During Catastrophic Failure of IDS. If any of the components of an IDS encounters a catastrophic failure to the extent that the IDS can no longer provide essential security services, then SCIF indoctrinated personnel shall provide security by physically occupying the SCIF until the IDS returns to normal operation. As an alternative, the outside SCIF perimeter shall be continuously protected by the response force or a guard force until the IDS returns to normal operation. If neither of these alternatives is possible, a catastrophic failure plan shall be submitted in writing to the CSA for review and approval prior to implementation. (See paragraph 6.1.2.) Examples of catastrophic failure are: loss of line security/communication, loss of alarm services, inoperability of IDS, loss of both primary and emergency power, or other such failure.

3.1.4 Safeguarding IDE, IDS Plans, Key Variable(s), and Passwords. System administration key variables and operational passwords shall be protected and shall be restricted to SCI-indoctrinated personnel. In areas outside of the United States,

Obtained via FOIA by Judicial Watch, Inc.

procured IDE shall remain solely under US control, or as otherwise authorized by the CSA in writing. Details of the IDS installation plans shall be controlled and restricted on a need-to-know basis.

3.1.5 IDE Acceptability. All IDE must comply with UL-2050 or equivalent as approved by the CSA in writing. Prior acceptance by the CSA does not constitute approval for use within another SCIF. Contractors shall comply with UL 2050 by maintaining an active UL certificate of installation and service. With sufficient justification, the CSA may issue written waivers to UL 2050. Any IDE that could allow unintentional audio or other intelligence-bearing signals in any form to pass beyond the confines of the SCIF is unacceptable and prohibited for IDS installation. IDE shall not include audio or video monitoring without appropriate countermeasures and CSA approval. IDS comprised of IDE with auto-reset features shall have the auto-reset capability disabled as required in paragraph 3.2.7.

3.1.6 IDS Approval. The CSA shall approve IDS proposals and plans prior to installation within a SCIF as part of the initial SCIF construction approval process. Final IDS acceptance tests as described herein and as prescribed in applicable manufacturer's literature shall be included as part of the SCIF accreditation package. Accreditation files for the SCIF shall be maintained as described in paragraph 6.3. The CSA shall approve the IDS prior to use for government or government-sponsored SCIFs.

3.2 Detailed IDS Requirements. The following detailed requirements apply to all SCIF IDSs.

3.2.1 Sensors. All sensors protecting a SCIF shall be located within that SCIF. Any failed IDE sensor shall cause an immediate and continuous alarm condition until the failure is corrected or compensated.

3.2.1.1 Motion Detection Sensors. All areas of a SCIF that reasonably afford access to the SCIF, or where SCI is stored, and that are not accredited for continuous operation shall be protected with UL-listed, equivalent or CSA approved motion detectors (see paragraph 3.1.1). Sufficient detectors shall be installed to assure meeting the requirements of paragraph 4.2.1. Within the US motion detection sensors are normally not required above false ceilings or below false floors; however, these detectors may be required by the CSA for such areas outside of the US.

3.2.1.2 Entrance Door Delay. Entrance door sensors may have an initial time delay built into the IDS to allow for change in alarm status, but shall not exceed 30 seconds.

3.2.1.3 SCIF Perimeter Sensors. With CSA approval, sensors supporting the external SCIF perimeter and perimeter equipment (if used) may be connected to the SCIF IDS provided the lines are installed on a separate zone and routed within grounded conduit.

3.2.1.4 Perimeter Door Sensor. Each SCIF perimeter door shall be protected by a Balanced Magnetic Switch (BMS) installed in accordance with section 4.1.2.

3.2.1.5 Emergency Exit-Door Detectors. The BMS installed on emergency exit doors shall be monitored 24 hours a day.

Obtained via FOIA by Judicial Watch, Inc.

3.2.1.6 Dual-Technology Sensors. The use of dual-technology sensors is authorized when each technology transmits alarm conditions independent from the other technology.

3.2.2 Premise Control Units and Access Control Switches. PCUs shall be located within the SCIF to assure that only SCIF personnel can initiate a change between *access* and *secure* mode. The means of changing between access and secure modes shall be located within the SCIF. Operation of the access/secure switch shall be restricted by using a device or procedure that verifies authorized PCU use. Any polling from the monitoring station to the PCU shall not exceed six minutes regardless of access state.

3.2.3 Communications between Sensors and the PCU. Cabling between the sensors and the PCUs shall be dedicated to the IDE and contained within the SCIF. Alternately, if the wiring cannot be contained within the SCIF, such cabling shall meet the transmission requirements of paragraph 3.2.8. All IDE cabling internal to the SCIF shall comply with national and local code standards. If applicable, the cabling shall be installed in accordance with TEMPEST and COMSEC requirements. Outside of the United States, if determined by the CSA, wiring will be protected within a closed conveyance. The use of wireless communications between sensors and PCU is normally prohibited. However, under exceptional circumstances, when such cabling is not possible or feasible, the wireless communications maintain continuous connection and are impervious to jamming, manipulation, and spoofing and meets other security requirements of this annex, the CSA may authorize in writing the use of wireless communications between sensors and the PCU. Co-utilizing agencies shall be notified of any such exception.

3.2.4 Monitor Station and Panel. Alarm status shall be provided at the monitoring station. The alarm-monitoring panel shall be designed and installed in a location that prevents observation by unauthorized persons. If an Access Control System (ACS) is integrated with an IDS, reports from the ACS shall be subordinate in priority to reports from intrusion alarms (see paragraph 3.1.2).

3.2.5 Alarms. Alarm annunciations shall exist for the below listed alarm conditions. A false/nuisance alarm is any alarm signal transmitted in the absence of a detected intrusion such as alarms caused by changes in the environment, equipment malfunction, operator failure, animals, electrical disturbances, or other such causes. False/nuisance alarms shall not exceed one alarm per 30-day period per zone (see paragraph 5.3.3).

3.2.5.1 Intrusion Alarm. An intrusion or attempted intrusion shall cause an immediate and continuous alarm condition.

3.2.5.2 Failed-Sensor Alarm. A failed IDE sensor shall cause an immediate and continuous alarm condition.

3.2.5.3 Maintenance Alarm. The IDS, when in the maintenance mode, shall cause an immediate and continuous alarm (or maintenance message) throughout the period the IDS is in the maintenance mode. Zones that are shunted or masked shall also cause such an alarm. (See paragraph 3.2.10.3 for additional requirements.)

3.2.5.4 Tamper Alarm. The IDS, when sustaining tampering, shall cause an immediate and continuous alarm. (See paragraph 3.2.12 for additional requirements.)

Obtained via FOIA by Judicial Watch, Inc.

3.2.5.5 Failed/Changed Electrical Power Alarm. Equipment at the monitoring station shall visibly and audibly indicate a failure in a power source, a change in power source, and the location of the failure or change. (See paragraph 3.2.11.2 for additional requirements.)

3.2.6 IDS Event (Alarm) Log. The IDS shall incorporate within the SCIF and at the monitoring station, a means for providing a historical record (items specified in paragraph 6.2.2) of all events through an automatic logging system. If the IDS has no provision of automatic entry into archive, as an alternative, a manual logging system shall be maintained in accordance with paragraph 6.2.2.

3.2.7 Alarm Reset. All alarm activations shall be reset by SCI-indoctrinated personnel. An IDS with an auto-reset feature shall have the auto-reset feature disabled.

3.2.8 External Transmission Line Security. When any IDS transmission line leaves a SCIF, line security shall be employed. The UL 2050 certificate shall state that line security has been employed. The following types of line security are acceptable:

3.2.8.1 Encrypted Lines. Encrypted-line security is achieved by using an approved 128-bit (or greater) encryption algorithm. The algorithm shall be certified by NIST or another independent testing laboratory.

3.2.8.2 Alternative Lines. If the communication technology described in 3.2.8.1 is not available, the SCIF owner and the CSA shall coordinate an optional supervised communication scheme. The communication scheme shall be adequately supervised to protect against modification and substitution of the transmitted signal.

3.2.9. Networked IDSs. In those cases in which an IDS has been integrated into a LAN or WAN, the following requirements shall be met. (See paragraphs 5.3.5 and 5.5.3.)

3.2.9.1 Dedicated IDS (Host) Computer. The IDS application software shall be installed and run on a host computer dedicated to security systems. The host computer shall be located in an alarmed area controlled at the SECRET or higher level.

3.2.9.2 IDS Host Computer Communications. All host computer communications to the LAN/WAN shall be protected through firewalls, or similar enhancements, that are configured to only allow data transfers between IDS components.

3.2.9.3 User IDs and Passwords. A unique user ID and password is required for each individual granted access to the IDS host computer. Passwords shall be a minimum of eight characters; consist of alpha, numeric, and special characters; and shall be changed a minimum of every six months.

3.2.9.4 Computer Auditing and Network Intrusion Detection. Computer auditing and network intrusion detection software (NIDS) shall monitor and log access attempts and all changes to IDS applications. Additionally, NIDS and IDS administrators shall be immediately notified of unauthorized modifications. The NIDS administrator shall possess a minimum of a TOP SECRET clearance and IDS system administrator shall be SCI-indoctrinated.

3.2.9.5 LAN/WAN Transmissions. All transmissions of IDS information over the

Obtained via FOIA by Judicial Watch, Inc.

LAN/WAN shall be encrypted using a NIST-approved algorithm with a minimum of 128-bit encryption.

3.2.9.6 Remote Terminals. Remote networked IDS terminals shall meet the following requirements: (a) Remote terminals shall be protected within a SCIF. (b) SCI-indoctrinated personnel shall ensure that personnel with access to the remote terminal are not able to modify Intrusion Detection System/Access Control System (IDS/ACS) information for areas for which they do not have access. (c) Each remote terminal shall require an independent user ID and password in addition to the host login requirements. (d) Network intrusion detection and auditing software shall log and monitor failed logins and IDS/ACS application program modifications.

3.2.10 IDS Modes of Operation. The IDS shall have three modes of operation: access mode, secure mode, and maintenance mode as described below. A fourth mode "Remote Service Mode" shall not exist unless the requirements of 3.2.10.4 are met. There shall be no capability for changing the mode of operation or access status of the IDS from a location outside the SCIF unless SCIF personnel conduct a daily audit of all openings and closings. Changing Access/Secure status of a SCIF shall be limited to SCI indoctrinated personnel. IDS modes shall meet the following requirements.

3.2.10.1 Access Mode. During access mode, normal authorized entry into the facility in accordance with prescribed security procedures shall not cause an alarm. Tamper and emergency exit door circuits shall remain in the secure mode of operation.

3.2.10.2 Secure Mode. In the secure mode, any unauthorized entry into the SCIF shall cause an alarm to be immediately transmitted to the monitoring station.

3.2.10.3 Maintenance Mode and Zone Shunting/Masking. When an alarm zone is placed in the maintenance mode, a signal for this condition shall be automatically sent to the monitoring station. This signal shall appear as an alarm (or maintenance message) at the monitoring station and shall continue to be displayed visibly at the monitoring station throughout the period of maintenance. The IDS shall not be securable while in the maintenance mode. All maintenance periods shall be archived in the system. The CSA may require that a maintenance Personal Identification Number (PIN) be established and controlled by SCI personnel. Additionally, a shunted or masked zone or sensor shall be displayed as such at the monitoring station throughout the period the condition exists. (See paragraph 6.2.3 for logging requirements.)

3.2.10.4 Remote Service Mode. After the initial installation, the capability for remote diagnostics, maintenance, or programming of IDE shall not exist unless accomplished only by appropriately SCI-indoctrinated personnel and shall be appropriately logged or recorded in the Remote Service Mode Archive. A self-test feature shall be limited to one second per occurrence. (See paragraph 5.5.4.)

3.2.11 Electrical Power. Primary electrical power for all IDE shall be commercially supplied in alternating current (AC) or direct current (DC) form. In the event such commercial power fails, the IDE shall automatically transfer to an emergency electrical power source without causing an alarm indication.

3.2.11.1 Emergency Backup Electrical Power. Emergency backup electrical

Obtained via FOIA by Judicial Watch, Inc.

power for the SCIF and monitoring station shall be provided by battery, generator, or both. If batteries are provided for emergency backup power, they shall provide a minimum of 24 hours (UL 1076) of backup power and they shall be maintained at full charge by automatic charging circuits. (See paragraph 5.3.4.)

3.2.11.2 Electrical Power Source and Failure Indication. An audible or visual indicator at the PCU shall provide an indication of the electrical power source in use (AC or DC). Equipment at the monitoring station shall visibly and audibly indicate a failure in a power source, a change in power source, and the location of the failure or change.

3.2.12 Tamper Protection. All IDE within the SCIF with removable covers shall be equipped with tamper detection devices. The tamper detection shall be monitored continuously whether the IDS is in the access or secure mode of operation.

4.0 Installation and Acceptance Testing Requirements

This section specifies the requirements for IDS installation and testing. Additionally, IDE installation and testing shall meet the following requirements.

4.1 Installation Requirements. The IDE shall be installed in a manner that assures conformance with all requirements of sections 3.1 and 3.2 of this standard and the following specific requirements. US citizens shall accomplish all IDE installation. Non-US citizens shall not provide these services without prior written approval by the CSA.

4.1.1 Motion Detector Installation. Motion detection equipment shall be installed in accordance with manufacturer specifications, UL, or equivalent standards.

4.1.2 Perimeter Door-Open Sensor Installation. SCIF perimeter door-open BMSs shall be installed so that an alarm signal initiates before the non-hinged side of the door opens beyond the thickness of the door from the seated position. That is, the sensor initiates after the door opens 1¼ inch for a 1¾ inch door.

4.2 Acceptance Testing. The IDE shall be tested to provide assurances that it meets all requirements of sections 3.1 and 3.2 of this standard and those detailed tests specified below. All SCIF IDS sensors shall be tested and found to meet the requirements herein prior to SCIF accreditation. Records of testing and test performance shall be maintained in accordance with paragraph 6.2.1. US citizens shall accomplish all IDE testing. Non-US citizens shall not provide testing services without prior written approval by the CSA.

4.2.1 Motion Detection Sensor Testing. Test all motion detection sensors to ensure that the sensitivity is adjusted to detect an intruder who walking toward/across the sensor at a minimum of four consecutive steps at a rate of one step per second. That is, 30 inches ± 3 inches or 760 mm ± 80 mm per second. The four-step movement shall constitute a "trial." An alarm shall be initiated in at least three out of every four such consecutive "trials" made moving progressively through the SCIF. The test is to be conducted by taking a four-step trial, stopping for three to five seconds, taking a four-step trial, stopping for three to five seconds, repeating the process throughout the SCIF. Whenever possible, the direction of the next trial is to be in a different direction.

4.2.2 BMS Testing. All BMSs shall be tested to ensure that an alarm signal initiates before the non-hinged side of the door opens beyond the thickness of the door from the seated position. That is, the sensor initiates after the door opens 1¼ inch for a 1¾ inch

door.

4.2.3 Tamper Testing. Remove each IDE cover individually and ensure that there is an alarm indication on the monitoring panel in both the secure and access modes. Tamper detection devices need only be tested upon installation with the exception of the tamper detection on the PCU that is activated when it is opened. The CSA may require more frequent testing of tamper circuits. (See paragraph 5.4 for tamper testing of PCU.)

4.2.4 Manufacturer's Prescribed Testing. All tests prescribed in manufacture's literature shall be conducted to assure that the IDE operates in accordance with manufacture's specifications and applicable requirements specified herein.

5.0 Operation, Maintenance, and Semi-Annual Testing Requirements

The IDS shall be operated and maintained to assure that the requirements of sections 3.1 and 3.2 of this standard are met. Additionally, IDE operation and maintenance shall meet the following requirements.

5.1 Monitoring.

5.1.1 Monitoring Station Staffing. The monitoring station shall be continuously supervised and operated by US citizens who have been subjected to a trust-worthiness determination (favorable NAC with no clearance required). Non-US citizens shall not provide these services without prior written approval by the CSA.

5.1.2 Monitoring Station Operator Training. Monitoring station operators shall be trained in IDE theory and operation to the extent required to effectively interpret incidents generated by the IDE and to take proper action when an alarm activates.

5.2 Response.

5.2.1 Alarm-Condition Response. All alarms shall be investigated and the results documented. Every alarm condition shall be considered a detected intrusion until resolved. The response force shall take appropriate steps to safeguard the SCIF as permitted by a written support agreement (see paragraph 6.1.3), local law enforcement, and circumstances surrounding the event until properly relieved (see paragraph 5.5.6). An SCI-indoctrinated individual must arrive as soon as possible, but not to exceed 60 minutes, to conduct an internal inspection of the SCIF, attempt to determine the probable cause of the alarm activation and reset the IDS prior to the departure of the response force. For SCIFs located within the US, the response force shall arrive at the SCIF within:

- Open Storage-five minutes without security in-depth
- Open Storage-15 minutes with security in-depth; and
- Closed Storage-15 minutes (up to 30 minutes with security in-depth and CSA approval)

For SCIFs located outside of the United States, security in-depth must be used and cleared or US Government personnel shall arrive at the SCIF within:

Obtained via FOIA by Judicial Watch, Inc.

- Open Storage-five minutes; and
- Closed Storage-10 minutes.

5.2.2 Response-Force Personnel Training and Testing. Response Force Personnel shall be appropriately trained and equipped according to SOPs to accomplish initial or follow-up response to situations that may threaten the SCIF's security. Such personnel may include local law enforcement support or other external forces as stated in formal agreements. Coordinated response force testing shall be conducted semi-annually. False alarm activations may be used in lieu of a response-force test provided the proper response times were met. A record of response-force personnel testing shall be maintained for a minimum of two years.

5.3 Maintenance.

5.3.1 Maintenance Staffing. The IDE shall be maintained by US citizens who have been subjected to a trustworthiness determination (favorable NAC with no clearance required). Non-US citizens shall not provide these services without prior written approval by the CSA.

5.3.2 Sensor Adjustment or Replacement. Sensors that do not meet prescribed requirements shall be adjusted or replaced as needed to assure that the requirements of sections 3 and 4 of this standard are continually met.

5.3.3 False Alarm Prevention. The maintenance program for the IDS shall ensure that false-alarm incidents do not exceed one in a period of 30 days per alarm zone.

5.3.4 Emergency-Power Battery Maintenance. The battery manufacturer's periodic maintenance schedule shall be followed and the results documented.

5.3.5 Network Maintenance. If the IDS is connected to a network, the IDS and NIDS system administrator shall maintain configuration control, ensure the latest operating system security patches have been applied, and shall configure the operating system to provide a high level of security. (See paragraph 3.2.9.)

5.4 Semiannual IDE Testing. The IDE shall be tested semiannually (every six months) to provide assurances that the IDS is in conformance with the requirements of paragraphs 4.2.1 through 4.2.4. Records of semiannual testing and test performance shall be maintained in accordance with paragraph 6.2.1. US citizens shall accomplish all IDE testing. Non-US citizens shall not provide such testing services without prior written approval by the CSA.

5.5 Operational Requirements Limited to SCI Indoctrinated Personnel.

5.5.1 Changing Access/Secure Status. Changing Access/Secure status of the SCIF shall be limited to SCI-indoctrinated personnel.

5.5.2 Resetting Alarm Activations. All alarm activations shall be reset by SCI-indoctrinated personnel.

5.5.3 IDS Administrator. If the IDS is connected to a network, the IDS system administrator shall maintain configuration control, ensure the latest operating system security patches have been applied, and shall configure the operating system to provide a

high level of security.

5.5.4 Remote Operations. After initial installation, remote diagnostics, maintenance, or programming of the IDE shall not exist unless accomplished by SCI-indoctrinated personnel only and shall be appropriately recorded.

5.5.5 Auditing External Changes of Access Status. If access status is changed externally, a daily audit of all of openings and closings of the SCIF shall be accomplished by SCIF personnel. (See paragraph 3.2.10.)

5.5.6 Alarm-Response Internal Investigation. An SCI-indoctrinated individual shall arrive within 60 minutes to conduct an internal inspection of the SCIF, attempt to determine the probable cause of the alarm activation, and reset the IDS prior to the departure of the response force.

5.5.7 IDS Catastrophic Failure Coverage. In the case of IDS failure, SCIF indoctrinated personnel shall provide security by physically occupying the SCIF until the IDS returns to normal operation. As an alternative, the outside SCIF perimeter shall be continuously protected by the response force or a guard force until the IDS returns to normal operation. If neither of these alternatives is possible, a catastrophic failure plan shall be submitted in writing to the CSA for review and approval prior to implementation. (See paragraph 6.1.2.)

6.0 Documentation Requirements

The following documentation shall be developed for the IDS. This documentation shall be made available to the CSA on request and shall be available within the SCIF.

6.1 Plans, Agreements, and Standard Operating Procedures (SOP).

6.1.1 IDS Plans. The IDS design and installation documentation shall be provided to the government sponsoring activity and maintained in the SCIF as specified in paragraph 3.1.4.

6.1.2 Catastrophic Failure Plan. If an alternative catastrophic failure plan is contemplated (see paragraph 3.1.3), the plan shall be submitted in writing to the CSA for review and approval prior to implementation.

6.1.3 Support Agreement. A written support agreement shall be established for external monitoring, response, or both. The agreement shall include the response time for both response force and SCIF personnel, responsibilities of the response force upon arrival, maintenance of SCIF points of contact, and length of time response personnel are required to remain on-site.

6.1.4 Monitoring Operator SOP. The duties of the monitor operator shall be documented in a SOP. The SOP shall include procedures for observing monitor panel(s) for reports of alarms, changes in IDE status, assessing these reports, and in the event of an intrusion alarm, dispatching the response force or notifying the proper authority to do so and notifying the appropriate authority of the event. [Note: These procedures shall state that the operator will not have any additional duties that may interfere with monitoring alarms, making assessments, and dispatching the response force.]

Obtained via FOIA by Judicial Watch, Inc.

6.1.5 Maintenance Access SOP. A written SOP shall be established to address the appropriate actions to be taken when maintenance access is indicated at the monitor-station panel. The SOP shall require that all maintenance periods shall be archived in the system.

6.2 Records, Logs, and Archives.

6.2.1 Test Records. A record of IDE testing shall be maintained within the SCIF. This record shall include: testing dates, names of individuals performing the test, specific equipment tested, malfunctions detected, and corrective actions taken. Records of the response-force personnel testing shall also be retained. All records of testing shall be maintained for a minimum of two years. (See paragraph 5.2.2.)

6.2.2 IDS Event (Alarm) Log. If the IDS has no provision for automatic entry into archive (see paragraph 3.2.6), the operator shall record the time, source, type of alarm, and action taken. The responsible security officer shall routinely review the historical record. Results of investigations and observations by the response force shall also be maintained at the monitoring station. The SCIF responsible security officer shall routinely review the historical record. Records of alarm annunciations shall be retained for a minimum of two years and longer if needed until investigations of system violations and incidents have been successfully resolved and recorded.

6.2.3 Annunciation of Shunting or Masking Condition Log. Shunting or masking of any zone or sensor shall be appropriately logged or recorded in an archive. (See paragraph 3.2.10.3.)

6.2.4 Maintenance Period Archives. All maintenance periods shall be archived into the system. (See paragraph 3.2.10.3.)

6.2.5 Remote Service Mode Archive. An archive shall be maintained for all remote service mode activities. (See paragraph 3.2.10.4.)

6.3 SCIF Accreditation File. IDS accreditation documentation shall be maintained on-site in the SCIF accreditation file. The following documents shall be included in the SCIF accreditation file along with other SCIF accreditation documentation: Final acceptance tests of original installation and any modifications; catastrophic failure plan (see paragraph 6.1.2); monitoring operator SOP (see paragraph 6.1.5); maintenance mode and remote service mode archives (see paragraphs 6.2.3 through 6.2.5); and, historical record of IDS logging (see paragraph 6.2.2). Final acceptance tests and the catastrophic failure plan shall be maintained in both the SCIF accreditation file and at the CSA location.

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 6/9

ANNEX C - Tactical Operations/Field Training

(Effective 27 May 1994)

This annex pertains to specialized Sensitive Compartmented Information Facilities (SCIFs)

Obtained via FOIA by Judicial Watch, Inc.

deployed in a tactical operations or field training environment. It is divided into three parts to reflect the accepted modes of tactical operation:

- Part I - Ground Operation
- Part II - Aircraft/Airborne Operation
- Part III - Shipborne Operation

Table of Contents

PART I GROUND OPERATION

- PURPOSE
- APPLICABILITY AND SCOPE
- RESPONSIBILITIES
- ACCREDITATION OF TACTICAL SCIFs
- PHYSICAL CONFIGURATION
- TACTICAL SCIF OPERATIONS USING VANS, SHELTERS, AND VEHICLES
- TACTICAL SCIF OPERATIONS WITHIN EXISTING PERMANENT STRUCTURES
- MOBILE SIGINT SCIFs
- SEMI-PERMANENT SCIFs
- ELECTRICAL POWER
- TEMPEST REQUIREMENTS
- TELEPHONE EQUIPMENT

PART II AIRCRAFT/AIRBORNE OPERATION

- PURPOSE
- APPLICABILITY
- RESPONSIBILITIES
- ACCREDITATION OF AIRCRAFT/AIRBORNE FACILITIES

- POST AND PATROL REQUIREMENTS
- ENTRY HATCHES
- TEMPEST REQUIREMENTS
- UNSCHEDULED AIRCRAFT LANDINGS
- VOICE TRANSMISSIONS
- DESTRUCTION REQUIREMENTS

PART III SHIPBOARD OPERATION

- PURPOSE
- APPLICABILITY AND SCOPE
- TYPES OF SHIPBOARD SCIFs (S/SCIFs)
- PERMANENT ACCREDITATION
- STANDARDS
- INTRUSION DETECTION SYSTEM (IDS)
- PASSING SCUTTLES AND WINDOWS
- LOCATION OF CRYPTOGRAPHIC EQUIPMENT
- SECURE STORAGE CONTAINERS
- TELEPHONES
- SECURE TELEPHONE UNIT-III (STU-III)
- SOUND POWERED TELEPHONES
- SCI INTERCOM ANNOUNCING SYSTEM
- SUPPORTING INTERCOMMUNICATION ANNOUNCING SYSTEMS
- COMMERCIAL INTERCOMMUNICATION EQUIPMENT
- GENERAL ANNOUNCING SYSTEMS
- PNEUMATIC TUBE SYSTEMS
- DESTRUCTION EQUIPMENT

- EMERGENCY POWER
 - SCI PROCESSING SYSTEMS
 - TEMPORARY ACCREDITATION
 - TEMPORARY SECURE WORKING AREAS (TSWAs)
 - EMBARKED PORTABLE SHIPBOARD COLLECTION VANS (PSCVs)
-

PART I GROUND OPERATION:

1.0 PURPOSE:

This Annex prescribes the procedures for the physical security requirements for the operation of a Sensitive Compartmented Information Facility (SCIF) while in a field or tactical configuration, including training exercises. It also addresses the standards for truck mounted or towed trailer style shelters designed for use in a tactical environment but used in a garrison environment known as a Semi-permanent SCIF (SPSCIF).

2.0 APPLICABILITY AND SCOPE:

Recognizing that field/tactical operations, as opposed to operations within a fixed military installation, are of the type considered least secure, the following minimum physical security requirements will be met and maintained. Situation and time permitting, these standards will be improved upon using the security considerations and requirements for permanent secure facilities as an ultimate goal. If available, permanent-type facilities will be used. Under field or combat conditions, a continuous 24-hour operation is mandatory. Every effort must be made to obtain the necessary support from the host command (e.g., security containers, vehicles, generators, fencing, guards, weapons, etc.).

2.1 The Tactical SCIF (T-SCIF) shall be located within the supported headquarters defensive perimeter and preferably, also within the Tactical Operations Center (TOC) perimeter.

2.2 The T-SCIF shall be established and clearly marked using a physical barrier. Where practical, the physical barrier should be triple-strand concertina or General Purpose Barbed Tape Obstacle (GPBTO). The Tactical SCIF approval authority shall determine whether proposed security measures provide adequate protection based on local threat conditions.

2.3 The perimeter shall be guarded by walking or fixed guards to provide observation of the entire controlled area. Guards shall be armed with weapons and ammunition. The types of weapons will be prescribed by the supported commander. Exceptions to this requirement during peace may only be granted by the T-SCIF approval authority based on local threat conditions.

2.4 Access to the controlled area shall be restricted to a single gate/entrance, which will be guarded on a continuous basis.

2.5 An access list shall be maintained, and access restricted to those people whose names appear

on the list.

2.6 The Tactical SCIF shall be staffed with sufficient personnel as determined by the on-site security authority based on the local threat conditions.

2.7 Emergency destruction and evacuation plans shall be kept current.

2.8 SCI material shall be stored in lockable containers when not in use.

2.9 Communications shall be established and maintained with backup response forces, if possible.

2.10 The SSO, or designee, shall conduct an inspection of the vacated Tactical SCIF area to ensure SCI materials are not inadvertently left behind when the T-SCIF moves.

2.11 Reconciliation of T-SCIF activation and operational data shall be made not more than 30 days after SCIF activation. Interim reporting of SCIF activities may be made to the CSA.

3.0 RESPONSIBILITIES:

The Cognizant Security Authority (CSA) is responsible for ensuring compliance with these standards and providing requisite SCI accreditation.. The CSA may further delegate T-SCIF accreditation authority one command level lower. The Senior Intelligence Officer (SIO) is responsible when a temporary field or Tactical SCIF is used in support of field training exercises. During a period of declared hostilities or general war, a T-SCIF may be established at any level of accreditation upon the verbal order of a General or Flag Officer Commander.

4.0 ACCREDITATION OF TACTICAL SCIFs:

4.1 An Accreditation Checklist shall not be required for establishment of a T-SCIF. Approval authorities may require use of a local tactical deployment checklist.

4.2 The element requesting establishment of a T-SCIF shall notify the CSA, or designee, prior to commencement of SCIF operations. The message shall provide the following information:

4.2.1 ID number of parent SCIF.

4.2.2 Name of the Tactical SCIF.

4.2.3 Deployed from (location).

4.2.4 Deployed to (location).

4.2.5 SCI level of operations.

4.2.6 Operational period.

4.2.7 Name of exercise or operation.

4.2.8 Identification of facility used for T-SCIF operations (e.g., vans, buildings, tents).

4.2.9 Points of contact (responsible officers).

4.2.10 Description of security measures for entire operational period of SCIF.

4.2.11 Comments.

5.0 PHYSICAL CONFIGURATION:

Obtained via FOIA by Judicial Watch, Inc.

A T-SCIF may be configured using vehicles, trailers, shelters, bunkers, tents, or available structures to suit the mission. Selection of a T-SCIF site should first consider effective and secure mission accomplishment.

6.0 TACTICAL SCIF OPERATIONS USING VANS, SHELTERS, AND VEHICLES:

6.1 When a rigid side shelter or portable van is used for SCI operations, it shall be equipped with either a combination lock that meets all requirements of Federal Specification FF-L-2740 or other CSA-approved lock. The combination to the lock or keys shall be controlled by the SSO at the security level for which the T-SCIF is accredited. The shelter or van shall be secured at all times when not activated as a SCIF.

6.2 The SCIF entrance of a radio frequency shielded enclosure designed for tactical operations may be secured with the manufacturer supplied locking device or any combination of the locking devices mentioned above.

7.0 TACTICAL SCIF OPERATIONS WITHIN EXISTING PERMANENT STRUCTURES:

7.1 A T-SCIF may be operated within an existing structure when:

7.1.1 Location is selected on a random basis.

7.1.2 The location is not reused within a 36 month period. If reused within 36 months for SCI discussion, a TSCM evaluation is recommended.

7.2 There is no restriction over SCI discussion within a T-SCIF during war.

8.0 MOBILE SIGINT SCIFs:

8.1 A continuous 24-hour operation is mandatory.

8.2 The T-SCIF shall be staffed with sufficient personnel as determined by the on-site security authority based on the local threat conditions.

8.3 External physical security measures shall be incorporated into the perimeter defense plans for the immediate area in which the T-SCIF is located.

8.3.1 A physical barrier is not required as a prerequisite to establish a mobile SIGINT T-SCIF.

8.3.2 External physical security controls will normally be a function of the people controlling the day-to-day operations of the T-SCIF.

8.4 Communications shall be established and maintained with backup guard forces, if possible.

8.5 Emergency destruction plans shall incorporate incendiary methods to ensure total destruction of SCI material in emergency situations.

8.6 A rigid side shelter or a portable van are two possible configurations that may be used.

8.6.1 When a rigid side shelter or portable van is used, it is subject to the following additional restrictions:

Obtained via FOIA by Judicial Watch, Inc.

8.6.1.1 If it is a shelter, it shall be mounted to a vehicle in such a way as to provide the shelter with the capability of moving on short notice.

8.6.1.2 A GSA-approved security container shall be permanently affixed within the shelter. The combination to the lock will be protected to the level of security of the material stored therein.

8.6.1.3 Entrance to the T-SCIF shall be controlled by SCI-indoctrinated people on duty within the shelter. When situations occur where there are no SCI-indoctrinated people within the shelter, i.e., during redeployment, classified material shall be stored within the locked GSA container and the exterior entrance to the shelter will be secured.

8.6.1.4 Entrance to the T-SCIF shall be limited to SCI-indoctrinated people with an established need-to-know whenever SCI material is used within the shelter.

8.6.2 When a rigid side shelter or portable van is not available and a facility is required for SCI operations, such as in the case of a soft side vehicle or man-portable system, it is subject to the following additional restrictions:

8.6.2.1 Protection will consist of an opaque container, i.e., leather pouch, metal storage box, or other suitable container that prevents unauthorized viewing of the material.

8.6.2.2 This container shall be kept in the physical possession of an SCI-indoctrinated person.

8.7 The quantity of SCI material permitted within the T-SCIF will be limited to that which is absolutely essential to sustain the mission. Stringent security arrangements shall be employed to ensure that the quantity of SCI material is not allowed to accumulate more than is absolutely necessary.

8.7.1 All working papers generated within the T-SCIF shall be destroyed at the earliest possible time after they have served their mission purpose to preclude accumulation of unnecessary classified material.

8.7.2 If AIS equipment is used to store or process SCI data, a rapid and certain means of destruction shall be available to AIS operators to ensure the total destruction of classified material under emergency or combat conditions.

8.8 Upon cessation of hostilities, all classified material shall be returned to the parent element of the SCIF for reconciliation of records and destruction of obsolete material.

9.0 SEMI-PERMANENT SCIFs:

9.1 Vehicles with mounted shelters or towed trailer type shelters, designed for field or tactical use, that are employed as tactical SCIFs when deployed may also be used as a SCIF in nontactical situations if the SIO determines there is a need for more SCIF area and time and/or funds are not available to construct or enlarge a permanent SCIF. These types of SCIFs are SEMI-PERMANENT SCIFs (SPSCIFs).

9.2 The SPSCIF shall be accredited and operated in the same manner as a permanent SCIF. Requirements for TEMPEST and AIS accreditation apply as well.

Obtained via FOIA by Judicial Watch, Inc.

9.3 The SPSCIF must be of rigid construction similar to a van, trailer, or transportable shelter. The construction material must be of such composition to show visible evidence of forced entry. Vents and air ducts must be constructed to prevent surreptitious entry. The doors must be solid construction and plumbed so the door forms a good acoustical seal. If installed, emergency exits and escape hatches must be constructed so they can only be opened from the interior of the SPSCIF.

9.4 The SPSCIF must be placed within a fenced compound on a military installation or equivalent, as determined by the CSA. The fence must be at least ten (10) feet from the SPSCIF and related building and equipment. The distance from the fence to the SPSCIF may have to be greater to provide acoustical security or to meet COMSEC or TEMPEST requirements. Access control to the fenced compound must be continuous.

9.5 All SPSCIFs must have a combination lock that meets all requirements of Federal Specification FF-L-2740 or other CSA approved lock. (NOTE: Just as with combinations, keys require protection equivalent to the information which they protect.)

9.6 SPSCIFs do not need any additional security measures if one of the following exists:

9.6.1 Continuous operations. Continuous operations exist when the SPSCIF is occupied by one or more SCI-indoctrinated persons 24 hours a day. When there are multiple vehicles/shelters within a fenced compound, only those occupied by one or more SCI-indoctrinated people qualify as continuous operations facilities.

9.6.2 Dedicated guard force who have been subjected to a trustworthiness determination (e.g., NAC with no clearance to be issued). The dedicated guard force must be present whenever the SPSCIF is not occupied and must have continuous surveillance of the SPSCIF entrances. The guard force must check the perimeter of the SPSCIF at least twice an hour at random intervals. Guard response time will be five minutes or less.

9.7 SPSCIFs not storing classified material and not meeting one of the requirements in the above paragraphs may be required to have an Intrusion Detection System (IDS) as prescribed in ANNEX B as required by the CSA.

9.8 Requirements for storage when unoccupied:

9.8.1 SCI material will not be stored in a SPSCIF except when removal is not feasible, i.e., computer hard disk.

9.8.2 Storage in the United States and Outside the United States. If the SPSCIF does not have continuous operations or a dedicated guard force, a combination lock that meets all requirements of Federal Specification FF-L-2740 or other CSA approved lock and an IDS for the SPSCIF interior is required. The interior SPSCIF IDS must be as prescribed in ANNEX B. The CSA may require exterior compound IDS.

10.0 ELECTRICAL POWER:

Electrical power supplied to T-SCIFs may be furnished by commercial or locally generated systems, as follows:

10.1 Tactical generator with access controls, including guards or surveillance of the generating equipment.

Obtained via FOIA by Judicial Watch, Inc.

10.1.1 The generating equipment shall be located within the protected perimeter of the organization supporting the T-SCIF. The generator shall not require location within the SCIF compound perimeter.

10.1.2 Generator operator and maintenance people shall be US citizens.

10.2 In general, RF filters or isolators are not required for TEMPEST protection of commercial AC (alternating current) power lines used for SCI processing equipment in a T-SCIF.

10.3 Filtering and isolation generators (an electrical motor coupled to a generator by non-conductive means) may be used to provide isolated electrical power to the SCIF. The motor generator location shall be within the SCIF compound perimeter.

11.0 TEMPEST REQUIREMENTS:

Authority for TEMPEST accreditation of all compartments of SCI processed in a Tactical SCIF is delegated to the CSA based on review by the Certified TEMPEST Technical Authority (CTTA).

12.0 TELEPHONE EQUIPMENT:

Telephone instruments used within a T-SCIF shall meet requirements outlined in the Telephone Security ANNEX. Restrictions contained within the Telephone Security ANNEX pertaining to SCIF telephone services do not apply to T-SCIF operations during war.

PART II AIRCRAFT/AIRBORNE OPERATION:

1.0 PURPOSE:

This annex prescribes the physical security procedures for the operation of a Sensitive Compartmented Information Facility (SCIF) for aircraft, including airborne missions.

2.0 APPLICABILITY:

This annex is applicable to all aircraft to be utilized as a SCIF. Existing or previously accredited facilities do not require modification to conform with these standards.

3.0 RESPONSIBILITIES:

The CSA is responsible for ensuring compliance with these standards and providing SCI accreditation. The CSA may delegate aircraft/airborne SCIF accreditation authority to the major command level.

The major command/organization Senior Intelligence Officer (SIO) is responsible when an aircraft is used as a temporary SCIF in support of field training exercises. During a period of declared hostilities or general war, an aircraft/airborne SCIF may be established at any level of accreditation upon the verbal order of a General or Flag Officer Commander. The major command/organization is responsible for ensuring compliance with this annex.

4.0 ACCREDITATION OF AIRCRAFT/AIRBORNE FACILITIES:

4.1 An accreditation checklist will not be required for the establishment of an aircraft/ airborne SCIF. Approval authorities may require use of a local deployment checklist, if necessary.

4.2 The element requesting establishment of an aircraft/airborne SCIF will notify the CSA prior to commencement of SCIF operations. The letter or message will indicate the following information:

- Name of aircraft/airborne SCIF
- Major command/organization
- ID number of parent SCIF, if applicable
- Deployed from (location) and dates
- Deployed to (location) and dates
- SCI level of operations
- Name of exercise or operation
- Points of Contact
- Type of Aircraft and area to be accredited as a SCIF
- Description of security measures for entire operational period of SCIF (SOP)

4.3 The SCIF will be staffed with sufficient personnel as determined by the on-site security authority based on the local threat environment.

4.4 SCI material will be removed from the aircraft on mission completion or at any landings, if feasible. When removal is not possible, or when suitable storage space/ locations are not available, two armed (with ammunition) SCI-indoctrinated personnel must remain with the aircraft to control entry to the SCIF. Waivers to the requirement for weapons and ammunition may be approved on a case-by-case basis by the Commander.

4.5 The SSO or senior SCI-cleared person will conduct an inspection of the vacated SCIF to ensure SCI materials are not left behind.

4.6 Aircraft that transport SCI material incidental to travel between airfields do not require accreditation. However, compliance with directives pertaining to security of SCI material and communications is mandatory.

5.0 POST AND PATROL REQUIREMENTS:

Accredited aircraft require perimeter access controls, a guard force, and a reserve security team.

5.1 Unless protected by an approved IDS, hourly inspections will be made of all hatches and seals (including seal numbers).

Obtained via FOIA by Judicial Watch, Inc.

5.2 A guard force and response team must be provided, capable of responding within five minutes if open storage is authorized. or 15 minutes for closed storage.

5.3 When aircraft are parked outside an established controlled area, a temporary controlled area must be established.

6.0 ENTRY HATCHES:

6.1 The aircraft commander or crew members will provide guard force personnel who have been subjected to a trustworthiness determination (e.g., NAC with no clearance to be issued) prior to departing from the immediate area of the aircraft.

6.2 All hatches will be locked to prevent unauthorized access. Hatches that cannot be secured from the outside will be sealed using serially numbered seals.

7.0 TEMPEST REQUIREMENTS:

Authority for TEMPEST accreditation of all compartments of SCI processed in an aircraft/airborne SCIF is delegated to the CSA, based on review by the Cognizant Certified TEMPEST Technical Authority (CTTA).

8.0 UNSCHEDULED AIRCRAFT LANDINGS:

8.1 US Military Bases: The local SSO or base security officer will be notified of the estimated arrival time and security protection required.

8.2 Other Airfields:

8.2.1 Within the United States, the local Federal Aviation Administration (FAA) Security Officer will be notified of the estimated arrival time and security protection required.

8.2.2 On arrival, the senior SCI-indoctrinated person is responsible for controlling entry and maintaining surveillance over the aircraft until all SCI material is secured in an accredited SCIF or the aircraft departs.

8.2.3 Any properly accredited US Government SCIF may be used for temporary storage of materials from the aircraft. If the facility is not accredited for the level of information to be stored, the material must be double wrapped with initialed seals and stored in a GSA-approved security container.

8.3 Unfriendly Territory:

If an aircraft landing in unfriendly territory is anticipated, all SCI material will be immediately destroyed, with the destruction process preferably taking place prior to landing.

8.3.1 When flights are planned over unfriendly territory, SCI to be carried on board will be selected by the intelligence mission personnel and consist of the absolute minimum required for mission accomplishment.

8.3.2 All personnel will rehearse emergency destruction before each mission. Such emergency preparation rehearsals will be made a matter of record.

9.0 VOICE TRANSMISSIONS:

SCI discussions will only be conducted via appropriately encrypted aircraft radio.

10.0 DESTRUCTION REQUIREMENTS:

10.1 An Emergency Action Plan (EAP) will be written that provides for the evacuation and/or destruction of classified material. Evacuation plans and destruction equipment must be approved by the CSA and tested by mission personnel 10.2 Emergency destruction and evacuation plans will be kept current.

PART III SHIPBOARD OPERATION:

1.0 PURPOSE:

This annex specifies the requirements for construction and security protection of SCIFs located on ships. The SCI accreditation checklist for ships may be obtained from the Director, Office of Naval Intelligence, 4301 Suitland Road, Washington, D.C. 20395.

2.0 APPLICABILITY AND SCOPE:

2.1 This annex is applicable to all new construction surface combatant ships. The application of this annex to surface non-combatants or sub-surface vessels will be referred to the CSA.

2.2 There may be instances in which circumstances constitute a threat of such proportion that they can only be offset by stringent security arrangements over and above those prescribed in this annex. Conversely, there may be instances in which time, location, mission, and/or condition of use of materials would make full compliance with these standards unreasonable or impossible. Such situations will be referred to the CSA for resolution on a case-by-case basis.

2.3 Existing or previously approved facilities do not require modification to conform with these standards

3.0 TYPES OF SHIPBOARD SCIFs (S/SCIFs):

3.1 Permanent S/SCIFs: An area aboard ship where SCI operations, processing, discussion, storage, or destruction takes place. The area will have a clearly defined physical perimeter barrier and continuous physical security safeguards. The area may contain one or more contiguous spaces requiring SCIF accreditation. This type S/ SCIF is routinely used during deployment and import operations.

3.2 Temporary S/SCIFs: An area aboard ship where temporary SCI operations, processing, discussion, storage, or discussion takes place. The area will have a clearly defined physical perimeter barrier and continuous physical security safeguards. The area may contain one or more contiguous spaces requiring SCIF accreditation. It will be continuously manned with sufficient SCI-cleared and -indoctrinated personnel, as determined by the on-site security authority based on the local threat environment, when SCI is present within the area. Temporary shipboard SCI operations will be limited to:

Obtained via FOIA by Judicial Watch, Inc.

3.2.1 A single deployment that will not exceed 12 months.

3.2.2 A single mission requiring SCI operations that cannot be defined in length of operational time.

3.2.3 During the period immediately preceding relocation of the ship to a refitting facility where the Temporary S/SCIF is scheduled for renovation and compliance with this annex. There will be a schedule established for renovation of the S/SCIF with confirmatory reporting of such to the CSA.

3.2.4 Temporary Platforms: A mobile or portable SCIF may be temporarily placed aboard a ship. Such platforms will be accredited on a temporary basis for a single deployment mission. The platform will be manned 24 hours a day by sufficient SCI-cleared and -indoctrinated personnel as determined by the on-site security authority. At the completion of the mission, the accreditation period will end and the CSA notified that the platform is certified clear and free of all SCI materials.

4.0 PERMANENT ACCREDITATION:

Ships requesting permanent accreditation status will provide to the CSA a complete inspection report and the Shipboard Inspection Checklist, certifying compliance with this Annex.

5.0 STANDARDS:

The physical security criteria for permanent S/SCIFs is as follows:

5.1 Physical Perimeter: The physical perimeter of an SCI space will be fabricated of structural bulkheads (aluminum or steel) with a thickness not less than 0.125 inch. Elements of the physical perimeter will be fully braced and welded in place.

5.2 Continuous SCI Spaces: Where several SCI spaces are contiguous to each other in any or all dimensions, the entire complex may be enclosed by a single physical perimeter barrier conforming to this annex.

5.2.1 Access to the SCI complex will be controlled by a single access door conforming to this annex. Each compartment within the complex may have a separate access door from within the common physical perimeter barrier. Such interior access control doors do not need to conform with this annex.

5.2.2 Access procedures will be established to ensure against cross-traffic of personnel not holding appropriate SCI access.

5.3 Normal Access Door: The normal access door will be a shipboard metal joiner door with honeycomb-core and fitted as specified below:

5.3.1 Where the normal access door is in a bulkhead that is part of an airtight perimeter, the airtight integrity may be maintained by colocating the airtight door with the metal joiner door, or by adding a vestibule.

5.3.2 The metal joiner door will be equipped with a combination lock that meets all requirements of Federal Specification FF-L-2740 or other CSA approved lock.

5.3.3 In addition to the lock, the door will be equipped with an access control device

5.3.4 The door will be constructed in a manner that will preclude unauthorized removal of hinge pins and anchor bolts, as well as to obstruct access to lock-in bolts between door and frame.

5.4 Emergency Exit: The emergency exit will be fabricated of aluminum plate or steel in accordance with this annex. The exit will be mounted in a frame braced and welded in place in a manner commensurate with the structural characteristics of the bulkhead, deck, or overhead in which it is situated.

5.5 Restriction on Damage Control Fittings and Cables: Because of the security restrictions imposed in gaining access to these spaces, no essential damage control fittings or cables will be located within or pass through an SCI space. This requirement is not applicable to damage control fittings, such as smoke dampers, that may be operated by personnel within the space during normal manning.

5.6 Removable Hatches and Deck Plates: Hatches and deck plates less than 10 square feet that are secured by exposed nuts and bolts (external to the SCI space) will be secured with externally attached, high security padlocks (unless their weight makes removal unreasonable). The padlock keys will be stored in a security container located within a space under appropriate security control.

5.7 Vent and Duct Barriers: Vents, ducts, or other physical perimeter barrier openings with a cross-sectional dimension greater than 96 square inches will be protected at the perimeter with a fixed barrier or security grill.

5.7.1 The grill will be fabricated of steel or aluminum grating or bars with a thickness equal to the thickness of the physical perimeter barrier. If a grating is used, bridge center-to-center measurements will not exceed 1.5 inches by 4 inches. Bars will be mounted on 6 inch centers. The grating or bars will be welded into place.

5.7.2 This requirement is not applicable to through ducts that have no opening into the space.

5.8 Acoustical Isolation: The physical perimeter barrier of all SCI spaces will be sealed or insulated with nonhardening caulking material to prevent inadvertent disclosure of SCI discussions or briefings from within the space, taking into account the normal ambient noise level, to persons located in adjacent passageways and/or compartments.

5.8.1 In cases where the perimeter material installation does not sufficiently attenuate voices or sounds of activities originating SCI information, the ambient noise level will be raised by the use of sound countermeasure devices, controlled sound generating source. or additional perimeter material installation.

5.8.2 Air handling units and ducts will be equipped with silencers or sound countermeasure devices unless continuous duty blowers provide a practical, effective level of masking (blower noise) in each air path. The effective level of security may be determined by stationing personnel in adjacent spaces or passageways to determine if SCI can be overheard outside the space.

5.9 Visual Isolation: Door or other openings in the physical perimeter barrier through which the interior may be viewed will be screened or curtained.

6.0 INTRUSION DETECTION SYSTEM (IDS):

Obtained via FOIA by Judicial Watch, Inc.

The S/SCIF access door and emergency exit will be protected by a visual and audible alarm system. The installation will consist of sensors connected at each door and alerting indicators located at the facility supervisor's position. The normal access door alarm may have a disconnect feature.

6.1 Emergency exits will be connected to the alarm system at all times and will not have a disconnect feature installed.

6.2 The IDS will be connected to a remote alarm monitor station, which may be colocated with other IDS, and located within a space which is continuously manned by personnel capable of responding to or directing a response to an alarm violation at the protected space when it is unmanned.

6.3 Primary power for the IDS will be connected to an emergency lighting panel within the space. SCI spaces that are under continuous manning will be staffed with sufficient personnel, as determined by the on-site security authority based on the local threat environment, who have the continuous capability of detecting forced or surreptitious entry without the aide of an IDS.

7.0 PASSING SCUTTLES AND WINDOWS;

Passing scuttles and windows will not be installed between SCI spaces and any other space on the ship.

8.0 LOCATION OF CRYPTOGRAPHIC EQUIPMENT:

On-line and off-line cryptographic equipment and terminal equipment processing SCI will be located only within the S/SCIF.

9.0 SECURE STORAGE CONTAINERS:

SCI material will be stored only in GSA approved Class 5, 6, or 7 security containers. Containers will be welded in place, or otherwise secured to a foundation for safety.

10.0 TELEPHONES:

Telephone instruments used within a S/SCIF will meet the Telephone Security Annex standards.

11.0 SECURE TELEPHONE UNIT-III (STU-III):

The STU-III Type I terminals may be installed within a S/SCIF.

12.0 SOUND POWERED TELEPHONES:

Where possible, sound powered telephones will be eliminated from S/SCIFs. Sound powered telephones located within the S/SCIF connecting to locations outside the S/SCIF will comply with the following

12.1 The telephone cable will not break out to jackboxes, switchboards, or telephone sets other than at the designated stations. The telephone cable will not be shared with any circuit other than call or signal systems associated with the S/SCIF circuit.

12.2 The telephone cable will be equipped with a selector switch, located at the controlling station,

which is capable of:

- 12.2.1 Disconnecting all stations;
- 12.2.2 Selecting any one station and disconnecting the remaining stations; and
- 12.2.3 Parallel connection to all stations.

12.3 Other S/SCIFs located aboard the same ship, which have sound powered telephones not equipped with the required selector switch, will have a positive disconnect device attached to the telephone circuit.

12.4 Sound powered telephones within a S/SCIF that are not used for passing SCI information will have a sign prominently affixed to them indicating that they are not to be used for passing SCI.

12.5 A call or signal system will be provided. Call signal station, type ID/D, when used for circuit EM will be modified to provide a disconnect in the line to prevent a loudspeaker from functioning as a microphone.

13.0 SCI INTERCOM ANNOUNCING SYSTEM:

An intercommunication type announcing system processing SI that connects to or passes through areas outside the S/SCIF must be approved by the CSA.

14.0 SUPPORTING INTERCOMMUNICATION ANNOUNCING SYSTEMS:

Intercommunication-type announcing systems installed within an S/SCIF that do not process SCI information will be designated or modified to provide the following physical or electrical security safeguards:

- 14.1 Operational mode of the unit installed within the S/SCIF will limit operation to push-to-talk mode only.
- 14.2 Receive elements will be equipped with a local amplifier as a buffer to prevent loud-speakers or earphones from functioning as microphones.
- 14.3 Except as specified, radio transmission capability for plain radio telephone (excluding secure voice) will not be connected. Cable conductors assigned to the transmission of plain language radio telephones will be connected to ground at each end of the cable.
- 14.4 Equipment modified will have an appropriate field change label affixed to the unit that indicates the restriction. Additionally, the front panel will have a sign warning the user that the system is not passing classified information.

15.0 COMMERCIAL INTERCOMMUNICATION EQUIPMENT:

Commercial intercommunication equipment will not be installed within a S/SCIF without prior CSA approval.

16.0 GENERAL ANNOUNCING SYSTEMS:

General announcing system loudspeakers will have an audio amplifier, and the output signal lines will be installed within the S/SCIF.

17.0 PNEUMATIC TUBE SYSTEMS:

Pneumatic tube systems will not be installed. Existing systems will be equipped with the following security features:

17.1 Locked cover at both ends.

17.2 Capability to maintain the pressure or vacuum and capability to lock in the secure position at the initiating end.

17.3 Direct voice communications link between both ends to confirm the transportation and receipt of passing cartridges.

17.4 Special, distinctive color for SCI material passing cartridges.

17.5 Pneumatic tubes will run through passageways and will be capable of being visually inspected along their entire length.

18.0 DESTRUCTION EQUIPMENT:

A CSA-approved means of destruction of SCI material will be provided for each S/SCIF. Non-combatant surface ships that transit hostile waters without combatant escort will have appropriate Anti-compromise Emergency Destruction (ACED) equipment on board and such equipment will be prepared for use. The ACED will be dedicated to SCI destruction. SCI material will not be destroyed by jettisoning overboard under any circumstances.

19.0 EMERGENCY POWER:

A S/SCIF will have emergency power available that will operate destruction equipment, alarm systems, access control devices, and emergency lighting equipment for a minimum of six hours.

20.0 SCI PROCESSING SYSTEMS:

A S/SCIF that processes SCI electronically or electrically should be provided a TEMPEST evaluation prior to activation. All computer and network systems that process SCI must be accredited or certified for operation by the cognizant SCI AIS Accreditation Authority.

21.0 TEMPORARY ACCREDITATION:

Ships requiring temporary accreditation status will be processed for accreditation upon completion of a physical security inspection and certification of compliance with the following security requirements:

21.1 If the space is used to electrically process SCI information, the CSA will make a TEMPEST evaluation based on threat.

21.2 The physical perimeter barrier will consist of standard structural, nonsupport, or metal joiner bulkheads welded or riveted into place and meet the acoustical isolation requirements of a S/SCIF.

21.3 Doors will be at least metal joiner doors equipped with door closures and capable of being secured from the inside. Dutch doors are not acceptable. If cryptographic equipment is installed or stored within the space and the space will be temporarily unmanned while cryptographic key

Obtained via FOIA by Judicial Watch, Inc.

material and/or SCI material are stored else-where, the door will be equipped with a tamper-proof hasp and combination pad-lock.

21.4 Doors and other openings in the perimeter that permit aural or visual penetration of the internal space will be screened, curtained, or blocked.

21.5 An effective, approved secure means of destruction of SCI material will be readily available in the space or nearby in general service spaces.

21.6 Cryptographic equipment used to process SCI information will be located in the SCI space or, if located in a secure processing center other than that accredited for SCI, will be electrically configured so as not to be compatible with the secure processing system of that secure processor.

21.7 All telephones (to include STU-III instruments and sound powered telephones) will be as specified for S/SCIFs.

21.8 Processing of SCI via AIS will be as specified for S/SCIFs.

22.0 TEMPORARY SECURE WORKING AREAS (TSWAs):

Ships requiring TSWA accreditation for "contingency" or "part-time" usage will be processed for accreditation upon completion of a physical security inspection and certification of compliance with the following security requirements:

22.1 The physical perimeter barrier requires no special construction, provided it can prevent visual and aural access during all periods of SCI operation.

22.2 Doors will be capable of being secured from the inside.

22.3 Provisions will be made for posting a temporary sign that reads "RESTRICTED AREA - KEEP OUT - AUTHORIZED PERSONNEL ONLY".

22.4 When SCI material is to be stored in the space, a secure storage container will be provided. Security storage containers will be welded in place, or otherwise secured to the foundation for safety and to prevent rapid removal.

22.5 The electrical security requirements for a shipboard TSWA will be specified by the CSA.

23.0 EMBARKED PORTABLE SHIPBOARD COLLECTION VANS (PSCVs):

PSCVs are vans that are temporarily placed aboard ship and not part of the permanent structure of the ship. Ships requiring accreditation of embarked PSCVs must be annually accredited by the CSA and may be activated upon certification to the CSA of compliance with the following security requirements:

23.1 The exterior surface of the van will be solid construction and capable of showing evidence of physical penetration (except for intended passages for antenna cables, power lines, etc.)

23.2 The access door will fit securely and be equipped with a substantial locking device to secure the door from the inside in order to prevent forcible entry without tools.

23.3 Adequate security measures will be established to preclude viewing of classified material by

uncleared personnel.

23.4 Adequate provisions will be established to control the approach of uncleared personnel within the vicinity of the van. These measures will consist of instructions promulgated by the station (ashore and afloat) in which the van is embarked, prohibiting loitering in the immediate vicinity of the van, and will include periodic visual security checks by appropriately SCI-indoctrinated personnel.

23.5 Adequate destruction equipment will be available and effective procedures established to ensure rapid and complete destruction of classified material in emergency situations.

23.6 All SCI material will be stored within the van and continuously manned by sufficient SCI-indoctrinated personnel as determined by the on-site security authority based on the local threat environment, when activated for SCI support. If SCI material is to be stored outside the van, the space must be accredited by the CSA and be in compliance with the above S/SCIF criteria.

23.7 The electrical security requirements for a PSCV will be as specified by the CSA.

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 6/9

ANNEX D

PART I - Electronic Equipment in Sensitive Compartmented Facilities (SCIFs)

(Effective 30 January 1994)

1.0 INTRODUCTION

It is the policy of the Director of Central Intelligence and the Senior Officials of the Intelligence Community (SOICs) that personally owned electronic equipment that has been approved for introduction into a SCIF should not be routinely carried into or out of the SCIF due to the possibility of technical compromise. It is also their policy that electronic equipment that is introduced into a SCIF is subject to technical and/or physical inspection at any time.

2.0 GUIDANCE

The following guidance is provided concerning the control of electronic equipment. SOICs retain the authority to apply more stringent requirements as deemed appropriate.

2.1 DOMESTIC UNITED STATES

The following personally owned electronic equipment may be introduced into a SCIF:

- 2.1.1 Electronic calculators, electronic spell-checkers, wrist watches, and data diaries.
NOTE: If equipped with data-ports, SOICs will ensure that procedures are established to prevent unauthorized connector to automated information systems that are processing classified information.

Obtained via FOIA by Judicial Watch, Inc.

2.1.2 Receive only pagers and beepers.

2.1.3 Audio and video equipment with only a "playback" feature (no recording capability), or with the "record" feature disabled/removed.

2.1.4 Radios

2.1.5 PROHIBITED EXCEPT FOR OFFICIAL DUTY

The following items are prohibited unless approved by the SOIC for conduct of official duties:

2.1.5.1 Two-way transmitting equipment.

2.1.5.2 Recording equipment (audio, video, optical). Associated media will be controlled.

2.1.5.3 Test, measurement, and diagnostic equipment.

2.1.6 PROHIBITED IN SCIFs

The following items are prohibited in SCIFs:

2.1.6.1 Personally owned photographic, video, and audio recording equipment.

2.1.6.2 Personally owned computers and associated media.

2.2 OVERSEAS

The provisions in paragraphs 2.1.5 and 2.1.6 above apply in the overseas environment with the exception that all personally owned electronic equipment may be introduced in the SCIF ONLY with the prior approval of the SOIC and on-site security representative, based on local threat conditions.

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 6/9

ANNEX D

Part II - Disposal of Laser Toner Cartridges

(Revised 05 June 1998)

1.0 INTRODUCTION

The Director of Central Intelligence and the Senior Officials of the Intelligence Community (SOICs) hereby establish the policy and procedures for the disposal of used laser toner cartridge drums (cartridges). The policy established herein is based on technical research that has confirmed that the laser printer toner cartridges, removed from properly functioning printers, do not retain any residual static charge that could be associated with previously printed information. Thus,

Obtained via FOIA by Judicial Watch, Inc.

countermeasures to "declassify" a cartridge before releasing it, such as printing multiple pages of unclassified information or physically destroying the cartridge drum, are unnecessary and the expense of destroying toner cartridges is not deemed to be justified. SOICs are responsible for implementation of this policy within their respective department/agency. When deemed necessary and appropriate, SOICs may establish additional security measures.

2.0 POLICY

This policy applies to all equipment that uses similar technology (a laser printer with removable toner cartridge) as part of its production process (i.e. Laser Faxes, Printers, Copiers, etc.).

2.1 Used toner cartridges may be treated, handled, stored and disposed of as UNCLASSIFIED, when removed from equipment that has successfully completed its last print cycle. However, should a print cycle not be completed, there is the potential that residual toner may be left on the drum that could cause an information compromise. The following procedures should be followed for those situations where the print cycle was not successfully completed.

2.1.1 When a laser printer has not completed the printing cycle (e.g., a paper jam or power failure occurs), completing a subsequent print cycle before removal of cartridge is sufficient to wipe residual toner from the cartridge drum.

2.1.2 When the print cycle is interrupted by a jam or other action, and the toner cartridge is removed from service at the same time, the toner cartridge drum will be inspected for residual toner by lifting the protective flap and viewing the exposed portion of the drum. If residual toner is present, manually rotating the drum is sufficient to wipe off residual toner material present.

2.2 After completing 2.1.1 or 2.1.2, the used toner cartridge may be treated, handled, stored and disposed of as UNCLASSIFIED and be returned for recycling or other agency approved method of disposal. In keeping with Environmental Protection Agency policy, agencies/departments are encouraged to establish procedures for recycling properly sanitized toner cartridges.

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 6/9

ANNEX E - Acoustical Control and Sound Masking Techniques

(Effective 30 January 1994)

1.0 Basic Design:

Acoustical protection measures and sound masking systems are designed to protect SCI against being inadvertently overheard by the casual passerby, not to protect against deliberate interception of audio. The ability of a SCIF structure to retain sound within the perimeter is rated using a descriptive value, the Sound Transmission Class (STC).

Obtained via FOIA by Judicial Watch, Inc.

1.1 The STC Rating: STC is a single number rating used to determine the sound barrier performance of walls, ceilings, floors, windows, and doors.

1.2 Use of Sound Groups: The current edition of Architectural Graphics Standards (AGS) describes various types of sound control, isolation requirements and office planning. The AGS established Sound Groups I through 4, of which Groups 3 and 4 are considered adequate for specific acoustical security requirements for SCIF construction.

1.2.1 Sound Group I - STC of 30 or better. Loud speech can be understood fairly well. Normal speech cannot be easily understood.

1.2.2 Sound Group 2 - STC of 40 or better. Loud speech can be heard, but is hardly intelligible. Normal speech can be heard only faintly if at all.

1.2.3 Sound Group 3 - STC of 45 or better. Loud speech can be faintly heard but not understood. Normal speech is unintelligible.

1.2.4 Sound Group 4 - STC of 50 or better. Very loud sounds, such as loud singing, brass musical instruments or a radio at full volume, can be heard only faintly or not at all.

2.0 Sound Reduction for SCIFs:

The amount of sound energy reduction may vary according to individual facility requirements. However, Sound Group ratings shall be used to describe the effectiveness of SCIF acoustical security measures afforded by various wall materials and other building components.

2.1 All SCIF perimeter walls shall meet Sound Group 3, unless additional protection is required for amplified sound.

2.2 If compartmentation is required within the SCIF, the dividing office walls must meet Sound Group 3.

3.0 Sound Masking and Stand-Off Distance:

3.1 When normal construction and baffling measures have been determined to be inadequate for meeting Sound Group 3 or 4, as appropriate, sound masking shall be employed. Protection against interception of SCI discussions may include use of sound masking devices, structural enhancements, or SCIF perimeter placement.

3.1.1 Sound masking devices may include vibration and noise generating systems located on the perimeter of the SCIF.

3.1.2 Structural enhancements may include the use of high density building materials (i.e. sound deadening materials) to increase the resistance of the perimeter to vibration at audio frequencies.

3.1.3 SCIF perimeter placement may include construction design of a stand-off distance between the closest point a non-SCI indoctrinated person could be positioned and the point when SCI discussions become available for interception. Use of a perimeter fence or protective zone between the SCIF perimeter walls and the closest "listening place" is permitted as an alternative to other sound protection measures.

3.2 Masking of sound which emanates from an SCI discussion area is commonly done by a sound

Obtained via FOIA by Judicial Watch, Inc.

masking system. A sound masking system may utilize a noise generator, tape, disc or record player as a noise source and an amplifier and speakers or transducers for distribution.

4.0 Placement of Speakers and Transducers:

To be effective, the masking device must produce sound at a higher volume on the exterior of the SCIF than the voice conversations within the SCIF. Speakers/transducers should be placed close to or mounted on any paths which would allow audio to leave the area. These paths may include doors, windows, common perimeter walls, vents/ducts, and any other means by which voice can leave the area.

4.1 For common walls, the speakers/transducers should be placed so the sound optimizes acoustical protection.

4.2 For doors and windows, the speakers/transducers should be close to the aperture of the window or door and the sound projected in a direction facing away from conversations.

4.3 Once the speakers or transducers are optimally placed, the system volume must be set and fixed. The level for each speaker should be determined by listening to conversations occurring within the SCIF and the masking sound and adjusting the level until conversations are unintelligible from outside the SCIF.

5.0 Installation of Equipment:

5.1 The sound masking system and all wires and transducers shall be located within the perimeter of the SCIF.

5.2 The sound masking system shall be subject to review during TSCM evaluations to ensure that the system does not create a technical security hazard.

6.0 Sound Sources:

The sound source must be obtained from a player unit located within the SCIF. Any device equipped with a capability to record ambient sound within the SCIF must have that capability disabled. Acceptable methods include:

6.1 Audio amplifier with a record turntable.

6.2 Audio amplifier with a cassette, reel-to-reel, Compact Disc (CD), or Digital Audio Tape (DAT) playback unit.

6.3 Integrated amplifier and playback unit incorporating any of the above music sources.

7.0 Emergency Notification Systems:

The introduction of electronic systems that have components outside the SCIF should be avoided. Speakers or other transducers, which are part of a system that is not wholly contained in the SCIF, are sometimes required to be in the SCIF by safety or fire regulations. In such instances, the system can be introduced if protected as follows:

7.1 All incoming wiring shall breach the SCIF perimeter at one point. TEMPEST or TSCM concerns may require electronic isolation.

Obtained via FOIA by Judicial Watch, Inc.

7.2 In systems that require notification only, the system shall have a high gain buffer amplifier. In systems that require two-way communication, the system shall have electronic isolation. SCIF occupants should be alerted when the system is activated. All electronic isolation components shall be installed within the SCIF as near to the point of SCIF egress as possible.

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) 6/9^[5]_[5]

ANNEX F - Personnel Access Controls

(Effective 18 November 2002)

1.0 General Requirements

All SCIFs shall have personnel access control systems to control access at all perimeter entrances. Placards, signs, notices, and similar items are not acceptable as personnel access control systems. Unless otherwise stated herein, SCIF entrances shall be under visual control to deny unauthorized access unless the SCIF is unoccupied and secured. Such visual control may be accomplished by employees, guards using closed circuit television (CCTV), or other similar and approved methods. If CCTV is used for providing visual control, the CCTV equipment shall be continuously monitored by appropriately SCI-indoctrinated personnel. Personnel access control systems as specified herein do not replace or modify any requirement to properly secure SCIF doors as specified in DCID 6/9.

2.0 Automated Access Control Systems

Automated personnel access control systems meeting the following criteria may be used to control admittance to SCIFs during working hours in lieu of visual control.

2.1 Identification Requirement. The automated personnel access control system shall verify the identity of an individual by one of the following methods.

2.1.1 Identification (ID) Badges or Cards. The ID badge or card must identify to the access control system the individual to whom the card is issued. A personal identification number (PIN) is required. The PIN must be separately entered into the system by each individual using a keypad device and shall consist of four or more digits, randomly selected, with no known or logical association with the individual.

2.1.2 Personal Identity Verification. Personal identity verification (biometrics device) identifies the individual requesting access by some unique personal characteristic.

2.2 Authentication Requirement. The automated personnel access control system shall authenticate an individual's authorization to enter the SCIF by matching the applicable information specified in the previous paragraph with personnel data contained in an automated database to authenticate the individual's authorization prior to giving the individual access to the SCIF.

Obtained via FOIA by Judicial Watch, Inc.

2.3 Accept/Reject Threshold Criteria. Automated personnel access control equipment or devices shall meet the following criteria during normal equipment operation: The probability of an unauthorized individual gaining access is no more than one in ten thousand while the probability of an authorized individual being rejected access is no more than one in one thousand. Prior to using such equipment, manufacturers must certify in writing that their equipment conforms to this criterion.

2.4 System Protection. Physical security protection must be established and continuously maintained for all devices/equipment that comprise the personnel access control system. The level of protection may vary depending upon the type of devices/equipment being protected. Existing security controls within the facility shall be used to the extent practical in meeting this requirement.

2.5 Transmission Line Protection. System data that is carried on transmission lines (e.g., access authorizations, personal identification, or verification data) to and from devices/equipment located outside the SCIF shall be encrypted with an approved 128 bit, or greater, encryption algorithm. The algorithm must be certified by NIST or another US government authorized independent testing laboratory. If the communication technology described above is not feasible, the transmission line will be installed within a protective covering to preclude surreptitious manipulation, or be adequately supervised to protect against modification and/or substitution of the transmitted signal.

2.6 Door Strikes. Electric door strikes installed for use in personnel access control systems shall be heavy-duty industrial grade.

2.7 Personnel and System Data Protection. Locations where authorization data, card encoded data, and personal identification or verification data is input, stored, or recorded must be protected within a SCIF or an alarmed area controlled at the SECRET level. Records and information concerning encoded ID data, PINs, authentication data, operating system software, or any identifying data associated with the personnel access control system shall be kept secured when unattended. Access to the data shall be restricted. (See paragraph 4.3.)

2.8 External Devices. Card readers, keypads, communication, or interface devices located outside the entrance to a SCIF, shall have tamper resistant enclosures and be securely fastened to a wall or other structure.

2.9 Electrical components, associated wiring, or mechanical links (cables, rods, and so on) should be accessible only from inside the SCIF, or if they transverse an uncontrolled area they shall be secured within a protective covering to preclude surreptitious manipulation of components.

2.10 Records shall be maintained to reflect the current active assignment of ID badge/card, PIN, level of access, entries, and similar system-related elements. Records concerning personnel removed from the system shall be retained for a minimum of two years. Records of entries to SCIFs shall be retained for a minimum of two years or until investigations of system violations and incidents have been successfully resolved and recorded.

3.0 Non-Automated Access Control

Non-automated access control (electric, mechanical, or electromechanical) that meet the criteria stated below may be used to control admittance to SCIF areas during working hours if the entrance is under visual control (see paragraph 1.0). These systems are also acceptable to control access to compartmented areas within the SCIF. Non-automated access system devices must be installed in

the following manner:

3.1 Control Panel Location and Shielding. The control panel in which the combination and all associated cabling and wiring is set shall be located inside the SCIF and will require minimal physical security designed to deny unauthorized access to its mechanism. The control panel shall be installed, or have a shielding device mounted, such that an unauthorized person in the immediate vicinity cannot observe the setting or changing of the combination. (See paragraph 4.4.)

3.2 Access Code Protection. Keypad devices shall be designed or installed in such a manner that unauthorized individuals in the immediate vicinity cannot observe the entry of the access code.

4.0 Personnel Requirements and Restrictions

Operating personnel access control systems in accordance with this annex requires that the below personnel requirements and restrictions be followed:

4.1 Entering and Leaving a SCIF. Personnel entering or leaving an area are required to ensure the entrance or exit point is properly closed. Authorized personnel who permit another individual to enter the area are responsible for confirming the individual's access and need-to-know.

4.2 Escorting. An SCI-indoctrinated person who is knowledgeable of the security procedures of the SCIF shall continuously escort persons within the SCIF who are not SCI-indoctrinated.

4.3 Access to Personnel and System Data. Access to records and information concerning encoded ID data and PINs shall be restricted to SCI-indoctrinated personnel. Access to identification or authentication data, operating system software, or any identifying data associated with the personnel access control system shall be limited to the least number of personnel possible.

4.4 Setting Combinations (*applies to non-automated access control only*). The selection and setting of the combination shall be accomplished by SCI-indoctrinated individuals. The combination shall be changed when compromised or an individual knowledgeable of the combination no longer requires access.

4.5 System Records Maintenance. A procedure shall be established for removing an individual's authorization to enter an area when the individual is transferred, terminated, or the individual's access is suspended, revoked, or downgraded to a level below that required for entry. Compromised access cards and/or PINs will be immediately reported and removed from the system.

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) 6/9 ^[6]_[6]

ANNEX G - Telecommunications Systems and Equipment

(Effective 18 November 2002)

This annex establishes a baseline requirement for the protection of sensitive information within Sensitive Compartmented Information Facilities (SCIFs) from intrusion and exploitation via unclassified telecommunications systems, devices, equipment, software, and features. Compliance with these standards is mandatory for all SCIFs and/or systems established after the effective date of this annex.

1.0 Applicability and Scope

The telecommunications security measures of this Annex apply to the planning, installation, maintenance, and management of telecommunication systems and equipment within SCIFs, in both foreign and domestic locations. The security measures of this Annex apply to any telecommunication system that provides service to a SCIF. The requirements contained in this annex are designed to prevent inadvertent disclosure or loss of sensitive, intelligence bearing information through telecommunication systems and to protect against the clandestine exploitation and/or disruption of SCIF operations through these systems. This Annex is compatible with but may not satisfy requirements of other security disciplines such as COMSEC, OPSEC, or TEMPEST.

2.0 Requirements

At a minimum, the following requirements must be met to ensure proper safeguards for the protection of information: configuration of telecommunications systems, devices, features, and software; access control; and control of the cable infrastructure. The audio protection requirements of this Annex do not apply if the SCIF is declared a "No Classified Discussion Area" and warning notices are posted prominently within the SCIF.

2.1 Baseline Configuration.

2.1.1 A baseline configuration of all telecommunications systems, devices, features, and software must be established, documented, and included in the Fixed Facility Checklist (DCID 6/9 Annex A) or as an attachment.

2.1.2 The Cognizant Security Authority (CSA) will review the telecommunications system baseline configuration and supporting/supplementing information to determine if the risk of information loss or exploitation has been suitably mitigated. When the following requirements are unachievable, the associated telecommunications equipment must be installed and maintained in non-discussion areas or a written waiver must be issued by the CSA.

2.2 Unclassified Telecommunications Systems. Unclassified telecommunications systems in SCIFs shall not pass/transmit sensitive audio discussions when they are idle and not in use. Additionally, these telecommunications systems shall be configured to prevent external control or activation. The concepts of "on-hook" and "off-hook" audio protection ^[7][7] outlined in telephone security group (TSG) standards 2 and 6 must be incorporated into SCIF telecommunications systems.

2.2.1 Unclassified telephone systems and services shall be configured to prevent technical exploitation or penetration. In addition, these systems shall incorporate physical and software access controls to prevent disclosure or manipulation of system programming and stored data.

The CSA must ensure that the following specific requirements are applied to unclassified telecommunications systems:

2.2.1.1 Provide on-hook audio protection by the use of TSG 6 instrument(s), TSG 6 approved disconnect devices, or equivalent TSG 2 system configuration.

2.2.1.2 Provide off-hook audio protection by use of a hold feature, modified handset (push-to-talk), or equivalent.

2.2.1.3 Provide isolation by use of a computerized telephone system (CTS) with software and hardware configuration control and control of audit reports (such as station message detail reporting, call detail reporting, etc.). System programming will not include the ability to place, or keep, a handset off-hook. Configuration of the system must ensure that all on-hook and off-hook vulnerabilities are identified and mitigated.

2.2.1.4 Ensure that equipment used for administration of telephone systems is installed inside an area where access is limited to authorized personnel. When local or remote administration terminals (for a CTS) are not or cannot be contained within the controlled area, and safeguarded against unauthorized manipulation, then the use of TSG 6 approved telephone instruments shall be required, regardless of the CTS configuration.

2.2.1.5 Ensure that remote maintenance, if used, is protected against manipulation/activation by means of a dial-back modem, network boundary security device (firewall), or other appropriate device.

2.2.1.6 Ensure that speakerphones and audio conferencing systems are not used on unclassified telecommunications systems in SCIFs. Exceptions to this requirement may be approved by the CSA, when these systems have sufficient audio isolation from other classified discussion areas in the SCIF, and procedures are established to prevent inadvertent transmission of classified information.

2.2.1.7 Ensure that features used for voice mail or unified messaging services, are configured to prevent unauthorized access to remote diagnostic ports or internal dial tone.

2.2.1.8 Ensure that telephone answering devices (TAD) and facsimile machines do not contain features that introduce security vulnerabilities, e.g., remote room monitoring, remote programming, or other similar features that may permit off-premise access to room audio. Prior CSA approval is required before installation or use.

2.2.2 All unclassified telecommunications systems and associated infrastructure must be electrically and physically isolated from any classified information/telecommunications systems in accordance with National Security Telecommunications and Information Systems Security Committee requirements or any other separation standards applied to the classified information system on site.

2.3 Unclassified Information Systems. Unclassified information systems must be safeguarded to prevent manipulation of features and software that could result in the loss/compromise of sensitive audio information or protected data.

Obtained via FOIA by Judicial Watch, Inc.

2.3.1 Ensure that all computer/telecommunications equipment with telephonic or audio features are protected against remote activation and/or exfiltration of audio information over any connections (i.e., disconnecting the microphone, inserting a blank plug in the microphone jack, etc.).

2.3.2 Ensure that all video cameras used for unclassified video teleconferencing and/or video recording equipment are deactivated and disconnected when not in use. In addition, video devices used in SCIFs must feature a clearly visible indicator to alert SCIF personnel when recording or transmitting.

2.4 Environmental Infrastructure Systems. Environmental infrastructure systems are the basic human comfort, security, and life safety systems that support SCIF operations. Advancements in technology have created conditions whereby many of these amenities are computer-automated with public switched telephone network or other connections for remote monitoring, access, and external control/manipulation of features and services. Fixed facility checklists (FFC) will identify any such connection to environmental systems within SCIFs, and document measures taken to provide protection against malicious activity, intrusion, and exploitation. Protection mechanisms and current configurations for infrastructure systems, such as premise management systems, environmental control systems, lighting and power control units, uninterrupted power sources, and such, which provide services to the SCIF, shall be included in the SCIF baseline evaluation (whether or not they reside in the SCIF).

2.5 Wireless Technology. The use of any device, or system utilizing wireless technology must be approved by the CSA prior to purchase and introduction into the SCIF. All TEMPEST/Technical Security concerns shall be weighed against the facilities overall security posture (i.e., facility location, threat, as well as any compensatory countermeasures that create a "security in-depth" concept) when evaluating these wireless systems. All separation and isolation standards provided in NSTISSC standards are applicable to unclassified wireless systems installed or used in SCIFs.

2.6 Access Control. Installation and maintenance of unclassified telecommunications systems and devices supporting SCIF operations may require physical and/or electronic access. Remote maintenance may be performed as described in paragraph 2.6.2. Under other circumstances, physical access may be required to perform computer-based diagnostics to make necessary repairs. Therefore, the following paragraphs identify the minimum requirements for providing access to unclassified telecommunications systems and devices supporting SCIF operations. These requirements are applicable regardless of whether or not the telecommunications device resides within the SCIF or is contained in a protected area outside the SCIF, so long as it is deemed as a critical infrastructure item by the CSA.

2.6.1 Physical Access Control. Installation and maintenance personnel will possess an appropriate clearance and access or will be escorted and monitored by technically knowledgeable cleared personnel at all times within the SCIF. Furthermore, physical access to telecommunications equipment shall be limited to prevent unauthorized modifications or reconfiguration.

2.6.2 Remote Maintenance and Diagnostic Access. All capabilities for remote maintenance and diagnostic services must be clearly specified in the FFC. The FFC will include all procedures and countermeasures preventing unauthorized system access, unauthorized system modification, or introduction of unauthorized software as specified in TSG 2 paragraph 4d.

2.6.2.1 Remote maintenance and diagnosis may be performed from a secure

facility over a protected link (i.e., dial-back or DES modem).

2.6.2.2 Failing the steps outlined in paragraph 2.6.2.1, remote maintenance and diagnosis may be performed over an unclassified telephone line as specified in TSG 2 paragraph 4c.

2.7 Memory and Storage Media. Any telecommunication system, component and/or like devices with memory or digital storage capabilities, to include multi-function devices, (i.e., facsimile, printers, copiers, scanners, etc.) will be sanitized of any sensitive information before being repaired or released to uncleared personnel.

2.7.1 The baseline configuration document, FFC, will identify all memory and data storage systems of all unclassified telecommunications systems that contain sensitive data or information that is of concern for operational security purposes. This storage media will be sanitized before it is removed from the facility for any purpose, including maintenance or disposal. Similarly, this storage media will not be made available to uncleared technicians or maintenance personnel.

2.7.2 Storage media that cannot be effectively sanitized will be removed from the telecommunications system prior to repair or disposal, and be destroyed by approved methods.

2.8 SCIF Cable Control.

2.8.1 All unclassified telecommunications cabling^[8]_[8] should enter the SCIF through a common opening. The cables should be installed in a professional manner, such that they can be visually inspected without difficulty.

2.8.2 Each conductor (fiber or metallic) should be accurately accounted for from the point of entry. The accountability should identify the precise use of every conductor through labeling, log, or journal entries. Spare conductors will be identified and appropriately grounded.

2.8.3 Unused conductors will be removed. If removal is not feasible, the CSA may require the metallic conductors be stripped, bound together, and grounded at the point of ingress/egress. Unused fiber conductors will be uncoupled from the interface within the SCIF, capped, and labeled as unused.

3.0 Responsibilities

3.1 **NTSWG.** The National Telecommunications Security Working Group (NTSWG) is responsible for developing security countermeasure solutions for unclassified telecommunications systems and devices.

3.2 **CSA.** The CSA is responsible for selecting, implementing, and verifying security measures to balance the vulnerabilities of the telecommunications system(s) against technical threats of its environment. This requires the CSA to:

3.2.1 Know this Annex and be able to assist site security personnel with implementation.

3.2.2 Review the fixed facility checklist and certify that all the requirements of this

Obtained via FOIA by Judicial Watch, Inc.

Annex have been met. When the requirements of this Annex cannot be met, the CSA must mitigate the risk through the application of countermeasures or waive the requirement.

3.2.3 Assist site security personnel in selecting telecommunications equipment and/or recommending appropriate countermeasures.

3.2.4 Maintain a current set of the reference documents. See references, section 4.0 below.

3.2.5 Responsible for ensuring that a full risk assessment is performed prior to issuance of a waiver or exception to the provisions of this document, and for ensuring that any waiver or exception is periodically reviewed. Any such waivers or exceptions must be documented.

3.2.6 Request technical surveillance countermeasures (TSCM) inspections as conditions warrant, to prevent the loss or compromise of protected information through the intrusion and exploitation of a telecommunications system IAW DCID 6/2.

3.3 Site Security Personnel. The site security personnel are responsible for implementing the requirements of this Annex and requesting CSA approval for new telecommunications systems, devices, features and hardware, and major modifications to existing systems by:

3.3.1 Submitting necessary documentation on new systems and/or modified systems and recommending security countermeasures and options to the CSA, as appropriate.

3.3.2 Maintaining a record set of documentation on site.

3.3.3 Adhering to the guidance set forth by the CSA.

3.3.4 Notifying the CSA of any suspected or actual attempts to intrude or exploit a telecommunications or infrastructure system supporting SCIF operations. When warranted, site security personnel will assist the CSA with investigating and resolving the incident, and applying additional countermeasures as required.

3.3.5 Determining that telecommunications systems and devices are properly sanitized or cleared prior to any maintenance procedures, and that all networked interconnections are removed (isolated) during maintenance routines.

3.3.6 Authorizing diagnostics connections (either remote or on-site) for the purpose of performing maintenance on telecommunications systems and devices, and conducting reviews of on-site test data prior to releasing it from the protected area.

4.0 References

4.1 *NTSWG (formerly known as the TSG)*. Standards and information series-refers to the published guidance provided by the NTSWG for the protection of sensitive information and unclassified telecommunications information processing systems and equipment. The following documents are intended for use by all personnel concerned with telecommunications security.

4.1.1 TSG Standard 1, (*Introduction to Telephone Security*). Provides telephone security background and TSG-approved options for telephone installations in US

Government sensitive discussion areas.

4.1.2 TSG Standard 2 (*TSG Guidelines for Computerized Telephone Systems*) and its Annexes. Establishes requirements for planning, installing, maintaining, and managing a CTS, and provides guidance for personnel involved in writing contract, inspecting, and system administration of a CTS.

4.1.3 TSG Standard 6, (*TSG-Approved Equipment*). Lists TSG-approved equipment which inherently provides protection against the accidental collection and conduction of information from within sensitive discussion areas.

4.1.4 TSG Standards 3,4,5,7, and 8. Contains design specifications for telecommunication manufacturers, and are not necessarily applicable to facility security personnel.

4.1.5 Information Series (*Computerized Telephone Systems (CTSs) A Review of Deficiencies, Threats, and Risks*, dated: December 1994). Describes deficiencies, threats, and risks associated with computerized telephone systems which impact the loss of "on-hook" audio, as well as the protection of unclassified information stored/contained within the CTS and its telephone devices.

4.1.6 Information Series (*Executive Overview*, dated: October 1996). Provides the salient points of the TSG standards and presents them in a non-technical format.

4.1.7 Information Series (*Central Office (CO) Interfaces*, dated: November 1997). Provides an understanding of the types of services delivered by the local central office and describes how they are connected to administrative telecommunications systems and devices.

4.1.8 Information Series (*Everything You Always Wanted to Know about Telephone Security...but were afraid to ask*, second edition, dated: December 1998). Distills the essence of the TSG standards (which contain sound telecommunications practices) and presents them in a readable, non-technical manner.

4.1.9 Information Series (*Infrastructure Surety Program...securing the last mile*, dated: April 1999). Provides a basic understanding of how to protect office automation and infrastructure systems that contribute to successful mission accomplishment.

4.1.10 Information Series (*Computerized Telephone Systems Security Plan Manual*, dated: May 1999). Assists in implementing and maintaining the "secure" operation of CTSs when used to support SCIF operations. The term "secure" relates to the safe and risk-free operation, not the use of encryption or a transmission security device.

4.2 Director of Central Intelligence Directive (DCID 6/2). Technical Surveillance Countermeasures, (TSCM).

4.3 Director of Central Intelligence Directive (DCID) 6/3. Protecting Sensitive Compartmented Information, (SCI) within Information Systems.

4.4 SPB Issuance 00-2 (18 January 2000). Infrastructure Surety Program (ISP) and the Management Assessment Tool (MAT).

5.0 Definitions

5.1 Critical Infrastructure Item. Any component or group of components that provides essential functions or support to the SCIF operation, or that is relied upon as an isolation component/device to assure that SCIF-based telecommunications cannot be electronically accessed to exploit information. Examples include: uninterrupted power sources (UPS); computerized telephone system (CTS); and/or energy management systems (EMS); which provide power, telephone, lighting, and HVAC for the SCIF (which often reside outside the SCIF perimeter).

5.2 Environmental Infrastructure Systems. Those systems and devices that provide critical support to the SCIF in which sensitive information processing takes place. The denial or degradation of environmental/ infrastructure systems will have a cascading effect on the denial or degradation of information processing and information availability. Therefore, this annex will address the minimum protection necessary to ensure a continuity of service to thwart the effects of denial of service attacks or external manipulation of environmental/infrastructure systems.

5.3 Sensitive Information. Information requiring safeguards per US Government directives for information such as: classified national security information (CNSI), sensitive compartmented information (SCI), restricted data (RD), sensitive but unclassified (SBU) information, and For Official Use Only (FOUO).

5.4 Site Security Personnel. Individual(s) responsible for SCIF security, including physical and technical security, and information protection. This term is synonymous with the Special Security Officer (SSO), Special Security Representative (SSR), Contractor Special Security Officers (CSSOs), Facility Security Officer (FSO), Facility Security Manager (FSM), and others; which may be agency specific terms.

5.5 Wireless. Any communications path or method that does not rely totally on a copper wire or fiber for its transmission medium, i.e., infra-red (IR), radio frequency (RF), etc.

5.6 Computerized Telephone System (CTS). A generic term used to describe any telephone systems that use centralized stored program computer technology to provide switched telephone networking features and services. CTSs are referred to commercially by such terms as computerized private branch exchange (CPBX), private branch exchange (PBX), private automatic branch exchange (PABX), electronic private automatic branch exchange (EPABX), computerized branch exchange (CBX), computerized key telephone system (CKTS), hybrid key systems, business communications systems, and office communications systems.

[1] A controlled building or compound is one to which access is restricted and unescorted entry is limited to authorized personnel.

[2] This requirement does not apply to the GSA approved Class 5, 6, and 8 vault doors.

[3] This should be interpreted to mean any windows which are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the window the windows, (e.g., electrical transformer, air conditioning units, vegetation or landscaping which can easily be climbed, etc.).

[4] Superseded Annex B dated 27 May 1994.

[5] Superseded Annex F dated 5 June 1998.

[6] Superseded Annex G dated 29 July 1994.

[7] On-hook audio protection is the assurance that a telephonic device does not pick-up and process audio when the phone is hung-up and considered to be idle. Off-hook audio protection is the assurance that when the phone is in use, but temporarily unattended, that near-by audio is not picked up and processed through the use of a "hold feature" or a push-to-talk handset.

[8] Telecommunications cabling includes all cables used to support SCIF operations, to include wiring for fire annunciation and evacuation systems which may only run throughout the building, but may not be connected to the PSTN.

[1][1] A controlled building or compound is one to which access is restricted and unescorted entry is limited to authorized personnel.

[2][2] This requirement does not apply to the GSA approved Class 5, 6 and 8 vault doors.

[3][3] This should be interpreted to mean any windows which are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows, (e.g., electrical transformer, air conditioning units, vegetation or landscaping which can easily be climbed, etc.).

[4][4] Superseded Annex B dated 27 May 1994.

[5][5] Superseded Annex F dated 5 June 1998.

[6][6] Superseded Annex G dated 29 July 1994.

[7][7] On-hook audio protection is the assurance that a telephonic device does not pick-up and process audio when the phone is hung-up and considered to be idle. Off-hook audio protection is the assurance that when the phone is in use, but temporarily unattended, that near-by audio is not picked up and processed through the use of a "hold feature" or a push-to-talk handset.

EXHIBIT #5

NOTE TO FOIA REQUESTERS

Exhibit #5 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(5)

EXHIBIT #6

NOTE TO FOIA REQUESTERS

Exhibit #6 to this report is redacted in its entirety pursuant to FOIA exemption (b)(2).

ENCLOSURE(6)

MEMORANDUM OF INTERVIEW OR ACTIVITY

Type of Activity: <input checked="" type="checkbox"/> Personal Interview <input type="checkbox"/> Telephone Interview <input type="checkbox"/> Records Review <input type="checkbox"/> Other	Date and Time: July 8, 2005 9:30 a.m.
Activity or Interview of: Samuel R. Berger	Conducted by: <div style="background-color: black; width: 150px; height: 15px; margin-bottom: 5px;"></div> <i>b6, b7C</i>
	Location of Interview/Activity: Washington, DC

Subject Matter/Remarks

On July 8, 2005, [REDACTED] interviewed Samuel "Sandy" R. Berger, former National Security Advisor (NSA) to President William J. Clinton, at the Bond Building, 1400 New York Avenue, Washington, DC. Mr. Berger participated as part of his plea agreement. *b6, b7C*

Also present were [REDACTED] *b6, b7C*

Mr. Berger described his personality as intense and a uni-tasker. He did not believe anyone would describe him as arrogant. He did not feel he was overbearing and did not seek to intimidate anyone while at the Archives. Mr. Berger provided the following information:

Mr. Berger visited the Archives, Washington, DC, to review documents requested from the Clinton Presidential materials. Mr. Berger did not have a vivid recollection of visiting the Archives on May 30, 2002, to review documents in preparation for his testimony before the Graham-Goss / Joint Intelligence Committee. Mr. Berger did recall his visits to the Archives to review documents to determine if Executive Privilege needed to be exerted prior to documents being provided to the National Commission on Terrorist Attacks Upon the United States (hereafter, the 9/11 Commission).

On every visit to the Archives, Mr. Berger came in the Pennsylvania Avenue entrance of the Archives, proceeded through the magnetometer, and signed a log book at the security desk. Someone from security called [REDACTED] office and someone from [REDACTED] office would escort Mr. Berger to [REDACTED] office. Mr. Berger always left late in the *b6, b7C*

Case Number: <div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> <i>b2</i>	Case Title: Samuel R. Berger [REDACTED] <i>b2</i>
---	--

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

2

evening, around 7 p.m. There were no guards in the lobby at that time. Therefore, no one ever checked his belongings on his way out.

██████████ was very professional and courteous. However, ██████ was not warm and "fuzzy" with Mr. Berger. ██████ told Mr. Berger he could take notes while he was at the Archives but ██████ made it clear he could not remove them. He did not understand the documents could have been sent to the National Security Council (NSC) for review and classification. [Mr. Berger did ask that his notes from his May 2002 review be sent to the NSC for review. The NSC returned his notes as classified.] He did understand the notes would remain at the Archives for him to use on subsequent visits. b6, b7C

All document reviews by Mr. Berger were conducted in ██████ office. Mr. Berger sat at a small table in ██████ office. ██████ did not brief Mr. Berger on security procedures. ██████ must have assumed a briefing was not required due to his previous positions as the NSA. ██████ did not advise Mr. Berger on what he could and could not bring into the Archives. ██████ did not provide Mr. Berger paper. On every visit, Mr. Berger brought his leather portfolio with a note pad inside. It was his practice to wear a suit but he did not recall if he wore a coat to the Archives. b6, b7C

Mr. Berger did not believe he received preferential treatment until after his visits when he learned ██████ office was not an appropriate facility to view classified material. Mr. Berger believed he was afforded the opportunity to review documents in a more comfortable environment after someone described the ██████ accommodations to him. At the time of his review, Mr. Berger did not know nor did he consider the nature of ██████ office and whether ██████. He believed he was in a suitable location to review the documents. Mr. Berger did not consider asking that the documents be sent to another location for review as he was not aware of another convenient location to conduct the review. b2, b6, b7C

Mr. Berger stated ██████ of the protocol in reviewing these records ██████ his notes had to remain at the Archives and the Archives would send them to the NSC for classification. b6, b7C

Mr. Berger made a general statement that he went to the restroom on an average of every thirty minutes to one hour to use the facilities and stretch his legs. This was the only room he went to besides ██████ office. b6, b7C

Mr. Berger explained that after 9/11, the Clinton Administration was inundated with calls on their response to this terrorist attack. It was obvious he was going to have to testify on their actions. Mr. Berger put in over 100 hours of his time, unpaid, in order to be responsive. Everyone else stepped back from the questions but Mr. Berger felt responsible.

Mr. Berger reviewed the documents at the Archives not only for privilege but also to refresh his recollection for his testimony and assisting in preparing others ██████ for their testimony. ██████ only had tangential contact with the records. Mr. Berger had unique knowledge of the records and the appropriate clearances. b5, b7C

Case Number: ██████████ b2	Case Title: Samuel R. Berger ██████ b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

3

In May or June 2003, [redacted] called Mr. Berger to say [redacted] received a request from the 9/11 Commission. [redacted] acted as the liaison between the Clinton Administration and the Archives. [redacted] asked Mr. Berger to go to the Archives to review records in response to the Executive Office of the President's (EOP) requests.

b6,
b7C

On July 18, 2003, Mr. Berger reviewed material in response to EOP 2. The boxes of materials were on a cart in [redacted] office between Mr. Berger's seat and the coffee table, or off to his side. [redacted] handed Mr. Berger "bunches" of folders. Once he completed the review, [redacted] would hand him another bunch. If [redacted] was not sitting with Mr. Berger, [redacted] was working at [redacted] desk, usually on the computer at an angle to him where he could see [redacted] over his right shoulder.

b6,
b7C

The documents were not organized chronologically. Mr. Berger would read the documents, trying to save all his questions instead of interrupting [redacted] work. He was trying to be sensitive to [redacted] work responsibilities. [redacted] and Mr. Berger would read over the documents on which he had questions. [redacted] ruled on responsiveness to the 9/11 Commission.

b6,
b7C

There were more questions to be answered in July 2003, as this was the first EOP request he was involved with. Some of the questions included what constitutes a document, does the 9/11 Commission want duplicate copies of the same information, do they want copies of the same document that contained additional notes, etc. There were two or three calls to [redacted] on these issues during Mr. Berger's review.

b6,
b7C

Mr. Berger started his own company, Stonebridge, in 2001. [redacted] had [redacted] phone number from setting up appointments for Mr. Berger's visits. He told his secretary not to call him at the Archives unless there was a time sensitive issue. His secretary probably called him at [redacted] number about a half dozen times on this visit. Mr. Berger told [redacted] he was happy to go outside [redacted] office to take the calls. [redacted] asked Mr. Berger if he needed privacy to which he said "yes." [redacted] said instead that [redacted] would go outside [redacted] office while he was on the phone, which [redacted] did. Once this pattern was established, he thought the offer for [redacted] to leave [redacted] office was "standing." [redacted]. Mr. Berger had no intent to order [redacted] out of [redacted] office. While Mr. Berger was on the phone, he was left alone in [redacted] office. He used the phone closest to the couch. It was a hard line and he wanted that privacy with his clients. Mr. Berger did not use his cell phone and never told [redacted] it was not working.

b6,
b7C

Mr. Berger could not recall specifically if [redacted] left [redacted] office when [redacted] made phone calls. The only other time [redacted] left [redacted] office during his reviews was maybe to step out to get more boxes or consult with [redacted] staff. He did not recall if any of [redacted] staff stepped in the office with him when [redacted] stepped for these moments. Mr. Berger did not take any breaks to leave the building during this visit.

b6,
b7C

[redacted]. At some point, Mr. Berger took notes. He realized he was not going to be able to reconstruct in detail all the documents he had reviewed, so he needed to take his notes with him, about ten to twenty pages.

b6,
b7C

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

At the end of the day, Mr. Berger tri-folded his notes and put them in his suit pocket. He took the opportunity to do this when [redacted] was out of [redacted] office due to him being on a private phone call. Mr. Berger said he did not recall being hesitant to remove his suit jacket during this visit. However, at some point, him not removing his jacket could have been related to the fact he placed the notes in his jacket. Mr. Berger knew he had to leave some notes behind so it would not be obvious he removed notes. He had been making notes and if he did not leave any behind it would have been noticeable. [Mr. Berger was surprised to learn he left only two pages of notes at the Archives.]

b6
b7C

The notes he removed were torn from the top of the note pad. Mr. Berger did not have time to sort through and determine which pages he wanted to take and which to leave. He said this was the scenario on all three occasions when he removed notes from the Archives. He was aware he would not have a complete set but some notes were better than none.

b6, b7C

Mr. Berger did not recall asking [redacted] to have the documents arranged chronologically on his next visit. However, he might have mentioned they were not arranged chronologically.

The Millennium Alert After Action Review (MAAR) should have been with the documents Mr. Berger was reviewing on this visit, but he does not recall seeing it. The Principals meeting was in June 2000 and invariably before these meetings a memo reflecting what they were going to talk about would have been circulated. The Principals consisted of the [redacted], and others.

b6,
b7C

Mr. Berger did not remove any documents on this visit.

[redacted] came to the Archives in July 2003, to review documents in response to EOP 2. Mr. Berger did not ask [redacted] to look for the MAAR or any other specific documents.

b6,
b7C

On **September 2, 2003**, Mr. Berger came to the Archives to review documents in response to EOP 3. Again, the boxes of materials were on a cart in [redacted] office between Mr. Berger's seat and the coffee table, or off to his side. [redacted] was working with Mr. Berger in the review of the documents. [redacted] spent about the same amount of time with Mr. Berger as [redacted] had on his visit in July 2003. Mr. Berger could not estimate a percentage on the amount of time. His recollection was that the documents were Xerox copies.

b6,
b7C

Again, [redacted] always stepped out of [redacted] office when Mr. Berger made or received phone calls. [redacted] may have also stepped out to consult with [redacted] staff, for a minute, but he has no recollection of whether [redacted] staff would step in when [redacted] was out.

b6,
b7C

Mr. Berger was not told anything about the process of the documents after his review and their presentation to the 9/11 Commission. It never occurred to Mr. Berger that by removing the MAAR from the Archives, it would not be provided to the 9/11 Commission. It was his assumption the box of documents he was reviewing at the Archives, or a copy of them, was going from the Archives to the

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

5

White House. He did not assume that his removal of documents kept them from going forward to the 9/11 Commission. Mr. Berger knew he was not reviewing originals.

In late November and early December 1999, there were five to fifteen [terrorist] attacks. During this time, the Principals met every day for about an hour. They were operating more like a working group to get through the millennium. During this time, Ahmed Ressam was caught in Washington State with explosives to be used at the Los Angeles International Airport.

After the millennium, Mr. Berger asked [REDACTED], to prepare the MAAR to determine where they were exposed and the vulnerabilities. There were fights over the jurisdiction of the funding. In March 2001, the Principals approved the recommendations and they were funded. After 9/11, the MAAR was widely discussed in the press. Mr. Berger commented the MAAR was not the most sensitive document he reviewed at the Archives. b6, b7C

Mr. Berger believed the MAAR was widely distributed among the FBI, the CIA, and the Department of State, for a total of about fifteen people. The MAAR was circulated three to four times to four or five people at each agency. All these agencies were subject to the EOP requests. [REDACTED] was going to testify concerning the MAAR. b6, b7C

Mr. Berger read through the MAAR and took notes. There were twenty-nine topics for recommendations under four categories. He thought the 9/11 Commission would want to know what the Clinton Administration did to "fill in the holes." He was trying to move quickly through the document review. [REDACTED] had told him he still had three more days' worth of documents to review. Mr. Berger now says it was a foolish decision to take the MAAR and the notes out of the Archives. b6, b7C

Mr. Berger believed this MAAR to be the final report. However, this would have been more likely if this version had a cover page/sheet. Mr. Berger did not return the MAAR to the pile that was returned to [REDACTED]. He did not have a recollection of putting other documents in this folder but he did have the intent to take the document. [There were two documents in what had been an empty folder after he removed the MAAR. [REDACTED] archivists did not move any documents into this folder.] He did not put any intentional markings on the documents. Mr. Berger did not recall receiving this folder separately from other folders. He did not recall seeing any other versions of the MAAR on this visit. b6, b7C

During this visit, Mr. Berger received more calls as there were two op-ed articles out. One article stated Sudan offered Osama Bin Laden to the United States in 1996 but the Clinton Administration did not take the offer. Mr. Berger referred to this as an urban legend. The other article was by former Secretary of Defense Casper Weinberger who said the Clinton Administration was responsible for the attacks on September 11, 2001. These articles initiated a "flurry" of activities.

Mr. Berger took the first opportunity when [REDACTED] was out of [REDACTED] office to remove the document. He most likely put it in his jacket pocket, after folding it, but he does not have a precise recollection of where he put the document. It is perceivable he put it in his pants pocket. It was also possible he placed it in his portfolio and took it out. The document was twelve to thirteen pages. The notes were folded and put in his pocket. He would have put the notes on his person at the end of the day. b6, b7C

Case Number: [REDACTED] b2	Case Title: Samuel R. Berger [REDACTED] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Mr. Berger did not believe [redacted] personnel were suspicious that he was removing documents. They did not give him any indications of this.

6
b6
b7c

Mr. Berger denied removing any documents in his socks. [He asked us to describe what the potential witness saw, which we did.] He stated his shoes frequently come untied [To which [redacted] said he was a witness.] and his socks frequently fall down. [At that point, Mr. Berger lifted his pant leg to reveal a sock falling down his ankle and pale skin.] Besides, it would have fallen out of his sock. He said this story was absurd and embarrassing.

b6
b7c

After leaving the Archives for the day, Mr. Berger went back to his office and put the document in an envelope on his desk.

On September 2, 2003, Mr. Berger called someone who was helping him review materials. He told them they should be prepared to answer the 9/11 Commission's questions concerning the MAAR.

It was asked that [redacted], former Clinton staffer, be cleared to review these documents. Mr. Berger had not worked on a document search in thirty years. If he was working at the NSC, this is certainly something someone on his staff would have done for him. [redacted] was able to [redacted] cleared for [redacted] material but the [redacted] clearance.

b2
b6, b7c

On October 2, 2003, Mr. Berger was reviewing documents at the Archives. The documents were in accordion files. [redacted] had the documents in a box, on the floor, by [redacted] desk. The time [redacted] spent with him in reviewing the documents did not change. He did not recall NARA staff being more or less restrictive with the documents than on other visits.

b6
b7c

[redacted] first provided Mr. Berger the documents marked for review by [redacted]. A version of the MAAR was with these documents, marked [redacted]. Mr. Berger did not know why it was classified differently than the version he removed in September which was [redacted]. It was obvious to him this was a different version of the MAAR. Mr. Berger wanted to know how it was edited to now be classified as [redacted]. He needed to compare the two versions of the MAAR. [redacted] had mentioned the MAAR went through several iterations but the changes were over money not substantive. Mr. Berger placed this version under his portfolio while [redacted] assistant was in the office. He then returned the folder to [redacted] assistant. Mr. Berger has no recollection of post-it notes on this document or moving them to another document. The assistant was standing in the area by [redacted] desk where the files were.

b2
b6, b7c

Next, [redacted] provided him all but two documents the White House had sent back from the documents he reviewed for EOP 2. [The White House sent those two documents on to the 9/11 Commission.]

b5, b6
b7c

[redacted]

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

7

Then they turned to the documents of the day. This time, the emails were organized. He recalled being handed the documents individually, not in a folder. About mid-day, Mr. Berger came across another version of the MAAR. In October, Mr. Berger saw a version of the MAAR and now had doubts that what he removed in September was the final report. At this point, he wanted to track the evolution of the MAAR. He slid the document under his portfolio.

██████████ told Mr. Berger there was a missing document, one that ██████████ could not find. Mr. Berger said at this point "the bomb should have burst in the air, but obviously it did not." However, Mr. Berger did apprehend the consequences of what ██████████ said. Mr. Berger disassembled first, then he asked ██████████ if the document could have been misfiled. ██████████ said "No." Mr. Berger asked if they had not produced this document already. ██████████ said it was a different version.

██████████ gave him another copy of the document. Mr. Berger slid this document under his portfolio also. ██████████ did not ask for it back. If ██████████ had asked for it back, it would have "triggered" a decision for him to give the documents back.

In total, he removed four documents, all versions of the MAAR. Mr. Berger does not recall if he placed all the documents on his person at once or at different times. He did not put the documents on his person until he was alone. He removed the notes, about fifteen pages, towards the end of the day.

Mr. Berger had a long day and wanted to go home around 6 p.m. ██████████ wanted him to finish the review and said they only had about an hours worth of work left. He understood ██████████ was getting pressure from the White House to provide a response so he agreed. ██████████ suggested he take a walk and come back and finish up. Mr. Berger left the building with all the documents he put in his pockets. He was aware of the risk he was taking, but he also knew ██████████.

Mr. Berger exited the Archives on to Pennsylvania Avenue, the north entrance. It was dark. He did not want to run the risk of bringing the documents back in the building risking the possibility ██████████ might notice something unusual. He headed towards a construction area on Ninth Street. Mr. Berger looked up and down the street, up into the windows of the Archives and the DOJ, and did not see anyone. He removed the documents from his pockets, folded the notes in a "V" shape and inserted the documents in the center. He walked inside the construction fence and slid the documents under a trailer.

Mr. Berger came back into the building without fearing the documents might slip out of his pockets or that ██████████ and ██████████ staff would notice that his pockets were bulging. ██████████

If Mr. Berger had been aware ██████████ staff was tracking the documents he was provided, he would not have removed them. He also said that if staff had escorted him out of the building for his walk, he would have felt less confident that no one was in the area and someone might be watching his actions.

Case Number: ██████████ b2	Case Title: Samuel R. Berger ██████████ b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

8

Mr. Berger does not recall reviewing his notes or [REDACTED] notes on this visit. b6, b7C

It is possible that [REDACTED], stopped by to introduce [REDACTED] but Mr. Berger did not have a vivid memory of this. b6, b7C

Mr. Berger was trying to balance his review carefully but was also trying to be expeditious. He skipped meals and drank diet cokes. He did go to the restroom, possibly with documents in his pockets, but did not discard documents there or rearrange them on his person. b6, b7C

On this visit, [REDACTED]

[REDACTED] did not tell Mr. Berger that [REDACTED] had numbered the documents or that [REDACTED] had a way of tracking these records. Mr. Berger said he would have "picked-up" on that comment. He said "I may be stupid, but I am not self destructive." As he left for the day between 7 and 7:30 p.m., [REDACTED] asked Mr. Berger [REDACTED]. He totally missed that signal later realizing it was [REDACTED] subtle way to ask him if he removed documents. Mr. Berger believed no one knew he removed documents. b6, b7C

Mr. Berger left the building, retrieved the documents and notes from the construction area, and returned to his office.

On **October 4, 2003**, late in the afternoon, [REDACTED] called Mr. Berger to tell him [REDACTED] called from the Archives. Mr. Berger was aware [REDACTED] was the [REDACTED]. [REDACTED] said documents were missing after Mr. Berger's visit on October 2, 2003. Mr. Berger panicked because he realized he was caught. Mr. Berger lied to [REDACTED] telling [REDACTED] he did not take the documents. b6, b7C

Mr. Berger remembers next calling [REDACTED] at [REDACTED] office. He knew it was not a good sign [REDACTED] was there on a Saturday. [REDACTED] described the documents stating there were four copies of three documents missing. Mr. Berger asked [REDACTED] if the four documents they were missing were copies of the MAAR. He told [REDACTED] he would see if he accidentally took them. Mr. Berger was agitated because he realized he was caught. b6, b7C

[REDACTED] called Mr. Berger and said "I hope you can find them because if not, we have to refer this to the NSC's [REDACTED]." [REDACTED] did not say what would be done if Mr. Berger returned the documents. When asked again, Mr. Berger became unsure whether [REDACTED] said this to him. However, he was sure the source of the statement was [REDACTED] asked Mr. Berger to go to his office to see if he could find the documents. b5, b6, b7C

Mr. Berger drove to his office late that afternoon. On the night of October 2, 2003, he had destroyed, cut into small pieces, three of the four documents. These were put in the trash. By Saturday, the trash had been picked-up. He tried to find the trash collector but had no luck. Neither [REDACTED] nor [REDACTED] offered to help him look through the trash. b6, b7C

Case Number:

b2

Case Title:

Samuel R. Berger [REDACTED]

b2

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

9
b6,
b7c

About 7 p.m., Mr. Berger called [redacted] and said "I think I solved the mystery." [redacted] said [redacted] was going into [redacted] and would call as soon as it was over. About 11:30 p.m., Mr. [redacted] called Mr. Berger. Mr. Berger told [redacted], "I found two documents but not the other two." [redacted] told him to get the documents from his office and lock them in the safe in his home. [redacted] was glad he found two but three were still missing.

Mr. Berger did not recall [redacted], unless [redacted] picked-up the documents.

b6, b7c

On **October 5, 2003**, Mr. Berger recalled NARA staff picking up the two documents at his home. He understands that NARA staff recalled picking up the documents at his office. Mr. Berger was willing to accept that NARA staff came to his office.

There were additional conference calls. [redacted] was surprised when Mr. Berger returned the documents he removed in September. He knew he was caught, so he purported he must have removed the documents accidentally or inadvertently by sweeping them up with his documents. Later, Mr. Berger made a decision, on his own, to tell the truth. He said "I realized I was giving a benign explanation for what was not benign." Mr. Berger wanted to return everything he had taken. He realized he was returning documents he removed in September. He did not realize he returned more than they knew he removed. Mr. Berger was aware of the consequences but he knew returning the documents was the right thing to do.

b6, b7c

Mr. Berger called [redacted] told [redacted] what happened, and asked what he should do. [redacted] told Mr. Berger to get a lawyer. Mr. Berger and [redacted] did not discuss this issue any further as they were [redacted] and knew it was better not to talk about this.

b6,
b7c

Mr. Berger specifically recalled returning his notes to NARA staff at his home. He had flown in from New York, spent about an hour at his home, then flew back to New York to continue his travel. NARA staff never mentioned his notes. Mr. Berger believed if he had not returned them, they would never have known he removed his notes.

Mr. Berger does not know [redacted], nor did he have any contact with [redacted]. Mr. Berger had not met [redacted] prior to these visits to the Archives. Additionally, he did not contact the NSC on this matter.

b6,
b7c

There were not any handwritten notes on the documents Mr. Berger removed from the Archives. Mr. Berger did not believe there was unique information in the three documents he destroyed. Mr. Berger never made any copies of these documents.

Mr. Berger said as a general point, he has dealt with classified information for twelve years. Some documents are sensitive and some are not super sensitive. This may not have anything to do with the documents classification. Other documents he reviewed had more sensitive information in them such as the Presidential Findings. He had seen most of the information in the MAAR disclosed in the press. He substituted his sense of sensitivity instead of thinking of classification. The MAAR did not involve sources and methods. It was a policy document.

Case Number: [redacted] <i>v2</i>	Case Title: Samuel R. Berger [redacted] <i>b2</i>
--------------------------------------	--

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

Some of the notes he removed did have information about the Presidential Findings. This was the authority from the President for actions to be taken.

██████████ had no reason to believe he was not acting in an appropriate manner. Mr. Berger said if there was always someone with him, he would not have taken any documents. After learning he was given special treatment by viewing the documents in ██████████ office, he suggested no exceptions to the rules should be given to former National Security Advisors or others. The Archives should thoroughly check people when they enter and exit the building. *b6, b7C*

Mr. Berger received enough phone calls which gave him the opportunity to remove the documents. He never sent ██████████ out of the room for the sole purpose of removing the documents. *b6, b7C*

The DOJ asked Mr. Berger if he removed any other documents from the Archives that we were not aware of to which Mr. Berger replied no.

Case Number: ██████████ <i>b2</i>	Case Title: Samuel R. Berger ██████████ <i>b2</i>
--------------------------------------	--

EXHIBIT #8

NOTE TO FOIA REQUESTERS

Exhibit #8 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(8)

b6, b7C

He walked out the door and into the hallway. The door closed. Shortly after it closed, started down the hall, he was stooped over right outside the doorway. He was fiddling with something white which looked to be a piece of paper or multiple pieces of paper. It appeared to be rolled around his ankle and underneath his pant leg, with a portion of the paper sticking out underneath.

ENCLOSURE(9)

EXHIBIT #10

NOTE TO FOIA REQUESTERS

Exhibit #10 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(10)

EXHIBIT #11

NOTE TO FOIA REQUESTERS

Exhibit #11 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(1)

EXHIBIT #12

NOTE TO FOIA REQUESTERS

Exhibit #12 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(12)

EXHIBIT #13

NOTE TO FOIA REQUESTERS

Exhibit #13 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(13)

EXHIBIT #14

NOTE TO FOIA REQUESTERS

Exhibit #14 to this report is redacted in its entirety pursuant to FOIA exemption (b)(2).

ENCLOSURE(4)

EXHIBIT #15

NOTE TO FOIA REQUESTERS

Exhibit #15 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(15)

EXHIBIT #16

NOTE TO FOIA REQUESTERS

Exhibit #16 to this report is redacted in its entirety pursuant to FOIA exemptions (b)(2), (b)(5), (b)(6), and (b)(7)(C).

ENCLOSURE(16)

MEMORANDUM OF INTERVIEW OR ACTIVITY

Type of Activity: <input type="checkbox"/> Personal Interview <input type="checkbox"/> Telephone Interview <input checked="" type="checkbox"/> Records Review <input type="checkbox"/> Other	Date and Time: June 2005
Activity or Interview of: Verification of Documents	Conducted by: <div style="background-color: black; width: 150px; height: 15px; display: inline-block;"></div> <i>b6, b7C</i>
	Location of Interview/Activity: Archives I, Washington, DC

Subject Matter/Remarks

This verification was done in [redacted] by [redacted]. This verification was done with the assistance of [redacted] and [redacted], in June 2005. Spreadsheets were generated in this verification process. They show the files identified as served on each visit and detailed notes. *b2, b6, b7C*

First, we went through all the [redacted] boxes [redacted] and recorded the information from all the "out cards" placed in those boxes. (If the box was sealed we interpreted that to be indicative it had not been opened since it arrived.) The out-cards were different colors to distinguish between the out-cards left behind from the Clinton Administration. *b2, b6, b7C*

Next we went to the boxes which were provided to Sandy Berger on May 30, 2002. We verified each National Security Council (NSC) numbered package he was provided was still available as a package. We cannot verify each page is intact. The originals were unassembled, photo copied, and then reassembled in the same order by [redacted]. (This negated the need to look for torn corners still remaining in the packages.) Each package may contain multiple documents which may or may not be numbered sequentially. Some pages contain changes and only those pages are attached, not the full document. *b6, b7C*

We verified each SMOF folder was still at NARA. We cannot verify the content of each folder. (We know documents had been removed from the folder titled [redacted] and others placed in the folder.) [redacted] has a file folder list but not a document level inventory. (Box 49 is the exception because the folder titles do not match the contents list.) The file folder lists reflecting the titles were with [redacted]. *b2, b6, b7C*

For the documents Mr. Berger was served in May 2002, we verified all the NSC numbered packages and the Staff Member Office Files (SMOF) folders [redacted]. (Whole SMOF files were *b2, b6, b7C*

Case Number: <div style="background-color: black; width: 100%; height: 15px;"></div> <i>b2</i>	Case Title: Samuel R. Berger <div style="background-color: black; width: 50px; height: 15px; display: inline-block;"></div> <i>b2</i>
---	--

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

2

provided to Mr. Berger but we believe [redacted] placed the documents [redacted] deemed non-responsive in an envelope in the back of the SMOF file.) For the May 2002 visit, no one reviewed documents pulled [redacted]. Mr. Berger took notes and left them with [redacted] to send to the NSC for classification. These were classified [redacted] [Note: Mr. Berger's notes reflected he reviewed a document similar to Millennium Alert After Action Report but not a copy of it. This document is believed to still be at NARA.]

b2,
b6,
b7C

For the documents Mr. Berger was served in July 2003 [EOP 2], we verified all NSC numbered packages and SMOF folders [redacted]. We did not verify any page counts as Mr. Berger was provided with original NSC numbered packages and original SMOF folders (with the responsive documents tabbed).

b2, b6,
b7C

Mr. Berger took notes on a notepad he brought to NARA. Mr. Berger stated he removed notes when [redacted] left [redacted] office. He later provided these notes to [redacted]. Two pages of notes were turned over by [redacted] with an annotation indicating the notes were from Mr. Berger's July 2003 review. Two pages of notes remain [redacted] from this visit.

b2,
b6, b7C

For July 2003 [EOP 2], [redacted] reviewed the documents pulled at [redacted] and sent to [redacted]. Mr. Berger did not review these documents at this time.

b6,
b7C

For the documents Mr. Berger was served in September 2003 [EOP 3], we verified all the NSC numbered packages and SMOF folders [redacted]. The SMOF files were reviewed and responsive materials were tabbed. Copies were made of the tabbed materials and served to Mr. Berger. We compared the items served to Mr. Berger and the tabbed documents from the SMOF files to verify page counts. The NSC numbered documents were not verified for page count as originals were served.

b2, b6,
b7C

[redacted] had sent up copies of documents responsive to EOP 3 which Mr. Berger reviewed. At one point, after it was discovered Mr. Berger removed documents, [redacted] requested [redacted] send up the cover sheet of each document along with the page count of the document. [redacted] verified the page count provided by [redacted] was the same as the copy set provided to Mr. Berger. This was verified again during this review.

b6,
b7C

In September 2003, emails were provided to Mr. Berger (see notes under ADDITIONAL CLARIFICATION).

Mr. Berger said he removed notes on the September visit.

For the documents Mr. Berger was served in October 2003 [EOP 3], we verified the page count of the copies of the NSC numbered documents provided to Mr. Berger with the page count of the original NSC numbered documents. (Keep in mind there is no way to verify all the pages of the original NSC numbered documents were accurate as Mr. Berger had access to some or all of these originals in May 2002; and July and September 2003.)

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

The documents were not in chronological order. Email #150 was placed at the front of the file so Mr. Berger would readily see it.

The SMOF files were reviewed and responsive materials were tabbed. Copies were made of the tabbed materials and served to Mr. Berger. For some reason (possibly the 9/11 commissions review) the tabs were removed. Instead, we compared the items served to Mr. Berger with the tabbed documents from the files to verify page counts.

This accounted for items numbered by [redacted] as 339 – 379. Items 1 – 338 are emails (see notes below). b2

ADDITIONAL CLARIFICATION:

The original recovered documents are [redacted] at NARA. The original recovered notes are at the FBI. b2

It was determined that it would be unrealistic to take Mr. Berger's notes and try to match them to each review. This is problematic as Mr. Berger's notes are not dated. His notes do not reference a document number or SMOF title, only a date. The boxes of what was produced on each visit do not exist as they did and it would take a considerable effort to recreate those. Also, Mr. Berger may have annotated in his words or from his recollection instead of taking exact notes off a document.

When pulling emails for EOP3, [redacted] used the search string provided by the NSC. [redacted] also searched by individual names and additional terms. [redacted] sat at the computer and reviewed the emails. If [redacted] thought they were non-responsive, they were never printed. [redacted] wrote the file number on the back of each email. After [redacted] printed the email, they were reviewed again for responsiveness, possibly by [redacted]. b6, b7C

To re-create this search for the email, [redacted] would have to determine the search terms and then filter out what [redacted] believed to be non-responsive. The remaining emails could be printed and compared to the emails provided to Mr. Berger for EOP3. Any emails for which there was not a duplicate copy could be reviewed again for responsiveness. This might give you emails which might be missing. This review would involve looking at a couple thousand emails. Currently, there is a problem with the email server and it is not accessible. b6, b7C

Case Number: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2
-------------------------------	---

From: GaryM Stern
To: John.Carlin@nara.gov,Lewis.Bellardo@nara.gov,Lori.Lisowski@nara.gov,Richard.Clayp
oole@nara.gov,Sharon.Fawcett@nara.gov,Susan.Cooper@nara.gov,John.Constance@nara.gov
Date: 8/8/04 10:41PM
Subject: House Investigation re Berger

In case you hadn't seen it, below is the story in Saturday's NY Times about the letter Waxman sent on Friday to Ashcroft concerning DOJ's decision to let us cooperate with the House investigation. That letter refers to a document request that we received on Friday from Chairman Davis. The letter is posted here: <http://www.house.gov/reform/min/>

Thus, I will be downtown on Monday morning working with (b) (6) on responding to the document request.

Note, however, that the interview(s) that were supposed to begin on Wednesday have been postponed until the end of the month.

August 7, 2004
Ashcroft Is Asked to Explain Department Role in Berger Case
By CARL HULSE

WASHINGTON, Aug. 6 - A top House Democrat called on Attorney General John Ashcroft on Friday to explain why the Justice Department was letting federal officials cooperate in a Congressional inquiry into the case of Samuel R. Berger despite a current criminal investigation.

The representative, Henry A. Waxman of California, the senior Democrat on the Government Reform Committee, said the department position regarding Mr. Berger, a national security adviser to President Bill Clinton accused of mishandling classified documents, was at odds with how inquiries tied to the Bush administration had been handled.

"For example, in the investigation into the leak of the identity of covert C.I.A. agent Valerie Plame, officials have said repeatedly that they cannot comment because the matter is currently under investigation," Mr. Waxman wrote. He said the policy was "intended to maintain the integrity of the investigation and protect the individuals involved."

The panel chairman, Representative Tom Davis, Republican of Virginia, called on the National Archives and Records Administration this week to provide materials related to Mr. Berger, who has acknowledged improperly removing documents from the archives last year but has said it was inadvertent.

Among the items Mr. Davis sought were internal archives communications about Mr. Berger's actions as well as the documents that granted him access to the classified papers while he prepared for an appearance before the Sept. 11 commission.

"The unauthorized removal of such documents raises serious questions as to N.A.R.A. procedures and policies in place to protect such important records and raises specific questions as to whether the 9/11 commission received all relevant requested documents," Mr. Davis wrote in a letter on Wednesday.

Mr. Davis's determination to investigate the Berger case has created a dispute with Mr. Waxman and other Democrats. They accuse the chairman and the House Republican leadership of applying a double standard since they have rejected Democrats' calls to look into the disclosure of Ms. Plame's identity and other matters related to Iraq.

Mr. Davis and his allies reject the assertion of unfairness. A committee spokesman said the investigation of Mr. Berger's handling of the classified documents went beyond the criminal aspect into questions of security at the archives, a matter under the panel's jurisdiction.

From: Paul Brachfeld
To: Bellardo, Lewis; Carlin, John; Claypoole, Richard; Constance, John; Fawcett, Sharon; Lisowski, Lori; (b) (6); Stern, GaryM
Date: 7/20/04 11:15AM
Subject: Re: proposed statement re Berger

I will not comment on Susan's language. (b) (5)

>>> Richard Claypoole 07/20/04 11:03AM >>>

(b) (5)

>>> Lewis Bellardo 07/20/04 10:57AM >>>

This looks good. (b) (5)

Lew

>>> Sharon Fawcett 07/20/04 10:52AM >>>

I think it's a good statement and shows we did the proper thing.

>>> Susan Cooper 07/20/04 10:51AM >>>

After a long conversation with (b) (6) and Gary, we came up with the following proposal for you all to consider. This would not be issued as a formal statement, but would be used in response to questions from the media.

(b) (5)

CC: Cooper, Susan; (b) (6), (b) (7)(C)

**Memo to the File about Incidents relating to 9/11 Commission Document
Production**

October 28, 2003

On the morning of October 6, 2003, John Carlin, Archivist of the United States briefed me regarding an apparent security breach involving Sandy Berger using records in the Archives I facility and apparently removing copies of classified records from the building. Carlin briefly recounted an episode in the document review area and described activities of (b) (6) of the Office of Presidential Libraries, Gary M. Stern, our General Counsel, and Stephen Hannestad, our person in charge of information security and the Archivist to investigate the matter and to try to recover missing documents.

Carlin stressed that he wanted me to take over and direct the review, decide how to handle the matter from a policy and legal perspective and to develop policies and procedures to minimize reoccurrence. I was subsequently briefed by Stephen Hannestad, Gary M. Stern, and (b) (6), who was the Office of Presidential Libraries manager who was present during the incident and events leading up to the apparent breach.

Jess Bellack
10/28/2003

10/7/03

5/18
Time
Laid out

Re-NSC Meeting

NSC attorney
→ all information

Return not

info. not pursued as secret

(b) (6)

10/17
Cover

Security Issue

(b) (6)

Review of statute
& laws violat

Product: ~~_____~~

criminal referral
include counsel
with Justice
in return
Attempts to obstruct
disclosure Request
not a subpoena

IF we provided records

9/2 → (b) (6) -
10/2 - (b) (6) (b) (6) -

how do we know we supplied

everything relevant

Production to White House
→ 9/11 Commission
Number

see Sept 2 - double
check anything might have
been missing for the White House

← EOP → 3 1st part
 9/2 → Produced report
 Little Rock &
 here
 Little Rock may have
 control set

① need to verify

We think we would have made copies

② ← need ~~of~~ recreate the search
 Search & Production —

also need closely

(b) (6)

← memo for the record ↔ memo for record

← information held closely →

Oct-9 2003

(b) (6)

→ Sandy Beys

too highly classified - 3 people (b) (6) (b) (6) (b) (6)

Day only to courier that material

May 30, 2002 - Senate Intelligence Committee what we knew about 9/11 +

(b) (6) Sandy Beys (b) (6)

NSC send letter saying Sandy the only one with the clearance

Little Rock - has some of the material - but not briefed into the program

May 30, 2002 - looked at Wash Boxes NSC - Washlyt

Looked at 3 boxes - Ken Campbell, Tiger Ferguson, Wing decided we would be to go

He was fine

Accessed out of (b) (6) office -

(b) (6) has been pushing for CIA Research room for 2 years

but delayed 3 weeks -

Nothing unusual - in behavior

clearly was of this program

office cleared for top secret

Copyright
~~Executive~~ Commission → but not on que
business of Congress
(2) ~~Request~~

On pay business of The President

→ Negotiated with Bush/NX
advice

June 4⁰³ ~~2003~~ The request

We alert former Pres. Reps

1998 - 2001 - similar lead

Structured - requests for records part
of formal NSC structure

Again (b) (6) said only SA only cleared
in → clearing - tried to get someone
else - (b) (6)

but his clearance had expired - we
tried to get renewed - Sandy tried to
to get ~~somebody~~ to not have to
come in - He was ~~permitted~~
forwards about hours
to come in

July 18, 03 - We had records for how
EOP - 2 - 1st for US

wash materials - reviewed only
wash stuff -
little bit reviewed by

(b) (6)

Originals were given to him to
~~review~~ for responsiveness

(b) (6) reviewed full record & this
at ~~request~~ request - that there be one person
day all

Originals were tabbed with etc

7/18 - access in (b) (6) office
she monitored

No problem - ^{except} he didn't keep
in actual hallway - she was called over
constantly to comment on each document

→ before she ~~was~~ enjoying with ^{over} hallway
So 2 she told staff

~~***~~ (b) (6) ^{thinks} ~~was~~ That visit of ~~the~~ ~~times~~
in later visits he asked to leave after
because of a confidential phone
call.

So she told staff that if he ~~calls~~ ^{comes} back
now easily organize & wherever we can
Xerox ~~of~~ or ~~where~~ ~~to~~ organize
better -

EOA 3 request - June -
It is broken

9/2 - 1st visit to Review EOA 3
Now only Sandy only - because different
views of relevances - told (b) (6) best to have
only 1 person - (b) (6) in Florida -
Sandy ~~is~~ is unhappy -



(b) (6) ^{hit} ~~not~~ ~~to~~ ~~do~~ ^{into} ^{secret & confidential}
~~level~~ ~~around~~ ^{So} (b) (6) reviewed the lane
9/2 ^{found} ~~all~~ ~~text~~ ~~to~~ ~~be~~ ~~done~~ Xerox ~~of~~ copies - all little Rob

all office files for West
only NSC originals ^{log} are The Numbered Documents

T. S. ^E item for Little Rock - stand up.
+ To Cook - W. staff - July 22nd ~~item~~

we know this is the item
returned on last
Sunday, the 5th of Oct.

9/2 access in (b)(6) office & (b)(6)
~~system~~

He asks to make private phone calls -
But not secure
But he had to go to the bathroom a
lot
At End of The Day. Staff that
saw outside of the office heard door
fiddle with paper
- Staff member didn't know for sure -

so she not sure
element of doubt - let's only send
him Xerox copies 2 # book of documents
mentioned to show - But found
National Security Advisor

NSC says get pages in as quickly as
possible
No collation made with
~~out~~ Originals & copies
yet

Still trying to **(b) (6)** cleared in —
 Practice is to retain of central set of what
 sent to white House —
 [We have ~~two~~ copies —
 We have left originals all filed together
 we can compare originals & copies in
 little book & was
 Only ~~three~~ ^{three} can track originals —
 But can't be ^{absolute} sure —

10/2 visit — call Xerox girl
 and he demanded she leave for
 no such confidential phone call she
 monitoring the phone —
 phone broken
 So she returned immediately
 & he was going to ~~enter~~
 bathroom as she was coming in.
 The pink tab of **(b) (6)** note
~~one folder contains~~
 When Sandy returns the folder its in
 another document & the actual document (the copy)
 is ~~the~~ gone

(b) (6) Late afternoon — Staff # 217 is missing
 Staff - could you have monitored & if so go to vault
 & if so - we'll give him another copy I say

There is a contact system
~~by name~~

to Sandy we have
a way - + Piss # is missing from list
we showed you - Piss # is missing so
I know you haven't seen it - he says
I think I saw it -

5 minutes before bathroom + then again to
bathroom -> He finishes dinner +

says no differences with (b) (6) -

6:00 PM He just drinks diet coke - I'm blessed
eyed + have to go - she says

Take a walk around building get awake
+ come back because white House counts this
done ->

He later says he's tired -
he came back + stayed to 7:00

-> Ben try take it to the vanet

(b) (6)

-> 10/3 - she to staff check the numbers

one staff in tears - 2 missing
E mails - + (b) (6) say "150 gone"

to -

~~The same as the
related doc~~

so 3 docs -

By 10:30 am - so then she called

(b) (6)

-> He asks ^{sure it's} ~~is~~ in middle -

C-1130

(b) (6)

so she keeps rally - she gets
+ says have (b) (6) call - also messages for

207,323
L
misses
times

Gay's voice mail - She insists
not a mistake
reverts to ~~the~~ ~~the~~ ~~emails~~ -
+ she has stuff

← Gay on 400 shuttle - Gets Back 4:30

He said have to call (b) (6)
+ tried to call (b) (6)
Steve Harnestad →

She said
Gay is
this guy
did to
call.

Gay reached (b) (6) c. 900

(b) (6) called (b) (6) 9:30

she told him copies - only -
he said deal with (b) (6) + Gay

They met 4:00 pm on Saturday -

She suspected calling (b) (6) (b) (6) first →
They ~~the~~ call (b) (6) → more calls

Sandy - + Sandy says I have nothing
then (b) (6) calls back -

c. 6 or 630 Sandy calls -
I know the document -

Sandy - said you notified
Sandy calls Gary - later
+ Gay calls him at c. 11:00
+ says he went to his office + found
2 documents

Is it that
you gave
me later
- yes

(b) (6) calls (b) (6) + is concerned c. 6:40 PM

On Sunday

Obtained via FOIA by Judicial Watch, Inc.

(b) (6)

c 11/9/63

~~Old time~~

after they ^{so} picked up the documents

~~they~~

They called (b) (6) & he quiet - Sandy
said he wanted to talk to him - I said I would

Called Sandy & didn't seem like on 10/2
knew they were copies & that you could
track by him

late that night Sandy to Gay - might be
could have gotten the documents on 9/2

Then call (b) (6) on Sunday & he call
back. Sandy right

I saw no notation -

From: GaryM Stern
To: Bellardo, Lewis; Brachfeld, Paul; Carlin, John; Claypoole, Richard; Constance, John; Fawcett, Sharon; Lisowski, Lori; (b) (6)
Date: 7/20/04 11:25AM
Subject: Re: proposed statement re Berger

I think we should meet to discuss this further. Can we set up a conference call between A1 and A2?

>>> Lori Lisowski 7/20/04 11:19:31 AM >>>

(b) (5)

>>> Richard Claypoole 07/20/04 11:17AM >>>

That language is ok with me.

>>> GaryM Stern 07/20/04 11:15AM >>>

(b) (5)

(b) (5)

I am waiting to hear back from DOJ on any guidance from them about making a statement of this sort.

>>> Richard Claypoole 7/20/04 11:03:27 AM >>>

(b) (5)

>>> Lewis Bellardo 07/20/04 10:57AM >>>

This looks good. (b) (5)

Lew

>>> Sharon Fawcett 07/20/04 10:52AM >>>

I think it's a good statement and shows we did the proper thing.

>>> Susan Cooper 07/20/04 10:51AM >>>

After a long conversation with (b) (6) and Gary, we came up with the following proposal for you all to consider. This would not be issued as a formal statement, but would be used in response to questions from the media.

(b) (5)

CC: Cooper, Susan

From: (b) (6)
To: Bellardo, Lewis; Brachfeld, Paul; Carlin, John; Claypoole, Richard; Constance, John; Fawcett, Sharon; Lisowski, Lori; Stern, GaryM
Date: 7/20/04 11:39AM
Subject: Re: proposed statement re Berger

John, Lew, et al:

(b) (5)

Thank you,
(b) (6)

CC: Cooper, Susan

From: Paul Brachfeld
To: Bellardo, Lewis; Carlin, John; Claypoole, Richard; Constance, John; Fawcett, Sharon; Lisowski, Lori; (b) (6); Stern, GaryM
Date: 7/20/04 11:54AM
Subject: Re: proposed statement re Berger

I will defer to program officials at this point. (b) (5)
 [Redacted]

>>> GaryM Stern 07/20/04 11:25AM >>>
 I think we should meet to discuss this further. Can we set up a conference call between A1 and A2?

>>> Lori Lisowski 7/20/04 11:19:31 AM >>>
 (b) (5)
 [Redacted]

>>> Richard Claypoole 07/20/04 11:17AM >>>
 That language is ok with me.

>>> GaryM Stern 07/20/04 11:15AM >>>
 (b) (5)
 [Redacted]

(b) (5)
 [Redacted]

I am waiting to hear back from DOJ on any guidance from them about making a statement of this sort.

>>> Richard Claypoole 7/20/04 11:03:27 AM >>>
 (b) (5)
 [Redacted]

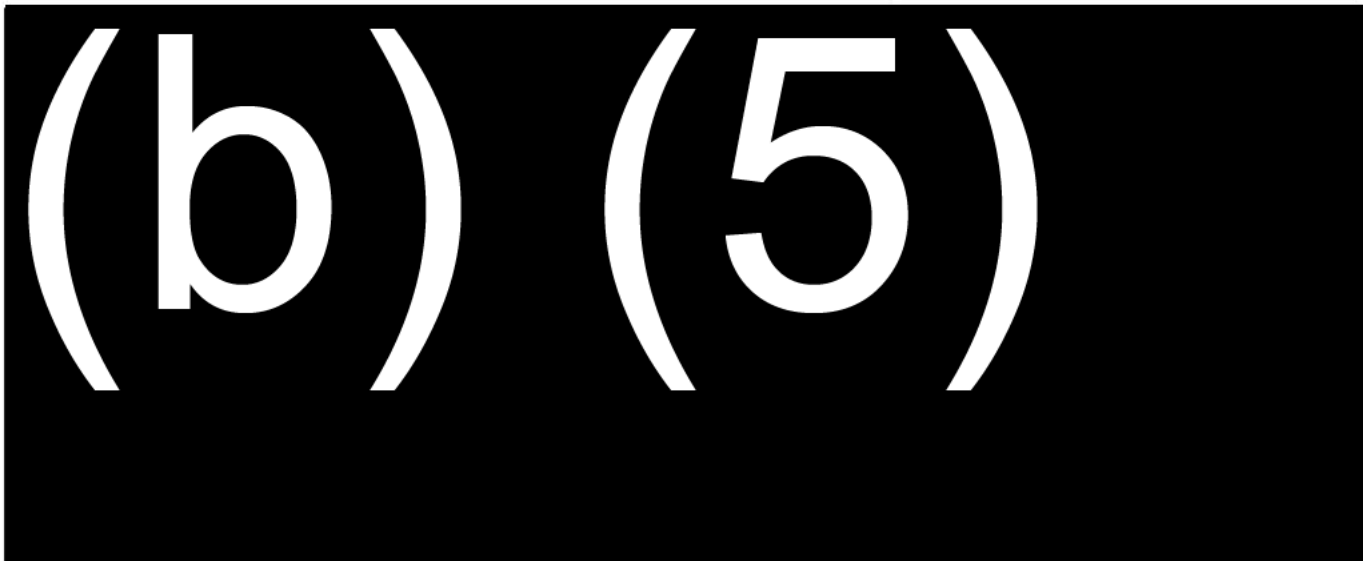
>>> Lewis Bellardo 07/20/04 10:57AM >>>
 This looks good. (b) (5)
 [Redacted]

Lew
 >>> Sharon Fawcett 07/20/04 10:52AM >>>
 I think it's a good statement and shows we did the proper thing.

>>> Susan Cooper 07/20/04 10:51AM >>>
 After a long conversation with (b) (6) and Gary, we came up with the following proposal for you all to consider. This would not be issued as a formal statement, but would be used in response to questions from the media.

(b) (5)
 [Redacted]

CC: Cooper, Susan; (b) (6), (b) (7)(C)



GARY M. STERN
General Counsel
National Archives and Records Administration
8601 Adelphi Road, Suite 3110
College Park, MD 20740-6001
301-837-1750 (main)
301-837-3026 (direct)
301-837-0293 (fax)
garym.stern@nara.gov

CC: (b) (6).A1D1P1.ARCH1D1

- Mr. Berger pled guilty on April 1, 2005. Under his plea agreement, he agreed to the following:
 - 11. The defendant agrees to continue to cooperate fully and truthfully with the United States, and provide all information known to him regarding this matter, In that regard:
 - a. The defendant agrees to continue to be reasonably available for debriefing as the United States may require, including debriefing by the Inspector General of the National Archives and Records Administration.
 - b. The defendant agrees to provide, in addition to materials already provided, all documents, records, writings, or materials of any kind, excepting those protected by the attorney-client privilege, in his possession or under the defendant's care, custody or control relating directly or indirectly to all areas of inquiry and investigation.
 - c. The defendant agrees that, upon request by the United States, he will voluntarily submit to polygraph examinations to be conducted by a polygraph examiner of the United States' choice. The defendant stipulates to the admissibility of the results of the polygraph examination if later offered in a proceeding to determine compliance with this plea agreement.
 - d. The defendant agrees that the accompanying Factual Basis for Plea is limited to information to support the plea. The defendant will provide more detailed facts relating to the case during ensuing debriefings.
- The plea agreement represented the end of the DOJ investigation of Mr. Berger. DOJ therefore had no further need to interview or debrief Mr. Berger.
- The only anticipated further debriefings of Mr. Berger were by the NARA Inspector General. It was assumed that the NARA OIG could and would request the use of a polygraph if it believed it to be necessary.
- The NARA OIG, with DOJ participation, interviewed Mr. Berger on July 8, 2005. The OIG appears to have declined its opportunity to request the use of a polygraph either during or subsequent to this interview, despite having apparent doubts as to the veracity of his testimony (as described by the IG on Fox News).

HEADLINE: JOHN MCLAUGHLIN'S "ONE ON ONE"

GUEST: ALLEN WEINSTEIN, ARCHIVIST OF THE UNITED STATES

SUBJECT: THE NATIONAL ARCHIVES

TAPED: THURSDAY, JUNE 30, 2005 **BROADCAST:** WEEKEND OF JULY 2-3, 2005

BODY:

MR. MCLAUGHLIN: The Treasure Trove. Dolley Madison risked her life and liberty to save documents preserved here. The collection includes the foundation of our liberties: the Declaration of Independence, the Articles of Confederation, the Constitution, the Bill Of Rights. There are also Cabinet minutes, White House papers and the presidential library system, including secret audiotapes and confidential memos.

What can average Americans find in this priceless legacy? Is it readily accessible? How many secrets reside in the repositories of our **National Archives**? Have any of those secrets ever been improperly penetrated and revealed? We'll ask the archivist of the United States, Allen Weinstein.

(Announcements.)

MR. MCLAUGHLIN: Dr. Allen Weinstein, it's a great pleasure having you with us, and an honor.

MR. WEINSTEIN: It's a pleasure to be here, Dr. McLaughlin.

MR. MCLAUGHLIN: Recently you brought to the Archives the new prime minister of Iraq. What did he -- what was his impression? What did he take away from your visit, and what did you show him?

MR. WEINSTEIN: Well, John, we have over a million visitors every year, and he was -- but he had the place to himself for a while. He was interested in seeing the charters of freedom. He was interested in seeing the Declaration of Independence, the Constitution and the --

MR. MCLAUGHLIN: U.N. Declaration --

MR. WEINSTEIN: -- no, no -- and the Bill of Rights, the U.S. charters of freedom.

He was also interested in the revolutionary period. Washington, of course, has fascinated him, and we spent some time with Washington's documents. He knew a great deal about

American history. Very interesting. We had a good, solid conversation about that.

He also knew a great deal about the American Revolution -- for example, that we, like so many other democracies, began with support from other countries. We began with French support. They, of course, have coalition support in Iraq. He was well aware that -- of the time that it took the United States to go from revolution to government, over a decade.

He was interested also in Lincoln and the Civil War, and we talked a lot about Lincoln, and we saw some Lincoln documents.

Then he has a very -- he had a very surprise (sic) request. He wanted to see some documents of a president -- apparently really fascinates him -- John Quincy Adams. So we showed him the Monroe --

MR. MCLAUGHLIN: Did he explain his interest in Adams?

MR. WEINSTEIN: Well, he didn't, beyond the point that he was fascinated with the father-son aspect of this. Adams Sr., Adams Jr., Bush Sr., Bush Jr.

MR. MCLAUGHLIN: Oh, I see.

Did he comment on anything, like transparency, that appears from the documents?

MR. WEINSTEIN: Well, we tried to explain that we are an access agency and that Americans are entitled to see the records of their country. And I think in fact I've been invited to come to Baghdad and see if we can't bring a delegation to advise them on organizing their own archives, which we may do.

MR. MCLAUGHLIN: You had an awful lot of experience before the Archives with the arrival of a measure of freedom for Russia, under Yeltsin and earlier, in fact, when you headed up the Center for Democracy.

MR. WEINSTEIN: That's right.

MR. MCLAUGHLIN: Is that correct?

MR. WEINSTEIN: Eighteen years.

MR. MCLAUGHLIN: You're kind of an expert on freedom, are you not?

MR. WEINSTEIN: I'm not an expert on freedom, but I spent 18 years of my life trying to help new democracies.

MR. MCLAUGHLIN: Well, you know that the Iraqis -- I don't -- did he bring any of this up? He did bring it up, apparently, indirectly, the prime minister.

And they're faced with signing a constitution, first of all, bringing it into existence by August the 15th, which is just weeks away. Do you have any impressions of whether, on the basis of your knowledge of what Russia went through, on the probability of their signing a constitution this year?

MR. WEINSTEIN: I think all that I would say, John, is that he seemed very determined on that score. He talked to the press in the Archives when we were there. And I wouldn't at this point bet against him.

But I should point out that we have a program of hosting distinguished visitors from abroad that we're getting started, because basically if they're here in the United States for a week or so visiting the president, visiting the Congress, they really ought to come to the Archives and take a look at some of the records of American history.

MR. MCLAUGHLIN: You're also familiar with the role of heads of state. President bush gave a speech this week to prepare the population, a realistic speech. It was almost tinged with a little bit of -- not pessimism, but indicating that our commitment, financial and military, is going to be more prolonged than some people think.

Do you think he was successful in galvanizing a measure of support for himself?

MR. WEINSTEIN: John, the archivist of the United States runs a non-political, totally professional operation. He is nonpartisan. Once a year I have the privilege of making a few comments, and that will be on the Fourth of July. So those who would like to hear my comments on that, I'm afraid, are going to have to come to the Archives on the Fourth of July, in which they're all invited to watch the parade.

MR. MCLAUGHLIN: What else are you going to do for the Fourth of July?

MR. WEINSTEIN: Well, we have two veterans of the Iraqi conflict, both wounded badly, both recovering, who are coming to read the Declaration of Independence with us that day.

MR. MCLAUGHLIN: Anything else?

MR. WEINSTEIN: We have games. We have dress-ups of the major leaders of the early republic. We have a number of activities. It's a two-day festival, a fiesta civica, as my Spanish friends would say, a civic festival. And it starts at the Archives on Sunday and it goes on to the Fourth of July on Monday. Everybody welcome.

Have you been there, John?

MR. MCLAUGHLIN: Where, the Archives?

MR. WEINSTEIN: Have you seen the new Public Vaults exhibit in the Rotunda?

MR. MCLAUGHLIN: No, I have not. I've seen the video that's coming out.

MR. WEINSTEIN: Well, please consider you and Cristina my guests whenever you'd like to come.

MR. MCLAUGHLIN: Well, thank you very much. I appreciate that.

MR. WEINSTEIN: Please bring the crew with you.

MR. MCLAUGHLIN: We'll get there, if not the Fourth, then later.

MR. WEINSTEIN: Whenever.

MR. MCLAUGHLIN: I know you don't want to comment particularly on the president's speech right now, but are you going to get early drafts of the speech as part of the Archives' collection?

MR. WEINSTEIN: Oh, yes. The White House -- every White House delivers over from time to time copies of virtually all of its documents, and they're held in trust until there's a presidential library to store them.

MR. MCLAUGHLIN: I was a speechwriter for President Nixon, one of that assemblage of Safire, Buchanan and Gergen and others.

MR. WEINSTEIN: I've heard them.

MR. MCLAUGHLIN: And of course there are a lot of memos written in connection with any presidential speech. This was a particularly sensitive speech, so he must get memoranda in connection with it. Will you get it at the Archives? This is more of an explication of what you do than it is --

MR. WEINSTEIN: Time will tell.

MR. MCLAUGHLIN: Time will tell?

MR. WEINSTEIN: Time will tell.

MR. MCLAUGHLIN: But you like those things, do you not?

MR. WEINSTEIN: I like the fullest possible record of every presidency.

MR. MCLAUGHLIN: Do you know that there is a school of thought that there should not be a paper trail because of the situation the way it is in America today; politicians are

trying to trap other politicians at every turn. Does that become an enemy for you, those who maintain that they should not have paper trails, or those who use the shredder?

MR. WEINSTEIN: Well, the interesting thing is, John -- it speaks to your generation and mine, because we're the same generation -- paper trails and shredders are things of the past. What we're looking at now are electronic trails. The electronic records have become the major problem we have to face at the Archives, and we're trying to confront that. We, for example, have two major companies now developing prototypes of the system that we call the Electronic Records Archive, to try to absorb the thousands and thousands of software patterns used within the federal government.

And the presidency, obviously, is one of those -- has one of those systems. So we're in the process of trying to sort of master the most complicated problem that archivists face these days, which is making certain that we don't lose most of the electronic records of our time.

MR. MCLAUGHLIN: So this is the digital age, and you have to face up to that.

MR. WEINSTEIN: We certainly do.

MR. MCLAUGHLIN: We can get into that a little bit in a moment, but I want to ask you this before -- before it escapes me, and that is: because of your close involvement with Russian democracy, do you think that Russian democracy is in any kind of peril under Vladimir Putin today?

MR. WEINSTEIN: I think Russian democracy has seen better days, let's put it that way. But keep in mind, John, that there's a major problem that's faced by all of these new democracies. The initial leaders of those democracies were trained -- were mostly opposition leaders, people who were great at protests, that were very eloquent, very, very good at organizing support for change. They were not necessarily administrators. And the changeover from opposition leaders to government leaders has been a real trial and difficulty for many of these folks. So Russia's gone through and had -- Yeltsin was a great opposition leader, not so good as an administrator. And Putin had no role particularly in the opposition before the changeover.

MR. MCLAUGHLIN: Do you think he is helped or hindered by his background in intelligence, Russian intelligence, the KGB?

MR. WEINSTEIN: I don't think it helps.

MR. MCLAUGHLIN: You do not?

MR. WEINSTEIN: Not these days.

MR. MCLAUGHLIN: So there's a lot of criminality in Russia.

MR. WEINSTEIN: Well, there's a lot of criminality in every country.

MR. MCLAUGHLIN: We'll be right back.

(Program break; music.)

MR. MCLAUGHLIN: Is eBay peddling historical pictures, autographs and documents stolen from the U.S. **National Archives**? If so, is legal action being taken against eBay, either civil or criminal? We'll put these questions to our guest. But first, here is his distinguished profile.

Born: New York City. 67 years of age. Wife: Adrienne Dominguez. Two sons, one stepson, one granddaughter. Jewish. Democrat. City College of New York, BA; Yale University MA and Ph.D., American Studies and History. Smith College, professor of History, 15 years. The Washington Quarterly, published by the Center for Strategic and International Studies, executive editor, 2 years. Georgetown University, university professor, 3 years. Boston University, history professor, 4 years. United States Institute of Peace, director, 15 years. The Center for Democracy - Washington, DC, founder and president, 18 years. **National Archives** and Records Administration -- NARA -- Archivist of the United States, 4 months and currently.

Author and co-author: eight books, including The Story of America, and The Haunted Wood: Soviet Espionage in America - The Stalin Era, and Perjury: The Hiss-Chambers Case.

Awards: United Nations Peace Medal, the UN's highest medal of honor given to an individual working for the cause of international peace, and the Council of Europe's Silver Medal, twice, for -- quote -- "outstanding assistance and guidance."

Allen Weinstein!

MR. MCLAUGHLIN: Dr. Weinstein. What is your mission at the U.S. **National Archives**, and are you able to fulfill that mission with a budget of about \$310 million?

MR. WEINSTEIN: Well, that's this year's budget, John. We hope for more.

MR. MCLAUGHLIN: Good.

MR. WEINSTEIN: The **National Archives** and Records Administration basically serves American democracy, and I'm going to read to you the very brief mission statement: "The **National Archives** preserves for the American people and their public servants the records of our federal government. We assure continuing access to the essential documentation of the rights of American citizens and the actions of government. We promote democracy, civic education and historic understanding of our national

experience."

MR. MCLAUGHLIN: So you store of billions of pieces of paper, do you not?

MR. WEINSTEIN: Over 1 billion in the building downtown alone, but the building downtown, John -- it's sometimes misunderstood -- we have four headquarters in Washington -- four different buildings. We have 11 presidential libraries that we oversee -- 11. If Nixon joins that list next year, it will be 12.

MR. MCLAUGHLIN: Well, you engineered that, did you not? Isn't that a done deal?

MR. WEINSTEIN: I encouraged the negotiation between all -- from both sides.

MR. MCLAUGHLIN: Why was there a standoff?

MR. WEINSTEIN: Well, we have an agreement. There were differences over what the library should do before it joined the system. We've come to an agreement. Now we're waiting to see the agreement --

MR. MCLAUGHLIN: Do you get clearance on the tapes?

MR. WEINSTEIN: We own -- we control the tapes, John. The **National Archives** now has all of the Nixon -- under federal statutes and federal law, we have that material.

MR. MCLAUGHLIN: They will stay with the Archives or will --

MR. WEINSTEIN: They would be transferred from the Archives in College Park, Maryland, eventually to the Archives in -- at the Nixon building.

MR. MCLAUGHLIN: They'll get the originals at the museum -- not the museum, but the Nixon library?

MR. WEINSTEIN: That's right. All of them.

MR. MCLAUGHLIN: But these are really also museums, are they not?

MR. WEINSTEIN: Of course they are. They really have a -- in addition to that, John, we have 14 regional archives and 17 regional record centers. Plus, we also publish the Federal Register, which most people don't know. So that the actions -- the regulatory actions of the federal government all come through the Archives. We publish the public papers of the president, and there's so much else.

MR. MCLAUGHLIN: How do you determine what is essential to keep, and what is trivial?

MR. WEINSTEIN: We have criteria for that. It's a process of evaluation. It's not -- we don't go into a fishbowl and pick a number out. We basically have ways of evaluating, document by document. But that's a lot of documents, and we need more people evaluating them. People are always, for example, concerned about declassification, but declassification takes time, and it takes experienced people analyzing this. And the **National Archives** can certainly use more of them.

MR. MCLAUGHLIN: Does it thrill you when you see American citizens looking at these documents almost -- and treating them almost -- and I guess in fact -- as sacred? Does it thrill you?

MR. WEINSTEIN: It thrills me every day, John, going to work and being at work, and I hardly want to leave. And I'll tell you one other thing I can't do -- which is the only frustration I have on this wonderful job; this is the best job in the world that I could have -- but I wish the **National Archives** could swear-in new citizens because it's such a wonderful place to swear-in people, to show them what America is, has been and will continue to be.

MR. MCLAUGHLIN: Are you going to do more to make visuals, like videotape of your archive operations and the presidential libraries, available to the press and to the citizenry?

MR. WEINSTEIN: The short answer, yes. But let me explain --

MR. MCLAUGHLIN: DVDs, for example --

MR. WEINSTEIN: Let me explain. We're doing that already, and I'll send you over some of the new materials we have. We have a wonderful partner, John, a public-private partnership called the Foundation for the **National Archives**. And if you -- when you come to the Archives you'll discover not only this beautiful rotunda with the three Charters of Freedom, you'll discover an extraordinary exhibit on American history called the Public Vaults exhibit, which is the best exhibit of this kind, as far as I'm concerned, in the world. And we have at least -- we have evidence that people have -- are discovering it because they're coming in droves. The lines outside the Archives every day are extraordinary.

MR. MCLAUGHLIN: You get researchers, you get students, you get historians, you get journalists, you get ordinary citizens -- some of them only want to engage in genealogical research, which is also somewhat available, is it not?

MR. WEINSTEIN: Well, the genealogists are my great friends. This is the largest single contingent of folks using the **National Archives** in research are the genealogists.

MR. MCLAUGHLIN: Really?

MR. WEINSTEIN: And they're wonderful people. They come from many different aspects, but yes, yes they are.

MR. MCLAUGHLIN: Do you have interactive exhibits?

MR. WEINSTEIN: We have -- the entire Public Vaults exhibit is interactive. And the foundation is now engaged in doing exactly what you're doing; doing videos, working on developing a learning center, getting all this material on the Web so that we can move it out of Washington into the entire world.

MR. MCLAUGHLIN: What about your exhibit that shows the manipulation and the duplicity of spying? I think it's called "black propaganda." Are you familiar with that?

MR. WEINSTEIN: We have several exhibits on espionage.

MR. MCLAUGHLIN: What --

MR. WEINSTEIN: Which I had nothing to do with, by the way. They were there before I got to the Archives.

MR. MCLAUGHLIN: Well, you don't disapprove of them?

MR. WEINSTEIN: Of course not.

MR. MCLAUGHLIN: Can you describe what happens at any one of them?

MR. WEINSTEIN: Well, we have a wonderful interactive exhibit in which people can basically take control of the exhibit by their hands and move it along from dramatic episode to dramatic episode -- the Nuremberg trials, the Rosenberg case, the various other things -- and actually read the documents as they go along, one by one. Watergate, for example, is one of those --

MR. MCLAUGHLIN: Well, what about Tibet. Do you remember Tibet?

MR. WEINSTEIN: I've heard of it, yes.

MR. MCLAUGHLIN: Here's what I show here. In the late '50s and '60s the U.S. had a covert program to support the Tibetans in their struggle against the Mao Chinese Communists. Part of the program involved what the CIA called "black propaganda" to distribute reports of Chinese atrocities to the U.N. and other international bodies. Many of these claims are phony, but they persisted as truth among the proponents of a free Tibet, down to the present day. So it shows our black propaganda techniques used by the United States government.

Do you get away with that?

MR. WEINSTEIN: John, I'll look into that, all right? Because basically, that's not an Archives question. You really want to be talking to the director of the CIA or the FBI or the State Department or somebody like that.

MR. MCLAUGHLIN: All right. You can point that person at this: That history is a hoot. Seeing isn't always believing. The use of trickery and deception and espionage. That's presentation.

MR. WEINSTEIN: Wonderful entertainment that's part of our Fourth of July.

MR. MCLAUGHLIN: But it's based on fiction, or is it based on fact?

MR. WEINSTEIN: I haven't looked at it. I've never seen it, but I will look at it.

MR. MCLAUGHLIN: Okay.

MR. WEINSTEIN: I'll let you know.

But do come to the Fourth. I mean, the best way to find out is by experiencing it personally.

MR. MCLAUGHLIN: You've got 2,800 employees, is that right?

MR. WEINSTEIN: Well, supposedly.

MR. MCLAUGHLIN: Three hundred and ten million (dollars) in your 2005 budget, and you want 313 (million dollars) in your 2006 budget -- a 1.2 percent increase.

MR. WEINSTEIN: Right. And I'm not going to tell you what we're asking for in 2007.

MR. MCLAUGHLIN: What are you going to spend that -- what are you going to bring in? You've got this huge digital challenge now.

MR. WEINSTEIN: Well, that's a good part of the budget. That's a good part of the budget.

MR. MCLAUGHLIN: E-mails -- are you going to be storing e-mails?

MR. WEINSTEIN: It's estimated that the e-mails in the Bush administration will be three times the number of e-mails in the Clinton administration, and it's just growing exponentially.

We are talking about billions and billions of electronic records, so.

MR. MCLAUGHLIN: Do you think there's -- some people in the administration hearing this program will have a nervous breakdown when they realize that their e-mails are going to be forever embalmed in your -- excuse the word -- but in a repository at your facility?

MR. WEINSTEIN: "Preserved" is the word we would use there.

MR. MCLAUGHLIN: (Chuckles.) You think they'll have a nervous breakdown?

MR. WEINSTEIN: I doubt it very much, John.

MR. MCLAUGHLIN: We'll be right back.

(Announcements.)

MR. MCLAUGHLIN: Dr. Weinstein, a couple of months ago you gave testimony, and you said e-commerce has inflated the risk that documents or images will be stolen for monetary gain. Are you blaming eBay --

MR. WEINSTEIN: No.

MR. MCLAUGHLIN: -- for peddling those documents?

MR. WEINSTEIN: No. In fact, they've been very cooperative with us when we point out to them that certain documents that have been offered for sale are documents that we think are part of our collections. And they've been very cooperative with us on every occasion. Not only eBay, but most of the -- most of the community of document sellers; legitimate document sellers -- are very cooperative.

Well, we have a problem, John. We've, in fact, just -- you may have read in the paper just a few weeks ago, one of the individuals who did steal from us, who was identified by, in fact, a private citizen who just happened to notice the fact that documents that he'd used in the archives were being offered for sale. We arrested -- this man was arrested, convicted, and sentenced to two years in jail. It's a serious offense. Two years in a --

MR. MCLAUGHLIN: Over how long a period had he been stealing.

MR. WEINSTEIN: He'd been stealing for several years.

MR. MCLAUGHLIN: Several? Seven?

MR. WEINSTEIN: Several. Several years. We don't -- we're not entirely certain how long.

MR. MCLAUGHLIN: At least five?

MR. WEINSTEIN: Well, several years. I'll keep to that.

MR. MCLAUGHLIN: There are some dates out there. There are some years.

MR. WEINSTEIN: There's some dates out there. There's some dates in there. For at least five, probably.

MR. MCLAUGHLIN: He was not an insider.

MR. WEINSTEIN: Well, he was a continuous researcher, and basically --

MR. MCLAUGHLIN: You mean, a daily hire?

MR. WEINSTEIN: No, he was an outside researcher, but he was working at the -- he would come into the archives to do research. We have strengthened our procedures since that case and since a few others like that a few years ago. We have strengthened our procedures, and we continue to do that every day, John. We're incredibly serious -- the penalty itself, the fact that we -- we invited in the gentleman who identified the theft and we had a ceremony in his honor. And we are urging citizens -- when, if you think something is stolen, please inform us and we will check it out.

MR. MCLAUGHLIN: How much money did he make?

MR. WEINSTEIN: Unclear, but at least probably \$30-\$40,000; maybe more.

MR. MCLAUGHLIN: I see 47.

MR. WEINSTEIN: Well --

MR. MCLAUGHLIN: I -- (trust ?) the estimate?

MR. WEINSTEIN: Press estimate.

MR. MCLAUGHLIN: What is eBay doing to help you with this problem?

MR. WEINSTEIN: I think you should ask the eBay people. I think they're probably reviewing people who offer documents for sale a little bit more carefully than they may once have done. But I don't want to say anything about that, because I basically -- I don't have the -- every detail on that.

MR. MCLAUGHLIN: You've got a general counsel, of course.

MR. WEINSTEIN: We have a terrific general counsel. We have a terrific staff. One of the things I should mention to you before we -- we have, as far as I'm concerned, the best

bureaucracy in government. There are people at the archives who've worked 30, 35, 40 years with the same vigor and energy and passion for their work --

MR. MCLAUGHLIN: You know, that doesn't surprise me, because -- you take librarians. Librarians love their work. They love it. And I think there's -- there's some analogous -- well, I guess there are quasi-librarians there. And I can see how people would love that kind of work, because if you love -- if you like it, you really love it.

MR. WEINSTEIN: John, we had our 20th anniversary recently as an independent agency, 20 years. The irony is, when I was on The Washington Post editorial board for a year, I wrote an editorial urging the independence of the Archives. But the 20th anniversary came, and I said let's honor those who have worked here 20 years. And my senior colleagues in the Archives laughed and chuckled and said that would be -- we have to honor a quarter of the agency, because people have worked there as much as 40 years or more, with the same dedication that they'd begun employment.

MR. MCLAUGHLIN: Are you saying that you're getting full cooperation from eBay, by the way?

MR. WEINSTEIN: I'm hoping for full cooperation from eBay.

MR. MCLAUGHLIN: Are you prepared to bring a legal case against them, either civil or criminal?

MR. WEINSTEIN: John, we've known each other a long time. You know I'm not going to talk about things like that anyway.

MR. MCLAUGHLIN: (Chuckles.) But your counsel stands ready.

MR. WEINSTEIN: We're serious people.

MR. MCLAUGHLIN: Your counsel stands ready.

MR. WEINSTEIN: We're deadly serious about -- we're --

MR. MCLAUGHLIN: About security.

MR. WEINSTEIN: -- about security, deadly serious. It's one of my priorities --

MR. MCLAUGHLIN: Okay. In that connection, we'll talk about a couple of high-profile cases. You've got of course the Sandy Berger -- Clinton national security adviser who removed five copies of documents from the Archives. In each case, the Archives retained the official presidential record copy of each document. First of all, why the big deal over his taking out a copy of a document, like a Xerox copy? Was that it?

MR. WEINSTEIN: John, the Berger case is still being -- is still in the courts. He hasn't been sentenced yet. He's pled guilty to the allegations. He hasn't been sentenced yet. I can't talk about the Berger case. You know that.

MR. MCLAUGHLIN: Okay. I'll accept that.

What measures are under review to prevent theft?

MR. WEINSTEIN: Well, we have better patrolling of the research rooms, and we have a greater number of guards. We have a whole series of procedures, which again I'm not going to talk about, because otherwise everybody would know what the procedures were. But we are in much better shape in order to monitor this problem, and not just -- mind you, it's not just at the downtown building. It's to monitor at 11 presidential libraries, at three other buildings in Washington, at 14 archival regional centers around the country and 17 record centers. We have this problem -- we could have this problem in a number of places. We're trying to avoid it in every place. We're trying to make security a major --

MR. MCLAUGHLIN: How long have you been at the Archives?

MR. WEINSTEIN: Four and a half happy months.

MR. MCLAUGHLIN: Four and a half happy months. When you went there, did you sense there was laxity with regard to security?

MR. WEINSTEIN: No. No.

MR. MCLAUGHLIN: You did not?

MR. WEINSTEIN: No. I sensed that there was very deep concern about this, and I prayed -- the reason -- just the one point I'll make about the Berger case is that it was the Archives employees who identified the fact that something was happening. It was people from the Archives who basically first said -- stepped forward and said, "We think that there's a problem here." I'm not going to go into the details.

The Archives employees do not -- look, we -- these are national treasures, our documents, all of them. And we do not intend to have any of them mishandled, lost, stolen, if possible, or in other -- dealt with badly in other ways.

MR. MCLAUGHLIN: You also preside over presidential libraries. How many are there?

MR. WEINSTEIN: Well, there are 11 now, and there will be 12 when the Nixon library joins the system.

MR. MCLAUGHLIN: It's a pleasure having you with us. You must come back.

MR. WEINSTEIN: I will.

MR. MCLAUGHLIN: And keep up the great work.

MR. WEINSTEIN: Thank you for having me, John.

MR. MCLAUGHLIN: Thank you.

MR. WEINSTEIN: Come visit.

MR. MCLAUGHLIN: We will.

MR. WEINSTEIN: Okay.

PBS SEGMENT

MR. MCLAUGHLIN: There are 11 presidential libraries.

MR. WEINSTEIN: At present, yes.

MR. MCLAUGHLIN: And that means that the presidents who were -- who preceded --

MR. WEINSTEIN: Right.

MR. MCLAUGHLIN: -- the immediate last 11 presidents have no presidential library.

MR. WEINSTEIN: Well, there are 11 presidential libraries in the federal presidential library system paid for by -- funded by the federal government, in cooperation with foundations at each library. For preceding presidents -- this whole system began under Franklin Roosevelt, although Herbert Hoover has a library as well. For preceding presidents, there are different adjustments. For example, there's a beautiful Lincoln library, which just opened a few months ago or weeks ago.

MR. MCLAUGHLIN: That's privately managed --

MR. WEINSTEIN: Well, privately managed --

MR. MCLAUGHLIN: -- and funded.

MR. WEINSTEIN: -- funded by the state -- and by private money. And there are 100 libraries for 19th century presidents, but they're funded privately by various commissions and states.

MR. MCLAUGHLIN: Would you like to see the **National Archives** gradually take over those other presidential libraries, and where necessary, create ones that all of our

presidents can be so memorialized?

MR. WEINSTEIN: What was that wonderful phrase from the film? Show me the money, John. I mean, it takes a lot of money to run these places, and we struggle every year to find the money to deal with what we're dealing with right now.

MR. MCLAUGHLIN: Well, can you imagine how much the appeal would be, if there were a George Washington Presidential Library?

MR. WEINSTEIN: Well, there are Washington collections all over. You're asking whether I wanted to build a presidential library empire; the answer is no.

MR. MCLAUGHLIN: But you've negotiated with the --

MR. WEINSTEIN: What we're doing, John, is we're bringing the various presidential library directors and foundations together for more cooperation, because basically they will -- they'll all benefit by working together in a variety of --

MR. MCLAUGHLIN: Do you know Michael Beschloff?

MR. WEINSTEIN: He's a good friend.

MR. MCLAUGHLIN: Good friend. He's on your board.

MR. WEINSTEIN: He's one of the --

MR. MCLAUGHLIN: He's a historian.

MR. WEINSTEIN: He's a member of the Foundation for the **National Archives**.

MR. MCLAUGHLIN: Okay. When he was --

MR. WEINSTEIN: Which is, by the way --

MR. MCLAUGHLIN: When he visited the LBJ library, he found a couple of precious jewels, so to speak. I mean, literary jewels that he used, with Johnson musing about how the war in Vietnam was unwinnable.

MR. WEINSTEIN: That's correct.

MR. MCLAUGHLIN: Do you think you're going to find anything like that in the Nixon papers?

MR. WEINSTEIN: Well, the Nixon papers are being processed right now as we talk at the **National Archives** in College Park, Maryland, the papers and tapes; they have been

for years and years.

MR. MCLAUGHLIN: Or has that -- has that vein been mined thoroughly?

MR. WEINSTEIN: Well, apparently the news media has a something on him there periodically. There was one a few days ago that you may have seen --

MR. MCLAUGHLIN: I'm not thinking about bad stuff, I'm thinking about good stuff.

MR. WEINSTEIN: Well --

MR. MCLAUGHLIN: I mean, he did introduce China into a relationship with us.

MR. WEINSTEIN: Of course.

MR. MCLAUGHLIN: And that could, of course, redound to his credit, could it not?

MR. WEINSTEIN: I'm not thinking bad stuff either. I'm thinking -- I think once you have the Nixon library in the presidential system, the focus can become more balanced, and people can look at the entire presidency. Not just the end of the presidency, but the entire presidency. Michael has done that with Johnson as well. But let me just mention the Foundation for the **National Archives**, which is a 501(c)(3). Michael is a member of the board of directors.

MR. MCLAUGHLIN: Now, you mentioned that before.

MR. WEINSTEIN: They --

MR. MCLAUGHLIN: I mean, you're really hitting that drum, aren't you?

MR. WEINSTEIN: They help pay for that wonderful exhibit on American history. Education's our game, John. We're trying to --

MR. MCLAUGHLIN: Do you think this a money-raising program, Allen?

MR. WEINSTEIN: No, I don't, John.

MR. MCLAUGHLIN: Al, we've been off the air for about a minute.

MR. WEINSTEIN: I figured you had.

MR. MCLAUGHLIN: (Laughing.)

MR. WEINSTEIN: We had a run.



Statement by the 9-11 Commission

April 7, 2004 — A team of Commission staff has completed its review of 10,800 pages of Clinton administration White House documents. We estimate that more than 90 percent of the material had already been produced, was irrelevant to our work, or was duplicative.

Out of the total, Commission staff identified 12 documents that we consider clearly or arguably responsive to our requests but had not yet been produced. The White House has now produced these documents to the Commission. The review team concludes that any errors in document production were inadvertent.

The Commission staff also identified 57 additional documents, not previously requested by the Commission from the White House, that nonetheless are relevant to our work. The Commission has asked for production of these documents. We are making a parallel request for Bush administration documents.

The process has been constructive.

Sharon Fawcett - AP Wire: Former Clinton attorney questions Bush policy on archive

From: Skip Rutherford <Skip.Rutherford@cjr.com>
 To: (b) (6) (b) (6)@nara.gov
 Date: 3/31/2004 11:09 PM
 Subject: AP Wire: Former Clinton attorney questions Bush policy on archive

Fyi.

AR--Clinton-Commission, Ark Bjt,530
 Former Clinton attorney questions Bush policy on archive records

Former Clinton attorney questions Bush policy on archive records
 mnphfonfls
 By MELISSA NELSON
 Associated Press Writer
 LITTLE ROCK (AP) _ A commission investigating the Sept. 11 attacks isn't getting a full picture of Bill Clinton's terrorism policies because of a Bush administration decision not to forward all of Clinton's records to the commission, Clinton's former deputy White House counsel said Wednesday.

Bruce Lindsey, Clinton's legal representative for records and a longtime confidant of the former president, said he has determined that only about 25 percent of nearly 11,000 pages from Clinton's presidential archives in Little Rock and from secure storage in the Washington area have been forwarded to the commission.

Lindsey said he feared the commission's conclusion could be compromised by the lack of information.

"I don't want (the commission) drawing the conclusion the Clinton administration didn't do X or Y and then there be a document that contradicts that and they didn't have access to that document because the current administration decided not to forward it to them," Lindsey told The Associated Press.

"If we go back later and say 'we did do X,' we're playing catch up, even if they were drawing conclusions based on a partial record," he said.

Under federal statutes, presidential records are sealed for five years after a president leaves office. The records can only be accessed by the current White House, Congress or through a court order.

Lindsey said the Bush administration did not consider the commission an arm of Congress for requesting records and instead made the request itself. After the administration received the thousands of pages from the Clinton archive, the National Security Council and administration attorneys decided which records were relevant to the commission's request, Lindsey said.

"What we have found is that the administration has interpreted the commission's request differently from the archives and, putting in the best light, has found that three-fourths of the pages did not comply with the commission's request. That's a fairly big difference of opinion," he said.

Lindsey also questioned the administration's decision to not consider the commission an arm of Congress for the purpose of requesting documents. He said the administration did consider the commission an arm of Congress when it argued that National Security Adviser Condoleezza Rice shouldn't testify publicly under oath before the commission because of an infringement on the division of powers between Congress and the White House.

In a reversal, the White House agreed Tuesday to allow Rice to testify publicly and under oath before the 10-member panel as early as next week.

Commission members are expected to question Rice about the transition between administrations _ something Lindsey believes the commission needs all of the Clinton records to fully understand.

"Commissioners could think they have gotten all of the documents on Osama bin-Laden and al-Qaida when three-fourths of the documents have been filtered out," he said.

AP-CS-03-31-04 1804EST



Copyright 2004 The New York Sun, One SL, LLC
All Rights Reserved
The New York Sun

December 8, 2004 Wednesday

SECTION: NATIONAL; Pg. 7

LENGTH: 1353 words

HEADLINE: Berger Investigation Stretches Into Second Year

BYLINE: By JOSH GERSTEIN, Staff Reporter of the Sun

BODY:

More than a year after President Clinton's top national security adviser, Samuel Berger, walked out of the **National Archives** with top-secret documents, a criminal investigation into the matter remains open with no sign of any imminent action.

Legal and national security experts say the delay may be an indication of how Mr. Berger's case has put the Justice Department in a tough political pickle. If prosecutors hit the former official with a criminal charge, Democrats will complain of a political vendetta. If Mr. Berger is let off with an administrative punishment, such as revocation of his security clearance, hard-liners will squawk about a double standard that overlooks classified information breaches committed by high-ranking officials.

"It's a complicated calculation," said a policy analyst at the Federation of American Scientists and a leading authority on classification issues, Steven Aftergood. "Everyone involved, I'm sure, is very uncomfortable with it."

In September and October 2003, Mr. Berger visited a secure room at the **National Archives** to review highly classified documents as he, Mr. Clinton, and other former officials prepared to give testimony to the commission investigating the September 11, 2001, terrorist attacks. During one of Mr. Berger's first visits, workers at the archives became suspicious that he might be removing some documents from the facility, people familiar with the inquiry said. When Mr. Berger returned, the clerks marked the papers so that any missing pages could be detected more easily. When they checked the documents later, some were, in fact, missing. After getting a call from senior officials at the archives, Mr. Berger returned some records but could not locate them all.

Among the documents reported missing were drafts of a Clinton administration after-action review on the handling of the so-called millennium plot to blow up American landmarks. The report, prepared by counterterrorism chief Richard Clarke, described the unraveling of the plot as a matter of luck rather than insightful planning.

In January, FBI investigators trying to locate the missing records carried out search warrants at the

offices of Mr. Berger's consulting firm and at his home, both in Washington.

The probe remained largely secret until July, when word about it was leaked to news outlets. In a statement prompted by the leak, Mr. Berger said he never intended to remove any classified documents from the archives. "In the course of reviewing over several days thousands of pages of documents... I inadvertently took a few documents from the archives," Mr. Berger said. He also acknowledged taking home his notes about the classified records, another violation of rules for handling such materials.

Mr. Berger's attorney, Lanny Breuer, angrily denied reports that the ex-official stuffed some documents into his socks.

As a result of the reports, Mr. Berger stepped down from his role as an adviser to the presidential campaign of Senator Kerry. Many Democrats complained bitterly that the leak was intended to produce just that result.

In a brief interview last week, Mr. Berger said he had no indication of when the probe might be completed. "Still no resolution," he said.

Mr. Breuer also said he's gotten no update from the government. "There's really nothing to report," he said in an interview Monday. "Things are status quo. We'll see what happens."

A spokesman for the Justice Department, Mark Corrallo, said he had no comment on the investigation.

Several legal experts said a key standard that prosecutors must consider is the handling of a similar case involving a former director of central intelligence under Mr. Clinton, John Deutch.

"That is the benchmark," said a former federal prosecutor, Joseph diGenova.

During the early and mid 1990s, Mr. Deutch repeatedly typed up and copied highly classified documents on his home computer, which was often connected to the Internet. After his practice was discovered when he left the agency in 1996, Mr. Deutch was investigated by the Justice Department, which initially declined to prosecute. However, the then attorney general, Janet Reno, re-opened the case after an outcry from some in the CIA and in Congress.

Mr. Deutch eventually agreed to plead guilty to a misdemeanor offense of mishandling classified data and to pay a \$5,000 fine. However, the plea was never formally entered because Mr. Clinton, during his final hours in office, granted a pardon to Mr. Deutch.

Mr. diGenova, a Republican who once served as an independent counsel, said the government will have to cancel Mr. Berger's security clearance, if it has not already done so. However, he said that alone will not be sufficient to meet the standard the Justice Department applied to Mr. Deutch.

"It is, to me, not a complicated matter," the former prosecutor said. "The facts as publicly known make it very difficult for the department not to charge him with some offense. It doesn't have to be a felony."

Mr. diGenova said he is dubious of the explanation Mr. Berger has offered thus far. "I don't care how much of a bumbler he was. There's more to this story. I want to know what it is," the former prosecutor said.

He added that undue leniency towards Mr. Berger "will not sit well with troops who get suspended from duty and pay suspensions for mishandling classified documents."

Mr. Breuer declined to discuss whether he considers Mr. Berger's situation similar to that involving Mr. Deutch.

Mr. Aftergood, the classification expert, said the probe has already had a serious impact on Mr. Berger's reputation and his livelihood as an international business consultant.

"Arguably, Berger has already been severely punished by being publicly humiliated and by having his participation in the Kerry campaign derailed," Mr. Aftergood said. "It could well be argued that justice has been served already and that no further expenditure of government resources is warranted."

"In both cases, the New York Times obit for them is going to mention these instances, and that's a hard thing to get past," Mr. Aftergood said. "What means more to these people than their reputation?"

An attorney who was a Justice Department official under President Reagan, Bruce Fein, said he believes that any criminal action against Mr. Berger would step up calls for prosecution over the alleged leak of the identity of CIA operative Valerie Plame to a conservative columnist, Robert Novak. Many suspect that leak came from the White House.

"The problem the administration confronts is that the display of a rather lackadaisical attitude towards the Bob Novak fiasco and Bush saying, 'Oh, well ... we may never solve this one,' then to go after Sandy Berger in a situation whether you can't show that there was in fact harm," Mr. Fein said. He said a prosecution of Mr. Berger would leave those investigating the leak to Mr. Novak in "an impossible political position."

Another potential concern for the administration is that it has often taken a tough line against low-level personnel accused of mishandling classified materials.

A former translator at Guantanamo Bay, Ahmed Mehalba, has been in pretrial detention in Massachusetts for more than a year as he awaits trial on one felony count of mishandling classified information and two counts of lying to law enforcement officials. He was accused of having information classified as "secret" on computer disks that were in his luggage as he went through customs at Boston's Logan Airport last September.

The documents Mr. Berger removed were reportedly classified as "code word," a special classification level that exceeds "top secret."

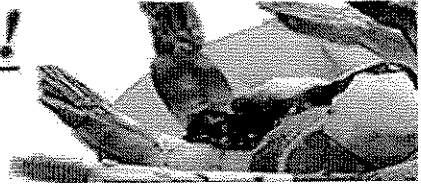
The general counsel to the September 11 commission, Daniel Marcus, said yesterday that archives staff members were able to locate additional copies of the documents Mr. Berger lost. "We had been assured by the Justice Department that the archives still had copies of everything," Mr. Marcus said yesterday.

Mr. Marcus denounced as "shocking" the original leak about the investigation. He said he wishes the Justice Department would now wrap it up. "It's just too bad it's dragged on so long," he said.

LOAD-DATE: December 8, 2004

Dinner at Red Lobster on us!

Hungry? Answer a few questions...
...get a \$50 Restaurant Card



Support The DrudgeReport; Visit Our Advertisers

MCAULIFFE FILES FREEDOM OF INFORMATION ACT REQUEST; Requests All Documents Shared Between Dept. of Justice and White House Regarding Investigation of Sandy Berger...



CLINTON DEFENDS BERGER: 'WE WERE ALL LAUGHING ABOUT IT'

DRUDGE REPORT

Nuclear arms reportedly found in Iraq...

'Concealed in a concrete trench'...

Iraq Interior Ministry Says Report 'Stupid'...

Iraq Militant Group Takes 6 New Hostages...

Saudis find slain US hostage's head in a refrigerator...

Sept. 11 Panel Lists Missed Opportunities

Celebrities' Anti-Bush Rhetoric Is Alienating Voters...

Berger: Incident Was 'Honest Mistake'...

POLL: Have you ever mistakenly shoved top secret documents down your pants and taken them out of the National Archives?

Dems worry big media threaten democracy...

China frees SARS doctor after 're-education'...

cle in the Journal last year.

Mr. Alamoudi, founder of two Muslim civil-rights groups, was arrested by FBI agents in 2001. He is being held at the Federal Detention Center in New York City. He is being held in connection with the investigation of the Sept. 11, 2001 terror attacks.

Berger Cleared of Withholding Material From 9/11 Commission

By SCOT J. PALTROW

Officials looking into the removal of classified documents from the National Archives by former Clinton National Security Adviser Samuel Berger say no original materials are missing and nothing Mr. Berger reviewed was withheld from the commission investigating the Sept. 11, 2001 terror attacks.

Several prominent Republicans, including House Speaker Dennis Hastert and House Majority Leader Tom DeLay, have voiced suspicion that when Mr. Berger was preparing materials for the 9/11 Commission on the Clinton administration's antiterror actions, he may have removed documents that were potentially damaging to the former president's record.

The conclusion by archives officials and others would seem to lay to rest the issue of whether any information was permanently destroyed or withheld from the commission.

Archives spokeswoman Susan Cooper said officials there "are confident that

there aren't any original documents missing in relation to this case." She said in most cases, Mr. Berger was given photocopies to review, and that in any event officials have accounted for all originals to which he had access.

That included all drafts of a so-called after-action report prepared by the White House and federal agencies in 2000 after the investigation into a foiled bombing plot aimed at the Millennium celebrations. That report and earlier drafts are at the center of allegations that Mr. Berger might have permanently removed some records from the archives. Some of the allegations have related to the possibility that drafts with handwritten notes on them may have disappeared, but Ms. Cooper said archives staff are confident those documents aren't missing either.

Daniel Marcus, general counsel of the 9/11 Commission, said the panel had been assured twice by the Justice Department that no originals were missing and that all of the material Mr. Berger had access to had been turned over to the commission. "We are told that the Justice Department is satisfied that we've seen everything that the archives saw," and "nothing was missing," he said.

Mr. Berger's lawyer has said his client returned all of the photocopies after he was questioned about missing items by archives staff. But officials have said they are still looking into whether some of the photocopies may have been destroyed. It is illegal to remove classified material in any form from the archives.

Late last year, archives personnel called in investigators when some classified materials were discovered missing after Mr. Berger reviewed them in response to a 9/11 Commission request for Clinton-era national-security records. Staff members became suspicious that Mr. Berger had removed items during a first visit, and on a second visit secretly numbered copies given to him and determined afterward that not all had been returned. By some accounts, Mr. Berger had been observed by the staff stuffing papers into his clothing, although Mr. Berger's lawyer, Lanny Breuer, has denied that.

So far no charges have been filed. Mr. Breuer has said that on two occasions his client had inadvertently removed several photocopies of the Millennium after-action report, but later returned them.

ceived call for more allied involvement. Iraq, in particular, doesn't offer over how he would persuade reluctant allies like France and Germany, who posed the war in the first place, to their troops in harm's way.

Still, last night he also used what came one of his biggest applause lines in recent weeks: "The United States of America never goes to war because we only go to war because we have to."

In the "values" debate, Mr. Kerry tried to shed the impression that his fellow party members—at least outside the South—are uncomfortable with religion. "We welcome people of all faiths," he said. "I don't wear my religion on my sleeve," he added—a dig at Bush's more-overt religious talk. "Faith has given me values and life by ... from Sunday to Sunday."

Mr. Kerry didn't match Mr. Bush's core Republican issues, such as abortion and gay marriage, but he tried to change the terms of the debate. He used the word "values" to appeal to sell more traditional Democratic positions on economic issues.

"We value jobs that actually create more than the job that you lost,"

Mr. Kerry seemed so eager to get time in the spotlight to embrace themes—and woo the swing voters that Bush has won—that his speechways paralleled that delivered by four years ago. "To all those who support our armed forces today, I say, 'Thank you for the way you've served the country,'" Mr. Kerry said—repeating a phrase Mr. Bush and Vice President Dick Cheney used in 2000 to honor armed forces they said had been funded by President Clinton.

Mr. Kerry vowed to "restore trust and credibility to the White House," echoing Mr. Bush's promise to "restore honor and integrity" to the Office after the Clinton scandals.

Throwing back at Mr. Bush the Republican's famous pledge to be a "uniter, not a divider," Mr. Kerry called the president directly to run for re-election. "Let's build unity in the American family, not anger," he said. That was just one of the ways Mr. Kerry mentioned his own name in the speech.

Also under the appeal to "value an America where the middle class is not being squeezed," he said he would use his speech to give the commission a detailed description of the economic situation he has laid out over the past few weeks of his campaign. He called for closing "tax loopholes" that he said encourage outsourcing jobs overseas. He called for tougher enforcement of trade agreements and talked about raising taxes on the wealthy, including more than \$200,000—for middle class families. He called for cutting the budget deficit in half in part by "ending tax giveaways to corporations and wealthy individuals" and "imposing limits on government spending." He called for making health care more available and less expensive. He called for a program to become "energy independent" of Middle East oil.

Call 800-WSJ-2206 ext. 174

Early A.M. Delivery At 50% Off

Talking Points for Oversight Committee meeting 7/27/04

- Truman, Johnson, Reagan, and Clinton have cameras. Requests are in our 2006 security initiative. Cameras are about \$1500 each and we average 2 per research room. Additional monitoring equipment is needed for the security control centers in some libraries. \$150,000 estimate to install cameras and monitoring equipment in remaining libraries.
- Recognize distinction between protection of original records and the protection of information in the records.
- Under the law, the former president and/or his designated representative have access to the records anytime, anywhere. As a matter of policy we do not send our originals out of our buildings. The procedures we used were drawn from the statutory requirements in 44 U.S.C § 2205(2) and E.O. 13233 which allows for review of presidential records for privilege concerns and states the records SHALL be available. This is also stated in our coded regulations without reservation. The limits we have placed on access, requiring designations in writing and not sending originals out of the facility, have been accepted but have caused considerable frustration by the reps when such limitations impeded timely access, i.e. the time required to make and send copies.
- Access to classified information requires necessary clearances and completion of an SF 312, Classified Information Nondisclosure Agreement. *at the agency sponsoring*
- If Sandy Berger ^{*or any other deny. rep*} had had a cleared venue in which to store the documents ^{*the clearance*} we could have provided copies of any or all of the documents he wished to review. *only occasionally happened*
- Not a research room venue or situation. NARA monitors were not required to be in the room. When NARA personnel were present it was a matter of assistance. Why should they take what they have a right to have? The situation is completely analogous to the access provided Congress to their materials housed in Archives I. *o*
- How could the monitor be ordered out of the room? We were dealing with the personal representative of the president and since the access was statutory we had no authority to deny the request. Given the subsequent events, we would not now leave a representative examining classified material alone nor permit the use of a cell phone. *used reg. phone* *not dedicated coverage*
- Given that, we have certainly reexamined these premises and set out new procedures for classified access so that we can be better assured the information is protected.
- Classified research room at A1 opened by February. That research room is constantly monitored and operates as a "clean" research room.

*Dedicated coverage →
monitoring →
assistance*

§ 1270.44

§ 1270.44 Exceptions to restricted access.

(a) Notwithstanding any restrictions on access imposed pursuant to section 2204 or these regulations, and subject to any rights, defenses, or privileges which the United States or any agency or person may invoke, Presidential records shall be made available in the following instances:

(1) Pursuant to subpoena or other judicial process properly issued by a court of competent jurisdiction for the purposes of any civil or criminal investigation or proceeding;

(2) To an incumbent President if the records sought contain information which is needed for the conduct of current business of his office and is not otherwise available;

(3) To either House of Congress, or, to the extent of matter within its jurisdiction, to a Congressional committee or subcommittee if the records sought contain information which is needed for the conduct of business within its jurisdiction and is not otherwise available.

(b) Requests by an incumbent President, a House of Congress, or a Congressional committee or subcommittee pursuant to paragraph (a) of this section shall be addressed to the Archivist. All requests shall be in writing and, where practicable, identify the records sought with reasonable specificity.

(c) Presidential records of a former President shall be available to the former President or his designated representative upon request.

§ 1270.46 Notice of intent to disclose Presidential records.

(a) The Archivist or his designee shall notify a former President or his designated representative(s) before any Presidential records of his Administration are disclosed.

(b)(1) The notice given by the Archivist or his designee shall:

- (i) Be in writing;
(ii) Identify the particular records with reasonable specificity;
(iii) State the reason for the disclosure; and
(iv) Specify the date on which the record will be disclosed.

36 CFR Ch. XII (7-1-02 Edition)

(2) In the case of records to be disclosed in accordance with § 1270.44, the notice shall also:

(i) Identify the requester and the nature of the request;

(ii) Specify whether the requested records contain materials to which access would otherwise be restricted pursuant to 44 U.S.C. 2204(a) and identify the category of restriction within which the record to be disclosed falls; and

(iii) Specify the date of the request.

(c) If, after receiving the notice required by paragraph (a) of this section, a former President raises rights or privileges which he believes should preclude the disclosure of a Presidential record, and the Archivist nevertheless determines that the record in question should be disclosed, in whole or in part, the Archivist shall notify the former President or his representative of this determination. The notice given by the Archivist or his designee shall:

- (1) Be in writing;
(2) State the basis upon which the determination to disclose the record is made; and

(3) Specify the date on which the record will be disclosed.

(d) The Archivist shall not disclose any records covered by any notice required by paragraph (a) or (c) of this section for at least 30 calendar days from receipt of the notice by the former President, unless a shorter time period is required by a demand for Presidential records under § 1270.44.

(e) Copies of all notices provided to former Presidents under this section shall be provided at the same time to the incumbent President.

Subpart E—Presidential Records Compiled for Law Enforcement Purposes

§ 1270.50 Consultation with law enforcement agencies.

(a) For the processing of Presidential records compiled for law enforcement purposes that may be subject to 5 U.S.C. 552(b)(7), the Archivist shall request specific guidance from the appropriate Federal agency on the proper treatment of a record if there is no general guidance applicable, if the record is particularly sensitive, or if

National

the type
widespre:
(b) Wh:
requeste:
section,
appropri:
sion rega
documen
following
(1) A
question
(2) Sta
scribed

- As a professional archivist I interject this note of caution: all of our precautions do two things: they help protect from accidental or inadvertent compromises or removal of documents and they help to deter the opportunist thief. They do NOT however prevent someone who seriously intends to steal a document or compromise information even with constant monitoring. You can only see what you think you see. A professional thief with a slight of hand can pocket a document while you believe he has only replaced his handkerchief.

- Archives has no authority to do body searches -

Former President's Privilege Review of Classified Presidential Records in the Custody of the Archivist of the United States

As there was no single directive for this type of access, the procedures followed in allowing a former President and/or his designated legal representative to conduct a privilege review of classified records were drawn from the statutory authority of the Presidential Records Act, 44 U.S.C. §§ 2201-2207, and NARA's required operating framework governing the access to and handling of classified information.

Procedures

1) NARA receives a request under 44 U.S.C. § 2205(2) for access to records that are not otherwise available to the public. Presidential records shall be made available in response to one of the following: a subpoena or other judicial process issued by a court of competent jurisdiction, a request by the incumbent President for on-going government business, or a request from either House of Congress or from a committee or subcommittee if such records are needed for the conduct of Congressional business.

2) If NARA locates documents responsive to the special access request, NARA will provide a notification of that fact to the former President and/or his designated legal representative. The PRA and E.O. 13233 allows for the review of those records for privilege concerns. The former President must designate in writing to NARA any individual he wants to conduct such a privilege review on his behalf. Further, 44 U.S.C. § 2205(3) states that "the Presidential records of a former President shall be available to such former President or his designated representative."

3) The PRA and NARA's implementing regulations at 36 C.F.R. § 1270.44(c) are the only authorities governing a privilege review by the former President and/or his designated representative. However, if the responsive Presidential records contain classified information, any privilege review must occur in accordance with Executive Order 12958, as amended, and NARA's Information Security Manual 202. This manual has no specific procedures for granting a former President and/or his designated representative access to classified information for a privilege review. However, NARA followed those procedures that were most appropriate, specifically those that apply to access for research by former Presidential appointees, historical researchers and safekeeping and storage of classified information. These are outlined below.

NARA Information Security Manual 202

Chapter 2, Part 1 – Access

4. Former Presidential Appointees.

Access is permitted when:

- a. The person has a current security clearance at the appropriate level and completes an SF 312, Classified Information Nondisclosure Agreement.
- c. The person seeking access agrees to:
 - (1) Safeguard the information (Accomplished by the SF 312);

— if NARA sponsors and at point of 1st clearance as long as maintained

- (2) Authorized review of his or her notes to make sure that they do not contain classified information; and
- (3) Make sure that the classified information to which he or she received access is not further disseminated or published.

5. Historical Researchers and Contract Historians.

- b. Verification in writing of the accessing individual's security clearance.
 - (2) The written verification must be provided by an official, other than the visitor, who is in a position to verify the visitor's security clearances
- c. Verification (orally or in writing), that the contractor/researcher has completed and filed with the contracting or authorizing agency a classified information nondisclosure agreement.

Chapter 4, Part 1 – Safekeeping and Storage

7. Custodial Precautions

- b. Care during working hours. Each person must take precautions to prevent access to classified information by unauthorized persons. The following precautions are to be observed:
 - (4) When classified information is to be made available to research, properly cleared employees move the material to a research room, supervise its use, return it to storage, and make sure that unauthorized persons do not have access to it. Notes taken from classified information in records or documents by researchers are to be safeguarded the same as the classified documents.

From: (b) (6)
To: GaryM Stern; John Constance; Sharon Fawcett
Date: 7/22/04 5:31PM
Subject: 'Procedures for Special Access for Designated Representatives of Former President under the PRA

Gary, Sharon and John:

Attached are what we have worked up that is the process that we have followed in the past in handling special access situations for the representatives of the former President under the PRA doing a review for privilege of classified information. These procedures as we discussed this morning are specific to requests only dealing with classified information.

I think it is important to keep in mind that these procedures are for a privilege review of classified information by the designated representative of a former President under the PRA when that representative comes to NARA. This is a different situation from a researcher coming in to do classified research. Additionally, there is nothing that would prohibit copies of classified information being sent to a designated representative or a former President for their review, if they have a classified storage facility. Since these are extremely complex situations, I am comfortable that if you use this attachment for talking points the situations will be characterize correctly. I think after you read this it would be helpful to discuss just to make sure that we all understand these points in the same way.

I have not sent these procedures to Susan yet because I would like you all to review, ask any questions you have and discuss those changes before sending to Susan. Also, it is my impression, and I would like clarification on this, that these are just briefing points, not necessarily to be given out to the public? We would like to do another review of the document if it is going to be given out to the public.

Please let me know what you think.

Thank you,

(b) (6)

CC:

(b) (6)

Talking Points for Oversight Committee meeting 7/27/04

- Truman, Johnson, Reagan, and Clinton have cameras. Requests are in our 2006 security initiative. Cameras are about \$1500 each and we average 2 per research room. Additional monitoring equipment is needed for the security control centers in some libraries. \$150,000 estimate to install cameras and monitoring equipment in remaining libraries.
- Recognize distinction between protection of original records and the protection of information in the records.
- Under the law, the former president and/or his designated representative have access to the records anytime, anywhere. As a matter of policy we do not send our originals out of our buildings. The procedures we used were drawn from the statutory requirements in 44 U.S.C § 2205(2) and E.O. 13233 which allows for review of presidential records for privilege concerns and states the records SHALL be available. This is also stated in our coded regulations without reservation. The limits we have placed on access, requiring designations in writing and not sending originals out of the facility, have been accepted but have caused considerable frustration by the reps when such limitations impeded timely access, i.e. the time required to make and send copies.
- Access to classified information requires necessary clearances and completion of an SF 312, Classified Information Nondisclosure Agreement.
- If Sandy Berger had had a cleared venue in which to store the documents we could have provided copies of any or all of the documents he wished to review.
- Not a research room venue or situation. NARA monitors were not required to be in the room. When NARA personnel were present it was a matter of assistance. Why should they take what they have a right to have? The situation is completely analogous to the access provided Congress to their materials housed in Archives I.
- How could the monitor be ordered out of the room? We were dealing with the personal representative of the president and since the access was statutory we had no authority to deny the request. Given the subsequent events, we would not now leave a representative examining classified material alone nor permit the use of a cell phone.
- Given that, we have certainly reexamined these premises and set out new procedures for classified access so that we can be better assured the information is protected.
- Classified research room at A1 opened by February. That research room is constantly monitored and operates as a “clean” research room.

■ As a professional archivist I interject this note of caution: all of our precautions do two things: they help protect from accidental or inadvertent compromises or removal of documents and they help to deter the opportunist thief. They do NOT however prevent someone who seriously intends to steal a document or compromise information even with constant monitoring. You can only see what you think you see. A professional thief with a slight of hand can pocket a document while you believe he has only replaced his handkerchief.

Staff Resources & Services	Supervisor Resources	NARA Policies & Guidance	Archives & Records Management	Safety, Security & Emergency	NARA Organizations	Procurement, Budget & Finance	Project Information	Information Technology	Strategic Planning & Reporting
----------------------------	----------------------	--------------------------	-------------------------------	------------------------------	--------------------	-------------------------------	---------------------	------------------------	--------------------------------

Home NARA Policies & Guidance Directives

Interim Guidance 1600-5, Access to Materials Containing Classified Information in NARA Research Rooms by Non-Governmental Persons

Directives

100 - Mission and Organization
200 - General Administration
300 - Human Resources
400 - Budget and Accounting
500 - Procurement (Acquisition)
600 - Travel
700 - Transportation
800 - Information Management
900 - Congressional and Legislative
1100 - Legal, Ethics, and Professional Conduct
1200 - Audits and Investigations
1300 - Records Lifecycle (general)
1400 - Front End
1500 - Archival
1600 - Access

Search NARA Directives:

<input type="text"/>
<input type="button" value="search"/>
Help
Advanced Search

Page Options

INTERIM GUIDANCE 1600-5

March 31, 2004

SUBJECT: Access to Materials Containing Classified Information in NARA Research Rooms by Non-Governmental Persons

TO: Office Heads, Staff Directors, ISOO, NHPRC, and OIG

1. What is the purpose of this directive?

a. This interim guidance supplements NARA's policy on using NARA research rooms by specifying the steps that NARA staff must take to control and monitor space for authorized non-Governmental researchers to view materials containing classified information (classified materials). (See the Information Security Manual [INFO. SECURITY 202], chapter 2.)

b. INFO. SECURITY 202 applies to Government persons viewing materials containing classified information.

2. What is the authority for this directive?

- a. 36 CFR 1254.48, 1270, and 1275;
- b. Executive Order 12958, as amended; and
- c. INFO. SECURITY 202

3. What are the general rules for using NARA research rooms?

Follow the regulations in subparts B and E of 36 CFR Part 1254.

4. Where must researchers view classified materials?

a. Limit the research of classified materials to a designated classified research room if the volume of research at the facility justifies the establishment of such a room.

b. If the facility does not have a classified research room, use a Sensitive Compartmented Information Facility (SCIF) or dedicated conference room or other limited-access area, not an active office (see par. 6). When using a dedicated conference room or other limited-access area, follow the procedures specified in INFO. SECURITY 202, ch. 4, subpar. 7d for care of working spaces.

c. Do not provide access to authorized researchers in any research room where

Print this Page
Email this Page
Find Text on this Page
Provide Feedback on this Page
Add Page to Favorites

Site Search

<input type="text"/>	<input type="button" value="Go"/>
<input checked="" type="radio"/> Entire Site <input type="radio"/> This Section	
Advanced Search	

Employee Locator

<input type="text"/>	<input type="button" value="Go"/>
Advanced Locator	

there are non-authorized researchers or staff not cleared at the appropriate level.

d. Researchers must be restricted from any location that holds records other than those to which they have due access authority, unless waived by the Deputy Archivist.

5. To whom and to what records does this directive apply?

This directive applies to non-Governmental persons who are provided access to classified materials in any NARA facility. It also applies to all types of classified materials that they use, regardless of the legal status, as per INFO. SECURITY 202 (e.g., accessioned records, all records center holdings regardless of disposition, Presidential records, and donated historical materials).

6. In addition to research room procedures cited in 36 CFR Part 1254, what special rules apply to classified research rooms?

a. Clean research room procedures must be strictly enforced. Notes or copies may not be removed from the research room unless authorized by the appropriate equity holder. Using NARA's derivative classification authority, any notes must be stamped with the appropriate classification markings or refer the notes to the appropriate equity-holding agency for review and appropriate classification marking. All notes must be taken on NARA-provided and identifiable stationery. Where necessary, NARA computers and floppy diskettes may be provided. (No non-NARA computers may be used.)

b. The following personal items are prohibited within the classified research room:

(1) Two-way transmitting equipment;

(2) Recording equipment (photographic, audio, video, or optical) and all associated media;

(3) Computers and associated media, with the exception of a NARA-provided computer, if approved in advance by the appropriate equity holders and if available;

(4) Cell phones;

(5) Two-way pagers;

(6) Palm pilots (or PDA); and

(7) Wrist watches with photographic capability.

c. Where available, implement secure, overt close circuit television (CCTV) monitoring and recording (if the classified research room is a SCIF).

d. Research room staff must

(1) Ensure that researchers complete the form, Notification to Researchers Using NARA Classified Research Rooms.

(2) Provide only one box to a researcher to review at one time. Multiple boxes may be pulled and made ready for review but researchers may have only one box on the table at one time. Boxes that are waiting to be reviewed must be monitored by NARA staff cleared at the appropriate level.

(3) Ensure that couriers handle classified materials in accordance with INFO.

SECURITY 202.

(4) Restrict the number of researchers to facilitate adequate monitoring by NARA personnel.

7. Why can't I leave the researcher alone if there is an active CCTV system that is recording all the time?

The CCTV system is a deterrent measure and aids in any investigations. However, it is not a substitute for continuous monitoring by NARA staff.

8. What are classified production reviews?

Production reviews are materials produced in response to special access requests to classified materials pursuant (1) to a subpoena or other court-ordered request, (2) for a Congressional request, and (3) for an independent investigation or commission.

9. What special procedures apply to classified production reviews?

Research room staff must

a. Ensure that the room and any researchers are continuously monitored by NARA staff cleared at the appropriate level (continuous monitoring means that a NARA staff member must be devoting full time to watching the researcher and not performing other duties). Where a researcher is reviewing records under a classified production review (see [par. 8](#)) and a waiver has been granted in accordance with [par. 10](#), two NARA staff members must continuously monitor the room and the researcher.

b. Provide only numbered copies unless a waiver has been granted (see [par. 10](#)). Number the pages of the copies sequentially, starting with page 1 of the first document through the last page of the last document.

c. Maintain a log (with description and page counts of the individual documents) or a second control set of all documents provided. (The original documents may be used as the second control set.)

d. Require the researcher to sign a receipt (NA Form 14001, Reference Service Slip) as each box is provided. Returned boxes must be reviewed by NARA staff before the researcher leaves the classified research room. When available, a second NARA staff member may review the returned documents while the first staff member monitors use of another box by the researcher.

10. How do I request a waiver for providing the original documents instead of copies?

Send a request, in writing, to the appropriate information security manager, explaining the need to provide original documents and affirming that double monitoring will be used. The information security manager sends the request to the General Counsel (NGC), the appropriate office head or deputy, and the Space and Security Management Division (NAS), who serve as a review group. The review group weighs the factors in the request along with time requirements and likely production quantities and makes a recommendation on whether or not to grant a waiver. NGC sends the request to the Deputy Archivist for the decision. The location providing access is responsible for providing dedicated double coverage in the classified research room.

11. How do I verify that a researcher has the proper security clearance?

Researchers must have their cognizant security office submit a visit request with verification of their clearances to the NARA Personnel Security Officer in NAS via fax on 301-837-3657. The NARA Personnel Security Officer notifies the custodial unit of the researcher's clearance. Special access programs must request appropriate clearances and process them through appropriate channels.

12. What if I suspect that a researcher is handling classified materials inappropriately in a research room?

a. Immediately contact the most senior NARA official responsible for the research room who is immediately available and report your suspicions to him or her.

b. Contact your support security personnel on-site, and have them stand by to assist as determined by the senior NARA official.

c. The senior NARA official responsible for the research room makes a determination as to what course of action to take in consultation with security personnel.

13. What is the process if I determine that a security incident has occurred?

Follow the procedures in INFO. SECURITY 202, Chapter 7, Violations of Security.

14. What if I suspect that a researcher is taking classified materials from the research room, and he or she does not respond to my request to stay and wait for a senior NARA official?

a. Activate the duress alarm in the research complex, if available.

b. Call security control or the local law enforcement emergency number for assistance.

c. Provide details as requested by security or law enforcement.

d. Be prepared to provide full identity and description of the researcher and the classified level of the materials that you suspect to be missing.

e. Promptly contact the Office of the Inspector General (OIG) and NAS to report the incident or suspected incident.

15. Who are the senior NARA officials for the purpose of this directive?

The following serve as the senior NARA officials to notify as specified in pars. 12 and 14. If these officials are unavailable, follow the normal chain of command up from the designated official.

a. Archives I

(1) NL classified materials - Director, NLMS

(2) NWL classified materials - Supervisory Archivist

(3) ISOO classified materials - Assistant Director

b. Archives II

(1) Classified Research Room - NWCTF

(2) Nixon Presidential Materials Staff - Director, NLNS

- c. Presidential library - Supervisory Archivist
- d. Regional archives - Director of Archival Operations

16. What if a researcher will not leave the classified research room upon request?

- a. Activate the duress alarm in the research complex, if available.
- b. Call security control or the local law enforcement emergency number for assistance.
- c. Provide details as requested by security or law enforcement and await their arrival.
- d. Do not place yourself in a position to be harmed or to become confrontational with the researcher.

17. Can I detain or physically remove a researcher from the classified research room?

No. The only time you can become physical with a researcher is in self-defense.

18. Can I request to search a researcher or any of their possessions?

No, you are not authorized to conduct any investigative inquiries or searches.

19. Do I have to cooperate with security and law enforcement regarding an official investigation?

Yes, you have an obligation to cooperate fully during any officially sanctioned administrative or criminal investigation.

20. How are records created by this directive maintained under NARA's records schedule?

Maintain records created by this directive under item numbers 1417 through 1421, as applicable.

21. Whom can I contact for more information?

For questions regarding this interim guidance, contact Joyce Thornton (NAS) in room 2300, All; on 301-837-0296; by fax on 301-837-3657; or by e-mail.

LEWIS J. BELLARDO
Deputy Archivist of the United States and Chief of Staff

Attachment
(Form - Notification to Researchers Using NARA Classified Research Rooms)

[Top of Page](#)

to LII (Legal Information Institute) home



US CODE COLLECTION

[collection home](#)

[search](#)

[donate](#)

[Prev](#) | [Next](#)

TITLE 18 > PART I > CHAPTER 1 > § 4

§ 4. Misprision of felony

Release date: 2004-08-06

Whoever, having knowledge of the actual commission of a felony cognizable by a court of the United States, conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States, shall be fined under this title or imprisoned not more than three years; or both.

Search this title:

- [Notes](#)
- [Updates](#)
- [Parallel authorities \(CFR\)](#)
- [Your comments](#)

[Prev](#) | [Next](#)

LII has no control over and does not endorse any external Internet site that contains links to or references LII.

[credits](#)

[about us](#)

[send email](#)

LII

US CODE COLLECTION

legal information institute



[collection home](#)

[search](#)

[donate](#)

[TITLE 18 > PART I > CHAPTER 37 > § 793](#)



[Prev](#) | [Next](#)

§ 793. Gathering, transmitting or losing defense information

Release date: 2004-08-06

Search this title:

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any

Search input field

Search Title 18

[Notes](#)

[Updates](#)

[Parallel authorities](#)

[\(CFR\)](#)

[Your comments](#)

foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense,

(1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or

(2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

Shall be fined under this title or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

(h)

(1) Any person convicted of a violation of this section shall forfeit to the United States, irrespective of any provision of State law, any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, from any foreign government, or any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, as the result of such violation. For the purposes of this subsection, the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1) of this subsection.

(3) The provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853 (b), (c), and (e)-(p)) shall apply to—

- (A) property subject to forfeiture under this subsection;
- (B) any seizure or disposition of such property; and

(C) any administrative or judicial proceeding in relation to such property, if not inconsistent with this subsection.

(4) Notwithstanding section 524 (c) of title 28, there shall be deposited in the Crime Victims Fund in the Treasury all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law.

[Prev](#) | [Next](#)

LII has no control over and does not endorse any external Internet site that contains links to or references LII.

[credits](#)

[about us](#)

[send email](#)

LII

legal information institute
collection home

US CODE COLLECTION

search



donate

Prev | Next

TITLE 18 > PART I > CHAPTER 47 > § 1001

§ 1001. Statements or entries generally

Release date: 2004-08-06

(a) Except as otherwise provided in this section, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully—

- (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact;
- (2) makes any materially false, fictitious, or fraudulent statement or representation; or
- (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry;

shall be fined under this title or imprisoned not more than 5 years, or both.

(b) Subsection (a) does not apply to a party to a judicial proceeding, or that party's counsel, for statements, representations, writings or documents submitted by such party or counsel to a judge or magistrate in that proceeding.

(c) With respect to any matter within the jurisdiction of the legislative branch, subsection (a) shall apply only to—

- (1) administrative matters, including a claim for payment, a matter related to the procurement of property or services, personnel or employment practices, or support services, or a document required by law, rule, or regulation to be submitted to the Congress or any office or officer within the legislative branch; or
- (2) any investigation or review, conducted pursuant to the authority of any committee, subcommittee, commission or office of the Congress, consistent with applicable rules of the House or Senate.

Search this title:

Search Title 18

- Notes
- Updates
- Parallel authorities (CFR)
- Your comments

Prev | Next

LII has no control over and does not endorse any external Internet site that contains links to or references LII.

credits

about us

send email



legal information institute
collection home

US CODE COLLECTION

search

to US Code home

donate

Prev | Next

TITLE 18 > PART I > CHAPTER 93 > § 1924 ~~1924~~

§ 1924. Unauthorized removal and retention of classified documents or material

Release date: 2004-08-06

(a) Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

(b) For purposes of this section, the provision of documents and materials to the Congress shall not constitute an offense under subsection (a).

(c) In this section, the term "classified information of the United States" means information originated, owned, or possessed by the United States Government concerning the national defense or foreign relations of the United States that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure in the interests of national security.

Search this title:

Search Title 18

- Notes
- Updates
- Parallel authorities (CFR)
- Your comments

Prev | Next

LII has no control over and does not endorse any external Internet site that contains links to or references LII.

credits

about us

send email

From: (b) (6)
To: (b) (6)
Date: 7/23/04 4:02PM
Subject: Fwd: Re: this morning's Post

(b) (6)

While I doubt they will do the NARA notice it was nice of Gary to make the suggestion.

(b) (6)

From: GaryM Stern
To: Bellardo, Lewis; Brachfeld, Paul; Carlin, John; Claypoole, Richard; Constance, John; Cooper, Susan; Fawcett, Sharon; Lisowski, Lori; (b) (6)
Date: 7/23/04 3:59PM
Subject: Re: this morning's Post

Assuming that the Post does issue a retraction, then I would think a NARA Notice on Monday might be appropriate, in order to explain that the Post was incorrect, to remind all NARA staff that all communications with the press must be coordinated with NCON, and to commend the NARA staff involved in this matter for having acted responsibly and appropriately throughout this entire matter.

>>> Susan Cooper 7/23/04 2:56:50 PM >>>

I just called the copy editor at the Post---(Fred Hiatt is on deadline and was not available). the copy editor said that he thinks there will be a retraction in tomorrow's paper. He will confirm that for me and let me know within an hour or two.

Susan

>>> Susan Cooper 07/23/04 10:24AM >>>

I want to try to shed some light on this morning's editorial. I have spoken to Sue Schmidt who wrote yesterday's detailed article about the Berger case and also to Fred Hiatt at the editorial board. Sue agreed that I had not commented on the case in our conversations and said that if the editorial board got their information from her article, that they were mistaken.

I then spoke to Fred Hiatt who asked me rather cryptically if I knew for a fact that I was the only person speaking from the National archives. I assured him that I was, and that I have not spoken to anyone from the editorial board in months. I told him that this matter was of the greatest importance to the National Archives and to me personally and that we wanted a retraction. He said that he would speak to the person who wrote the story and let me know.

I will get back to all of you with any further updates.

susan

From: Susan Cooper
To: GaryM Stern; John Carlin; John Constance; Lewis Bellardo; Lori Lisowski; (b) (6)
(b) (6) Richard Claypoole; Sharon Fawcett
Date: 7/23/04 5:15PM
Subject: press update

Besides the Post retraction, there may be a Post story on research room regulations. There will definitely be a NYT article on Research Room regulations. Time Magazine is going to do a story that will probably include something on our regulations.

Michael Barone (US News) also called about Berger--wasn't sure, but may do an editorial.

susan

John Laster - Fwd: Re: NARA Notice 2004-189, Classified Research at NARA

From: (b) (6)
To: (b) (6)
Date: 7/21/2004 3:22 PM
Subject: Fwd: Re: NARA Notice 2004-189, Classified Research at NARA

(b) (6)
I thought you would be interested in seeing Rich's comment.

(b) (6)

From: Richard Claypoole
To: Bellardo, Lewis; Carlin, John; Constance, John; Cooper, Susan; Fawcett, Sharon; Lisowski, Lori; (b) (6) Stern, GaryM; Thomas, Adrienne
Date: 7/21/04 3:08PM
Subject: Re: NARA Notice 2004-189, Classified Research at NARA

We were surprised to see this notice without any prior discussion. We thought a decision had been made not to go beyond the basic "no comment" of the first para. In particular, the third para. seems defensive and an admission of, at least, carelessness. Since this notice will certainly end up in the media, do we still just say "no comment" and refer all callers to Susan?

>>> NOTICE 07/21/04 02:34PM >>>

This is a NARA notice to all employees.

Attention supervisors: If you have employees who do not have access to a computer, please ensure that he or she receives a copy of this notice. This includes employees on LWOP or paid leave.

July 21, 2004

You have no doubt read or heard a lot in the news this week about the National Archives, classified records and former Clinton Administration official Samuel Berger. As this matter is currently under investigation by the Justice Department and the FBI, it is not appropriate for NARA to make any statements about the case.

I do want to reiterate to you, however, that we take the security of our holdings very seriously. Internally, we have taken steps to be sure that we are adequately protecting our holdings, especially classified holdings. This has included updating our guidance on access to classified records in Interim Guidance 1600-5, Access to Materials Containing Classified Information in NARA Research Rooms by Non-Governmental Persons, which was issued in March.

If there are other things we learn as a result of this investigation, you can be assured we will make whatever changes are necessary to ensure the proper handling and security of our holdings.

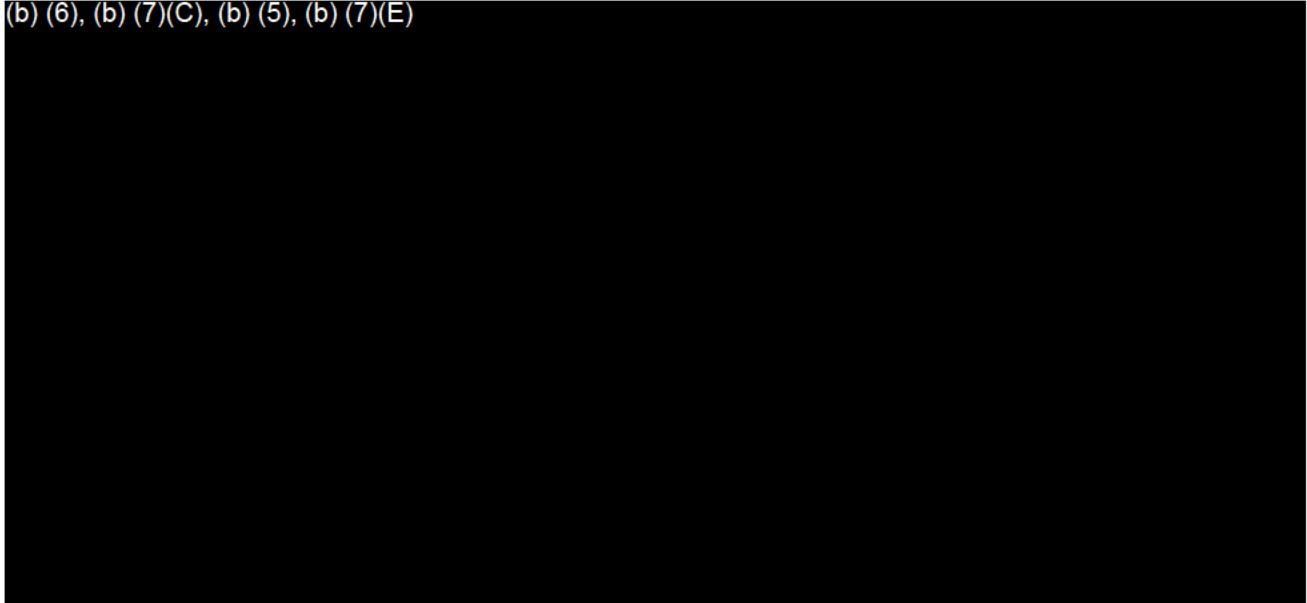
John W. Carlin
Archivist of the United States

For questions on this notice contact:
Lori Lisowski, NPOL
lori.lisowski@nara.gov
Room 4100, AII
Phone: 301-837-1850
Fax: 301-837-0319

From: (b) (6), (b) (7)(C)
To: (b) (6)
Date: 8/25/04 8:25AM
Subject: Interview

(b) (6)

(b) (6), (b) (7)(C), (b) (5), (b) (7)(E)



(b) (6), (b) (7)(C)

CC: Brachfeld, Paul

(b) (6), (b) (7)(E), (b) (7)(C)

Obtained via FOIA by Judicial Watch, Inc.

Filename: bjl 2 3 2004.doc
Directory: D:\My Documents
Template: C:\Documents and Settings\ (b) (6) Application
Data\Microsoft\Templates\NORMAL.DOT
Title: The following docs were not located at NLMS
Subject:
Author: Vault
Keywords:
Comments:
Creation Date: 2/3/2004 1:45 PM
Change Number: 1
Last Saved On: 2/3/2004 5:12 PM
Last Saved By: Vault
Total Editing Time: 97 Minutes
Last Printed On: 5/24/2005 2:33 PM
As of Last Complete Printing
Number of Pages: 1 (approx.)
Number of Words: 20 (approx.)
Number of Characters: 118 (approx.)

9800322	0067738
9800407	0006009
9806476	0005802
9801594	9906471
0004240	9808221
9808069	9803158
9907201	9901422
9908717	0100054
	98041843

~~9826303~~
0007764
9909274
0004215

9901422	9930241
0100054	9830086
9804143	0030192
9900228	9930178
9907150	0002563
0004677	0001712
	9820692
	9820622

Filename: Original Numbered Docs pulled from NLMS for Terror
Comm.xls
Directory: D:\My Documents
Template: C:\Documents and Settings\ (b) (6) Application
Data\Microsoft\Templates\NORMAL.DOT
Title:
Subject:
Author: (b) (6)
Keywords:
Comments:
Creation Date: ~~5/24/2005 3:24 PM~~ Actually created 10/10/03
Change Number: 1
Last Saved On:
Last Saved By:
Total Editing Time: 0 Minutes
Last Printed On: 5/24/2005 3:24 PM
As of Last Complete Printing
Number of Pages: 2
Number of Words: 90 (approx.)
Number of Characters: 516 (approx.)

I think (check)
This equals those
docs found in NLMS
Search of RMS for EOP2
I don't do have "3" as
3CC Light. [This doesn't include
docs that BF had already found &
indicated ~~as~~ from the
direct RMS printout. That info is on printout]

Original Numbered
Documents from NLMS

9830013
9930178
9930325
30051
30072
30105
30122
30218
30305
9808571
9830223
30140
30040
30020
30375
30495
30441
30168
30130
9830163
9830173
9930262
9830318
9830194
9830193
9830135
9830137
9930212
9930211
9930195
9930182
9930141
9930126
9900521
9808457
9930335
9930240
9930233
9930214
9909164
9909178
9930339
30450
30438
9930011
9930345
9930200
9930150
9830309
9930172
9930281
9930156
9830215

9905980
9903731
9902943
9830154
9830178
9830259
9930237
9830204
9930351
30003
30171
30201
30241

9808457

Filename: Terrorism List for NLCP in Word.doc
Directory: S:\Access Issues\NLMS ACCESS FILES\NLMS 2003-035
(SAGB - Terrorism Commission) (CP)
Template: C:\Documents and Settings\ (b) (6) Application
Data\Microsoft\Templates\NORMAL.DOT
Title: Number Request
Subject:
Author: nara
Keywords:
Comments:
Creation Date: 6/11/2003 5:01 PM
Change Number: 2
Last Saved On: 6/11/2003 5:01 PM
Last Saved By: nara
Total Editing Time: 1 Minute
Last Printed On: 5/24/2005 2:28 PM
As of Last Complete Printing
Number of Pages: 3
Number of Words: 208 (approx.)
Number of Characters: 1,188 (approx.)

This equals those
docs found in
NLMS search of
RMS for ^{EP2} that don't have
"3" as the 3rd digit
[This doesn't include docs that BF had already
found & indicated from the direct RMS
printouts. That info is on those
printouts.]

Number	File Series
9802004	PA
9805755	PA
9805869	PA
9805870	PA
9805874	WH
9805909	PA
9805958	PA
9805961	PA
9806026	WH
9806027	PA
9806082	WH
9806085	PA
9806086	PA
9806097	PA
9806134	NOT LISTED
9806136	PA
9806475	PA
9806594	PA
9806652	WH
9806751	PA - LIMITED ACCESS
9806787	PA
9806843	WH
9807077	PA
9807189	PA
9807344	WH
9807671	PA
9807938	PA
9808325	WH
9808457	PA
9808571	PA - LIMITED ACCESS
9808694	PA - LIMITED ACCESS
9820231	IFD
9820232	IFD
9820365	IFD
9820460	IFD O
9820461	IFD O
9820464	IFD O
9820471	IFD O
9820479	IFD
9820492	IFD
9820519	IFD
9820530	IFD O
9820531	IFD
9820563	IFM
9820685	IFD O
9820819	NS

9820944	IFD
9900080	IFD
9900181	PA
9900521	PA - LIMITED ACCESS
9900689	PA
9900703	PA
9900789	PA
9901048	NS
9901172	PA
9901266	PA
9901551	PA
9901751	PA
9902173	PA
9902291	ADMIN
9902885	PA
9902943	PA
9903209	NOT LISTED
9903731	PA - LIMITED ACCESS
9904062	PA
9904222	PA
9904505	PA
9904777	PA
9905058	PA
9905235	PA
9905337	NOT LISTED
9905785	PA
9905810	PA
9905980	PA - LIMITED ACCESS
9906524	PA
9907620	PA
9907864	PA
9908157	PA
9909122	PA
9909164	PA
9909178	PA
9909363	PA - LIMITED ACCESS
0001065	PA
0001071	PA
0001172	PA
0001307	PA
0001599	PA
0001656	PA
0001892	PA
0002004	PA
0002052	PA
0002388	PA
0003464	PA

0004219	PA
0005885	PA
0006435	PA
0006455	PA
0006555	PA
0007029	PA

Filename: Search Results from NSC 061803.doc
Directory: S:\Access Issues\NLMS ACCESS FILES\NLMS 2003-035
(SAGB - Terrorism Commission) (CP)
Template: C:\Documents and Settings\██████████(b) (6).Application
Data\Microsoft\Templates\NORMAL.DOT
Title: 9608338
Subject:
Author: nara
Keywords:
Comments:
Creation Date: 6/18/2003 11:26 AM
Change Number: 1
Last Saved On: 6/18/2003 11:36 AM
Last Saved By: nara
Total Editing Time: 11 Minutes
Last Printed On: 5/24/2005 2:26 PM
As of Last Complete Printing
Number of Pages: 1
Number of Words: 62 (approx.)
Number of Characters: 355 (approx.)

*This seems to
equal docs from
lists sent forward
by John Ficklin*

9608338	0006175
9800929	0006616
9801642	0006718
9806286	0006733
9806389	0100015
9806511	0100070
9806817	
9820047	
9820068	
9820092	
9820092	
9820144	
9820233	
9820251	
9820258	
9820310	
9820312	
9820316	
9820359	
9820360	
9820381	
9820424	
9820454	
9820622	
9820630	
9820692	
9820699	
9820700	
9820701	
9820702	
9900024	
9900392	
9900590	
9901426	
9901911	
9902128	
9902179	
9902603	
9909363	
0000403	
0000403	
0001712	
0002563	
0002563	
0002563	
0002563	

Filename: Terrorism Search Results.doc
Directory: S:\Access Issues\NLMS ACCESS FILES\NLMS 2003-035
(SAGB - Terrorism Commission) (CP)
Template: C:\Documents and Settings\ (b) (6) Application
Data\Microsoft\Templates\NORMAL.DOT
Title: Narrow Search Results
Subject:
Author: nara
Keywords:
Comments:
Creation Date: 6/11/2003 9:11 AM
Change Number: 1
Last Saved On: 6/11/2003 9:18 AM
Last Saved By: nara
Total Editing Time: 8 Minutes
Last Printed On: 5/24/2005 2:29 PM
As of Last Complete Printing
Number of Pages: 1 (approx.)
Number of Words: 134 (approx.)
Number of Characters: 770 (approx.)

Narrow Search Results

-Only searching Afghanistan in conjunction with the terms terror* or counterterror*. It also means only searching the terms terror* or counterterror* in conjunction with the countries listed in part 3.

(Because we do not yet have the ability to limit by date on the cable and e-mail systems and because one bucket of the e-mail for the relevant time period could not be searched, these numbers are approximate.)

RMS	208
E-mail	32,779
Cables	36,558

Broad Search Results

-Searching Afghanistan alone (not in conjunction with the terms terror* or counterterror*) and searching the terms terror* or counterterror* alone.

(Because we do not yet have the ability to limit by date on the cable and e-mail systems and because one bucket of the e-mail for the relevant time period could not be searched, these numbers are approximate.)

RMS	1003
E-mail	95,895
Cables	132,515

SpD Sentencing Memor Burguis Plea

SPD Sentencing Memorandum Plea

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

-----X
 :
 :
 UNITED STATES OF AMERICA :
 :
 :
 v. :
 :
 :
 SAMUEL R. BERGER, :
 Defendant :
 :
 :
 -----X

Docket No. 05-0175M-01

SENTENCING MEMORANDUM ON BEHALF OF
SAMUEL R. BERGER

Lanny A. Breuer
David N. Fagan
Covington & Burling
1201 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
(202) 662-6000

Attorneys for Samuel R. Berger

TABLE OF CONTENTS

APPENDIX OF EXHIBITS ii

I. Preliminary Statement..... - 1 -

II. Facts - 4 -

1. Mr. Berger has led an extraordinary life of devotion and service to his country, community, and family...... - 4 -

2. Mr. Berger’s actions at issue, for which he has accepted full responsibility and deeply regrets, were an aberrational departure stemming from unique pressures that he felt to be prepared to answer fully questions related to 9/11...... - 10 -

3. Mr. Berger has cooperated fully with the government...... - 17 -

III. Sentencing..... - 17 -

IV. Conclusion - 19 -

APPENDIX OF EXHIBITS

Curt Anderson, "Sept. 11 Commissioners Say Berger Missing Document Probe Didn't Affect Report," Associated Press, July 23, 2004.	Exhibit 1
Letter from Eli Segal, founding CEO of AmeriCorps and longtime friend of Mr. Berger	Exhibit 2
Letter from Anthony Lake, Distinguished Professor, Georgetown University, and former National Security Advisor	Exhibit 3
Letter from Fred Reiner, Senior Rabbi, Temple Sinai, Washington, D.C.	Exhibit 4

I. Preliminary Statement

On April 1, 2005, Samuel R. ("Sandy") Berger pled guilty to a single misdemeanor violation of 18 U.S.C. § 1924(a), removing and retaining without authorization classified documents. Mr. Berger admitted before Your Honor that he removed from the National Archives and Records Administration ("NARA") and retained in his office a total of five copies of classified documents. Mr. Berger also admitted that he removed from NARA his own handwritten notes of classified material that he had reviewed there. These acts occurred in the summer and fall of 2003 in connection with Mr. Berger's review at NARA of Clinton Administration presidential materials responsive to document production requests issued by The National Commission on Terrorist Attacks Upon the United States ("9/11 Commission"). Mr. Berger is scheduled to be sentenced by Your Honor on September 8, 2005.

Mr. Berger has fully accepted responsibility for his conduct. He voluntarily made a factual proffer to the government, and he also provided a detailed statement acknowledging his wrongdoing to the United States Probation Officer. In addition, in compliance with the Plea Agreement reached with the Department of Justice, Mr. Berger has continued to cooperate fully and truthfully with the United States, and to provide all information known to him regarding this matter, including through a debriefing by the Inspector General of NARA. Under the terms of the Plea Agreement, this cooperation further reflects Mr. Berger's acceptance of responsibility for his actions.

As discussed in detail below, Mr. Berger's conduct in this case represented a foolish and aberrational departure from an otherwise extraordinary record of personal achievement and public service to this country. A devoted husband to his wife of 36 years, supportive father to his three children, selfless friend, and dedicated citizen to his community, Mr. Berger has led a truly exemplary and distinguished life. Even as he has achieved the highest

professional success and ably performed vast public duties, he has always managed to fulfill family and personal responsibilities and pursue valuable civic work. He has accomplished this fine balance with integrity and probity and in no small part through quiet personal sacrifice, intent to give up his time, to delay his professional ambition, and to sacrifice personal wealth (indeed, whatever has been required of him) in service of a friend, his community, his country.

More than anything, Mr. Berger's personal and professional success derive from two characteristics that define him: an unending drive to get it right, and a sincere dedication to the well-being of others. He brings these two qualities to every endeavor that he undertakes, and so, too, did they contribute to his exercise of reviewing materials at NARA. Mr. Berger spent many hours at NARA reviewing hundreds, if not thousands, of pages of material, designating every document that was potentially relevant for production to the 9/11 Commission. He voluntarily performed this public service under extraordinary time pressures and at daily expense to his personal business. He did so because he felt a responsibility to be able to answer fully all the questions of the 9/11 Commission, to help prepare colleagues to testify before the Commission, and to create as complete and accurate a public record on 9/11 as possible.

Mr. Berger's actions at issue, while misguided and wrong, were borne solely out of these same desires. At no time did Mr. Berger intend to harm the United States or deprive the 9/11 Commission of any material. Indeed, all of the documents at issue were copies, and the Commission has publicly confirmed that it received everything it requested and needed. (Exhibit 1). Nevertheless, Mr. Berger, in removing the materials in question for his own preparation, made a grievous error, and he has accepted the consequences of his actions.

Those consequences have had a profound effect on Mr. Berger and his family. His failure to live up to his own high standards of conduct has embarrassed him. His impeccable

record of public service has undoubtedly suffered, and, for that matter, his ability to perform public service in the area of national security — which is a true passion for him — will be limited for at least three years, unless the government on its own accord determines to restore his clearances before then. The emotional and financial costs of the entire ordeal have been considerable. And he and his family have endured a media frenzy that has included stakeouts of their home, false innuendo, and gross mischaracterizations of what actually occurred.

In accepting responsibility for his actions, Mr. Berger has made clear to the Department of Justice, the United States Probation Officer, and NARA that he understands his conduct was wrong and in no way seeks to excuse or justify it — a point that he will also make to Your Honor during sentencing on September 8. The parties have agreed that the appropriate fine for Mr. Berger's conduct is \$10,000, and that, as a consequence of his actions, Mr. Berger will not apply for or seek a United States government security clearance for a period of three years from the entry of the plea, although the government can choose to provide such a security clearance to Mr. Berger at any time. The government also has agreed not to oppose a request by the defense that Mr. Berger receive a non-custodial sentence.

In submitting this memorandum on Mr. Berger's behalf, we likewise do not seek to minimize the wrongdoing to which he has pled guilty. Rather, we submit this memorandum to provide context for the Court's consideration of an appropriate sentence and in support of Mr. Berger's request that, in light of all the facts and circumstances, the Court exercise its discretion to impose a non-custodial sentence and apply the penalties that the parties, through the Plea Agreement, have agreed are appropriate.

II. Facts

1. *Mr. Berger has led an extraordinary life of devotion and service to his country, community, and family.*

Born on October 28, 1945, Mr. Berger lived his entire childhood in Millerton, New York, the second child of a merchant and schoolteacher. From an early age, Mr. Berger demonstrated an appetite and aptitude for leadership, an innate drive for perfection, and a desire to perform public service. The valedictorian of his high school class, Mr. Berger enrolled in Cornell University in 1963 where he would become President of the Inter-Fraternity Council and a member of Quill and Dagger, an honor society recognizing outstanding leadership and service. He was selected as "Outstanding Member" of the entire graduating class of 1967. Following graduation, Mr. Berger sought to pursue his commitment to government service by serving as Special Assistant to former New York City Mayor John Lindsay and Legislative Assistant to Congressman Joseph Resnick (N.Y.). He also joined the United States Army Reserves in 1968, from which he was honorably discharged six years later.

After graduating *cum laude* from Harvard Law School in 1971, Mr. Berger set forth on a distinguished career moving from jobs in government and private law practice. His first position out of law school was as an assistant to Senator Harold Hughes (Iowa). In 1972, he joined the staff of Senator George McGovern and served as a speechwriter for Senator McGovern in his presidential campaign that year. After four years as an associate at Hogan & Hartson — where he would later become partner and head of the International Trade practice area — Mr. Berger returned to the public sector to serve as Deputy Director of the Policy Planning Staff at the Department of State (1977-1980).

It was in his early days of government and political service that Mr. Berger met many of the individuals with whom he would form lifelong friendships, among them Eli Segal,

Tony Lake, and Bill Clinton. Eli Segal describes the values that formed their early bonds and the evolution of that relationship into a lifelong friendship:

A common interest in public service lies at the heart of my friendship with Sandy Berger. We met in the late 60's when we assisted a U.S. Congressman. In subsequent years, we worked together on several presidential campaigns, helped numerous policy groups, and served together in the Clinton Administration. In the almost 40 years since we first made contact, I doubt that a week has gone by without a communication between us on some important public issue of the day.

But to define our relationship in that way understates the extent to which our lives are intertwined. Our wives and our children are extraordinarily close, we holiday with the Bergers on a regular basis, I am proud to have been Sandy's first client at Hogan and Hartson and Sandy has been there for me during all of those moments in life when you just need a friend and wise counselor in your corner.

(Exhibit 2).¹

In 1992, Mr. Berger took a leave from his highly successful private law practice to serve as a Senior Foreign Policy Advisor to Governor Bill Clinton's presidential campaign and, then, Assistant Transition Director for National Security as part of the Clinton transition team. Mr. Berger was named Deputy Assistant to the President for National Security Affairs ("Deputy National Security Advisor") in January 1993, and was appointed to the position of National Security Advisor in January 1997, serving until the end of President Clinton's second term. Thus, for eight years, Mr. Berger served in the most sensitive positions in government at a unique time in our nation's history — the first full-term post-Cold War presidency.

¹ While we could have submitted many more letters to Your Honor on Mr. Berger's behalf, including from the former President and other statesmen, we have elected to submit the three attached letters, which are from individuals who represent distinct aspects of Mr. Berger's life and who eloquently speak to Mr. Berger's commitment to public service, his qualities as a friend, husband and father, and his dedication to his community.

Such positions naturally impose incredible demands on those who hold them, and Mr. Berger was no exception. He worked days and nights — in fact, he became legendary around the White House for his stamina and the amount of work that he generated — to effect U.S. interests abroad, improve the well-being of other nations, and protect our nation against threats to our security. He performed this work admirably, contributing to successes that positively affected the lives of millions of people. These included helping to formulate and prosecute humanitarian interventions (e.g., Haiti, Bosnia, Kosovo), designing and pursuing strategic engagements relationships with historic rivals (e.g., engagement with Russian and China), liberalizing and expanding trade throughout the world, pursuing the NATO engagement in Kosovo and fostering a peaceful regime change in the former Yugoslavia, and driving negotiations for peaces in troubled regions (e.g., Northern Ireland, Middle East). There always will be debate about individual initiatives undertaken by any Administration, but one thing is unequivocally clear about Mr. Berger's record: in every issue that he pursued over the course of these eight years — indeed, in all that he has pursued both in his public and private capacities — Mr. Berger earned the trust of those closest to him through his unceasing integrity and honesty and commitment to doing the job the right way.

Tony Lake, Mr. Berger's former boss at the Policy Planning Staff and again in the White House, speaks to these qualities:

I have known Sandy very well for some thirty years I have known him, always, as a man of extraordinary integrity.

As my Deputy, and then as National Security Advisor, Sandy was notable -- and widely noted -- for his exemplary ability to bring before the President the views of his colleagues fairly and openly. He did not play games in his role as "honest broker."

While advising political candidates over the years, Sandy was most certainly doing so from a partisan perspective. But I have often been

struck by how he proceeded from, and was bound by, an honest assessment of the substance of the issues.

And, in many personal dealings with Sandy over the years, I have never known him to be anything but honest and candid. I would trust him, and have trusted him, with anything and everything.

(Exhibit 3).

Eli Segal adds: "Sandy Berger is the ultimate workhorse. Whether building a dollhouse for each of his daughters, doing legal work for a client, or representing the interests of his country, Sandy's approach is simple and consistent: get it right, without regard to whether he derives any personal benefit from the effort." (Exhibit 2).

Beyond his well-known professional record, Mr. Berger has applied the very qualities of which Tony Lake and Eli Segal speak so highly — his reputation for honesty and integrity and his commitment to doing things the right way — in pursuit of important civic work. For example, for the last three years, he has served as senior counselor to the International Commission on Holocaust Era Insurance Claims (ICHEIC), crafting the criteria for, and assisting in, the evaluation of claims made by thousands of Holocaust survivors and their heirs to insurance policies from the Holocaust period. In this capacity, Mr. Berger has assisted in the award of more than \$26 million to Holocaust victims and their descendants. He also has been an active member of his synagogue, serving as trustee and officer and chairing a capital contribution campaign even while he was heavily involved in the presidential campaign of 1992. Rabbi Fred Reiner, chief rabbi of Mr. Berger's congregation, Temple Sinai, in Washington, D.C., says:

Sandy has been extraordinarily generous with his time and expertise in co-chairing our capital campaign, staff evaluations, and providing thoughtful and wise counsel on many occasions. Often we have turned to him for difficult assignments in the congregation, and he has responded with dedication and commitment

While we have had many members who have made significant contributions to our national life, Sandy Berger really stands alone as an

individual who has also made an enormous difference in the life [of] our congregation and religious community.

(Exhibit 4).

These examples do not even begin to recount the many hundreds of pro bono hours Mr. Berger contributed while in private law practice. These included service on the Board of Directors of the International Human Rights Law Group, pro bono assistance to the new Solidarity government in Poland after the fall of communism, and pro bono representation for three years of an indigent client under the Criminal Justice Act.

But perhaps what most defines Mr. Berger's generous spirit are the many works that he has done quietly to improve the lives of friends, colleagues, and neighbors — deeds that no one would ever know about but for the testimony of those closest to him. Eli Segal speaks of Mr. Berger's "unique commitment to others":

Sandy is completely selfless in the service of people regardless of rank.

It would be easy to address this attribute by appeal to the extensive public records. That record, however, would not include the hours he spent sitting with a dying friend at the same time he was serving as Deputy National Security Advisor, or the time he gave to complete the capital campaign that he led at his synagogue while fulfilling his public responsibilities, or the financial sacrifice he made when he purchased a home for a beloved, but nearly destitute, former teacher. The public record might, but probably doesn't, reflect his recommendation to President Clinton who wanted Sandy as his first National Security Advisor that someone else should have the appointment because he believed him to be better qualified.

(Exhibit 2).

Mr. Berger's commitment to matters about which he cares deeply also is evident in the personal and professional interests that he has pursued since leaving government office. In the spring of 2001, Mr. Berger founded Stonebridge International LLC, a global business strategy consulting firm. In four years, he and his partners have built the company to include

more than two dozen clients with offices in Washington, D.C. and abroad. Through Stonebridge and as a frequent public speaker, Mr. Berger has continued to serve as one of the brightest American foreign policy minds, helping to drive thinking and debate over issues such as how best to prosecute the war on terrorism, the potential for and obstacles to peace in the Middle East, and our strategic relationship with China. He is frequently called upon to testify on foreign policy issues before the Congress.

While Mr. Berger takes pride in the assistance that he has provided to his country, friends, community members, and clients over the years, nothing provides more joy or has received more attention than his family. Married for 36 years, he and his wife, Susan, are true partners in all of life's successes and travails. Their three children — Deborah, 32; Sarah, 28; and Alexander, 25 — have entered disparate, successful careers, and are making important contributions in the fields of media, law, and entertainment. In each of their lives, Mr. Berger has been the consummate dad, from coaching his son's baseball team for five years, building by hand elaborate dollhouses for his daughters (one took him two years to complete), tending to and nurturing their various interests, helping with their homework, and forming a monthly parent-children book club in their youth, to being their confidant, friend, and source of emotional support from their early adulthood to today. No matter the heights of his professional success or the extent of his public and other commitments, Mr. Berger has always had time to give first to his family. Rabbi Reiner speaks to this commitment:

I have had the privilege of officiating at several life cycle services and ceremonies with Sandy's family and know them well. I know him as a caring husband and dedicated father. I have witnessed his support for his family in the face of enormous professional and public service pressures. I have seen his dedication to our religious schools, where his children were educated, and to special programs that were important to his family.

(Exhibit 4).

American poet Ella Wheeler Wilcox wrote that “fortune smiles on those who work and wait.” That is certainly true of Sandy Berger. Mr. Berger has had the good fortune to be a successful husband, father, citizen, attorney, and public servant, and to be admired and loved by his family, friends, and colleagues. He has had such fortune because, as his friend Eli Segal writes, he is “a good man in the best sense of that term -- a man where good intentions have met good deeds over a lifetime.” (Exhibit 2).

2. Mr. Berger’s actions at issue, for which he has accepted full responsibility and deeply regrets, were an aberrational departure stemming from unique pressures that he felt to be prepared to answer fully questions related to 9/11.

Those who know Mr. Berger well and are familiar with his life’s work fairly ask how he came to take the actions at issue in reviewing documents at NARA. The answer starts with the terrorist attacks of September 11. The events of that day almost certainly touched every American, evoking a unique reaction in each one of us. For Mr. Berger, the outrage and sorrow over the tragedy were compounded both by the fact that he had been responsible for coordinating the response to terrorism issue while at the White House and because he immediately was deluged by questions from the press. These produced what, in retrospect, was a predictable response on his part — to become immersed in an effort to compile an accurate record of the Clinton Administration’s activities regarding terrorism in the 1990s. This also meant striving to fulfill what he believed to be an obligation, as former National Security Advisor, to assist first the Joint Congressional Intelligence Committee review of 9/11 and later the review of the 9/11 Commission and to prepare his former colleagues to answer the various 9/11-related inquiries accurately. Unfortunately, and inexcusably, Mr. Berger’s intense focus on these objectives, combined with the stress of the document review, produced a lapse in judgment at NARA that

resulted in the actions at issue. The record is clear, however, that those actions, while misguided, were taken entirely for his own preparation, and not for any other reason.

Following the attacks of September 11, Mr. Berger, like many of his former senior colleagues in the Clinton Administration, faced continuing press inquiries regarding what the Clinton Administration knew about Al-Qa'ida, and what the Administration did to address a range of issues related to it (e.g., terrorist financing, efforts to capture Bin Laden, policies toward Afghanistan and the Taliban, homeland security). For Mr. Berger, facing such intense interest and demands without the staff, organization and resources of his former office was an unfamiliar challenge. It also required a delicate touch — while many of the inquiries from the press, Congress, and others were legitimate, some were politically motivated, even in the short weeks after 9/11. Thus, Mr. Berger confronted a duty to respond to the legitimate questions and contribute to the overall education of the public, while also refuting, with facts, those critiques that were specious. Despite the lack of resources and having a new business to run, Mr. Berger, uniquely among his colleagues, assumed the leadership role in responding to these inquiries.

In particular, to respond to the questions relating to 9/11, Mr. Berger led an effort to reconstruct the entire Clinton record on terrorism. This proved a monumental undertaking for a variety of reasons. First, terrorism was just one of many issues (e.g., Iraq, the Balkans, the Middle East Peace Process, Russia, China, India-Pakistan, nonproliferation) that Mr. Berger and his colleagues dealt with over the course of eight years. Second, the issue of “terrorism” was complex, touching on many agencies and activities (e.g., tracking and seeking to find Al-Qa'ida operatives, blocking their finances, gathering intelligence and countering specific new threats, encouraging our allies and others to combat terrorism, protecting American assets at home and abroad). Third, in turn, no one person had all the details, and the numerous people who had dealt

with the various aspects of the "terrorism" issue were scattered all over the world. Fourth, there was a constant stream of new questions that Mr. Berger felt a responsibility to answer accurately. As a result, from 2001-2003, Mr. Berger spent hundred of hours on 9/11-related work and recreating the Clinton Administration record on terrorism, resulting in the production of literally volumes of materials addressing every aspect of the terrorism issue. (And, not surprisingly, this work paid off — a senior staffer for the Joint Congressional Inquiry into 9/11 remarked that Mr. Berger was the most helpful witness they interviewed.)

In the course of this work, Mr. Berger was designated to review Clinton Administration presidential materials at NARA, and later, in June 2003, was asked to review materials at NARA in response to document production requests from the 9/11 Commission. The purpose of this review was to approve the responsiveness of materials to the 9/11 Commission and to determine whether any materials should be exempted from the production on the basis of executive privilege. Mr. Berger, with the approval of the former President, determined to produce all potentially relevant materials and not to assert executive privilege over any document, even though many of the documents he reviewed fell within the clear boundaries of the privilege.

The document reviews turned out to be a protracted process, involving very long days that required Mr. Berger to be at the National Archives for eight to ten hours at a time. The reviews also were tiring, requiring Mr. Berger to review hundreds, if not thousands, of pages of materials on each occasion. Such an undertaking would have been a burden for a younger person, whose time was more his or her own and who perhaps would have been more accustomed to long document reviews. It was an extraordinary task for the former National Security Advisor.

The onerous nature of the reviews was particularly important because, in addition to reviewing and producing materials responsive to the 9/11 Commission, Mr. Berger viewed his visits to NARA as an opportunity to effect an important secondary purpose — namely, to use the document review to re-familiarize himself with the historical record dating back five years. In Mr. Berger's mind, such a re-familiarization was important to create a more complete record of the Clinton Administration's actions as they related to 9/11 and, in turn, be better prepared to testify before the 9/11 Commission and to prepare other Clinton Administration officials to testify as well. Ultimately, each of these factors in combination — the tiring nature of the review, the burden it imposed on Mr. Berger's schedule, and the importance that Mr. Berger attached to being prepared to testify before the 9/11 Commission and to prepare his colleagues — led Mr. Berger, acting wholly out of character, to take the actions summarized in the Factual Proffer read to Your Honor on April 1.

Specifically, during the course of his document review on September 2, 2003, Mr. Berger encountered a memorandum entitled the "Millennium After-Action Report" ("MAAR"), a self-critical assessment that Mr. Berger had asked Richard Clarke, the coordinator of the Counterterrorism Security Group of the National Security Council, to prepare in early 2000 after the United States had successfully averted planned Al-Qa'ida attacks over the millennium. Mr. Berger believed that the report would be of keen interest to the 9/11 Commission because it (i) reviewed vulnerabilities that had been manifest as a result of the Millennium exercise, (ii) concluded with a prescriptive section on measures to improve homeland security against terrorist threats, and (iii) already had received considerable public attention, including being mentioned in the New York Times and discussed in an article in The New Yorker. The report, however, was longer than many other documents that needed to be

reviewed, and there were many recommendations. Mr. Berger was certain that he would not be able to remember every point, and, at the time he came across the document, he was daunted by the prospect of trying to complete the document review that day, which he hoped would be the last time he would need to review materials at NARA. Accordingly, rather than ask to see the document at a later date, Mr. Berger, in what he fully acknowledges was a terrible decision, took the document when he left the Archives on September 2.

Notwithstanding his sincere hope to have concluded the review at the Archives in September, Mr. Berger was required to return on October 2 to review additional documents. During this review, he encountered additional draft versions of the MAAR, which did not appear to be identical (e.g., one had a different classification than the others). This raised a question in Mr. Berger's mind about whether there had been meaningful changes during its drafting process and, in turn, produced conflicting instincts: On the one hand, Mr. Berger wanted to be able to study the different versions so that he could be prepared to answer questions if there had been meaningful changes; on the other hand, he desperately wanted to complete the document review that day so that he would not have to return to NARA. Deciding that he could not reasonably take the time to compare the documents and still complete the document review that day, Mr. Berger repeated his unwise decision from September and determined to take the versions of the MAAR back with him to his office at the end of the day.

Importantly, none of the documents that Mr. Berger took were ever revealed to anyone outside of the Archives, nor, for that matter, did Mr. Berger ever discuss the fact that he had the documents. Mr. Berger compared the October 2 documents at his office later that night, and, after determining that there did not appear to be any substantial differences among them, cut up three and disposed of them to prevent anyone else from reading them. He kept a fourth to

compare to the September version at a later, less exhausted time. These were the two documents (the September version and one copy from the October review) that he returned a few days later to the Archives.

Furthermore, at no time did Mr. Berger believe that, by taking the document on September 2 or the additional versions on October 2, he would be depriving the 9/11 Commission of important material. Indeed, he assumed the opposite — namely, that the Commission would know about and have access to the MAAR from multiple sources and would ask questions about the document and its recommendations. It was apparent to Mr. Berger when he was reviewing the MAAR documents that they were copies, not originals. Mr. Berger also was aware that the report had been circulated widely through the inter-agency review process on multiple occasions while it was being prepared and considered. It therefore was inconceivable to him that other copies would not exist in other agencies, which copies the 9/11 Commission would be able to access. Moreover, as mentioned, the existence of the MAAR had been prominently discussed in public materials, leading Mr. Berger to conclude that the Commission staff would independently know of it. And, as the 9/11 Commission itself later confirmed and the Factual Proffer makes clear, the Commission in fact did receive all the documents that it requested and needed.

The Factual Proffer also refers to notes that Mr. Berger took with him from the Archives. Mr. Berger realized during his first review on July 18 that the documents were not ordered chronologically, by subject matter, or in any other way that would enable him to retain information. Specifically, the documents appeared to Mr. Berger as though they had simply been lifted from various National Security Council files, with the result being that they randomly jumped among topics — for example, one document would relate to efforts in Afghanistan in

1999, while the next document might deal more broadly with terrorist financing in Saudi Arabia and Iran in 2000. This presentation of materials made it difficult for Mr. Berger to fill in gaps in his own record of the Administration's actions and, in turn, prepare to testify before the 9/11 Commission.

Unable to piece together the information that he was reviewing in a logical manner, Mr. Berger decided to take his notes on the documents from the Archives. To be clear, Mr. Berger was permitted to take notes on a notepad while reviewing the documents, and he could have submitted the notes that he wanted to take with him for a classification review, with certain of the notes presumably being produced to him at a later date. However, weary from the document review and not thinking clearly, Mr. Berger failed to follow the proper protocols and simply took many of the notes from the notepad for the purpose of later putting their contents into chronological order to assist in his preparation for the 9/11 Commission. Having taken the notes in July without anyone from NARA saying anything to him about it, Mr. Berger likewise took notes with him following his two later visits, on September 2 and October 2, 2003. None of these notes, however, were ever incorporated into any materials outside of NARA, and Mr. Berger voluntarily returned all the notes when contacted by NARA in October 2003, notwithstanding that NARA officials did not ask about the notes at the time.

Mr. Berger has accepted responsibility for all of his actions. He admits that he made a mistake in acting for his own expediency, and then in not initially telling Archives officials what had happened because he was embarrassed by his conduct. He also has repeatedly acknowledged that no extenuating factor — not the public service that he sought to perform in conducting the review, the extraordinary nature of the documents reviews and the stress that he felt while performing them, his voluntary return of all the notes, or the facts that the documents

at issue were copies, the Commission received all the relevant materials, and no one else saw the documents — excuses his lapse in judgment. But the context of Mr. Berger's review does make clear that he had no ill intent and that his actions, while not justifiable, also did not harm anyone. Indeed, at the end of the day, the only damage that Mr. Berger inflicted was to himself. He has accepted those consequences, and looks forward to putting this entire episode behind him so that he can continue his private and public service to his clients, community, and country.

3. *Mr. Berger has cooperated fully with the government.*

Mr. Berger has fulfilled his commitment under the Plea Agreement to cooperate fully and truthfully with the government, and to provide all relevant information known to him. Through counsel, Mr. Berger first advised NARA and, later, the Department of Justice that he wished to cooperate completely with their investigations and was readily available to answer any questions. Prior to entering the Plea Agreement, Mr. Berger provided a complete debriefing to the government, and he voluntarily met with and answered additional questions from the Inspector General of NARA this past July. While such cooperation was mandated under the Plea Agreement, Mr. Berger also views it as his duty to help remedy his actions, and he has and will continue to remain available to answer questions from the Department of Justice or NARA and to assist the Inspector General in any way that he can.

III. Sentencing

The parties agree, and the United States Probation Office concurs, that the appropriate Guideline for the offense at issue is U.S.S.G. § 2X5.1, and because there is no analogous Guideline, the provisions of 18 U.S.C. § 3553(b) shall control Mr. Berger's sentencing. Under the Plea Agreement, the parties also have agreed that the appropriate fine for Mr. Berger's offense is \$10,000, and that Mr. Berger will not apply for or seek a United States government security clearance for a period of three years from the entry of the plea, although the government

can choose to provide such a security clearance to Mr. Berger at any time. The government also does not oppose our request that Mr. Berger receive a non-custodial sentence.

We respectfully submit that these terms are appropriate to serve the interests of justice. As the foregoing factual discussion makes clear, Mr. Berger has served his country with distinction and has been a pillar of his community. His devotion to civic and public work is surpassed only by his loyalty to his friends and his commitment to his family. He is respected in both public and private life as a man of the utmost integrity and highest character. The actions at issue were an anomalous and embarrassing departure from an otherwise impeccable public record. They also were taken during the course of an unusual public service and with the intent of fulfilling a public duty to assist in the inquiry into the greatest tragedy this country has ever known. Nonetheless, Mr. Berger has fully acknowledged his wrongdoing and expressed his sincere regret. He also has cooperated in the government's investigation. There can be no doubt that, should Mr. Berger have occasion to handle classified information again, there will be absolutely no risk of recurrence.

In light of these factors, and given the misdemeanor nature of the offense, we believe that a fine of \$10,000 — in addition to the three-year restriction on Mr. Berger's classified clearance imposed under the Plea Agreement — is an entirely appropriate and sufficient sentence.


IV. Conclusion

For the foregoing reasons, we respectfully request that the Court exercise its discretion to impose a non-custodial sentence that reflects the terms of the Plea Agreement.

Dated: Washington, D.C.
September 2, 2005

Respectfully submitted,

By: _____



Lanny A. Breuer
David N. Fagan

Covington & Burling
1201 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
(202) 662-6000

Attorneys for Samuel R. Berger

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA)	
)	
v.)	Criminal No. 05-0175m-01
)	
SAMUEL R. BERGER,)	Hon. Deborah A. Robinson
)	
Defendant.)	Sentencing: September 8, 2005; 1:30 p.m.

GOVERNMENT'S SENTENCING MEMORANDUM

Defendant Samuel R. Berger pleaded guilty on April 1, 2005, to one count of the unauthorized removal and retention of classified material in violation of 18 U.S.C. §1924. The United States agrees with the conclusion in the Presentence Investigation Report that there is no applicable Sentencing Guideline for this offense, and the provision of 18 U.S.C. § 3553(b) controls. The defendant entered into a plea agreement with the United States, pursuant to which the defendant admitted to the factual basis supporting the conviction and agreed to cooperate with the United States.¹ Pursuant to that agreement, the United States recommends that the defendant's sentence reflect that he has accepted responsibility for his crime and has complied with the terms of the agreement by cooperating with the government. The United States further agreed that an appropriate fine in this matter is \$10,000. The defendant and the United States both acknowledge that the Court is not bound by this agreement and the Court may impose any sentence, up to the maximum sentence permitted by law. As a consultant to the government the

¹ The defendant also agreed not to seek a United States government security clearance or access to classified information for a three year period. At the conclusion of that three year period, the defendant's security clearance will not be reinstated automatically, rather, he may request a clearance and the appropriate United States government authority will make a suitability determination before the defendant can receive such clearance.

defendant assumed an important task to review highly classified documents relating to national security and in the course of that review he breached the trust given to him by unlawfully removing, retaining and destroying classified documents. Based upon the defendant's conduct, the United States respectfully submits that defendant should be sentenced to a term of probation of at least one year, a fine of \$10,000, a term of community service and any other sentence the Court chooses to impose. The United States does not oppose defendant's request for a non-custodial sentence.

Facts

In May 2002 the defendant was asked to, and agreed to, be designated to review presidential records from the Clinton Administration that were stored by the National Archives and Record Administration (Archives). At the time, the defendant possessed, and had possessed for many years, a United States government security clearance and was well aware of the laws and rules regarding the handling and storage of classified information.

in 2003 the defendant visited the Archives in Washington, DC, to review classified documents in connection with a production of records to the National Commission on Terrorist Attacks Upon the United States (the 9-11 Commission). The defendant was reviewing these documents pursuant to the Presidential Records Act, 44 U.S.C. § 2201 et seq., which allows a former president, or his representative, to review presidential records to determine whether the former president will assert any privilege over the records prior to their production. The defendant also took this opportunity to review the documents to prepare himself and other former Clinton administration officials for anticipated testimony before the 9-11 Commission. Prior to his review, the defendant was advised that he could take notes, but that he would have to leave

those notes at the Archives so that a classification review could be done.

On July 18, 2003 the defendant visited the Archives and spent a full day reviewing documents which included copies of documents and original files. After his review, the defendant advised the Archives staff that the lack of organization of the documents impeded his review and asked that in the future, the documents be organized for him to review in chronological order. Finally, after finishing his review that day, the defendant knowingly concealed and removed the notes he had taken during the review, even though he knew he was not permitted to do so.

On September 2, 2003, the defendant returned to the Archives to review additional documents for production to the 9-11 Commission. In this review, the documents were copied and were organized chronologically pursuant to the defendant's previous request. Again, the defendant spent an entire day reviewing documents. In the course of this review he came across a copy of a Top Secret document that he had directed be written when he was the National Security Adviser. The defendant believed that this document would be helpful to him in preparing for his testimony before the 9-11 Commission and expected that the 9-11 Commission would ask him, and others, questions about this document. The document the defendant reviewed was a copy of the document that had been faxed from the Clinton Presidential Library in Little Rock, AK, to the Archives in Washington, DC. The defendant set this document aside, and deciding he did not want to review it at the Archives, concealed the document and removed it from the Archives even though he knew he was not permitted to do so. Additionally, the defendant again knowingly concealed and removed his handwritten notes. The defendant took the document and the notes with him back to his office several blocks away. The defendant took

the document and put in an envelope, sealed the envelope and put it on his desk with the intention to review it at some later time. The defendant knew that his office was not an authorized storage location for classified United States government documents. The envelope and document remained on his desk undisturbed until October 2, 2003.

On October 2, 2003, the defendant again returned to the Archives to review additional documents for production to the 9-11 Commission. The documents the defendant reviewed consisted of copies of emails printed from the database of electronically stored emails from the Clinton Administration stored at the Archives. In the course of this review the defendant came upon print-outs of emails which contained a draft of the Top Secret document the defendant removed in September. One of the print-outs, however, was classified Secret. He set this document aside. Additionally, there were two other email print-outs attaching drafts of the Top Secret document that were classified Top Secret. He set these two documents aside.

Unknown to the defendant, the Archives staff had numbered the documents he was reviewing. As they took the folders from the defendant as he finished his review, they noticed that a document was missing. An Archives staff member approached the defendant, gave him a copy of the missing document and asked him if he had seen the document and advised him that they believed it was missing from the pages he reviewed. The defendant told that staff member that he had reviewed it. The defendant then set this document aside with the other emails.

As the end of the day approached the defendant advised the Archives staff member that he did not think he could finish the review that day. The staff member suggested that the defendant take a quick break and try to finish the remaining documents. The defendant took this opportunity to conceal the four email print-outs he had set aside and removed them from the

Archives. The defendant secreted the emails outside the Archives and returned to finish the review. Upon conclusion of the review the defendant again concealed and removed his handwritten notes.

After the defendant left the Archives he retrieved the secreted emails, which were undisturbed, and took them to his office. At his office, he reviewed the four emails to identify differences among them. After this review, he determined that there were only minor differences and began to cut up the print-outs to dispose of them. However, before he cut up the final email print out he remembered that he had a copy of the final version of the document in the envelope on his desk, and that he had not compared that document for changes. The defendant decided that he would leave one email uncut, throw out the cut up pieces of the others and compare the remaining copies at some later time. He left the print-out in his office and went home.

On October 4, 2003, the Archives staff reviewed their files and determined that documents were indeed missing from the Archives. Archives staff decided to call Bruce Lindsey, President Clinton's designated representative under the Presidential Records Act, and advise him that documents were missing from the Archives after the defendant's review. They asked Mr. Lindsey to call the defendant to determine whether the defendant possessed the missing documents. Mr. Lindsey called the defendant and advised him that documents were missing from the Archives. The defendant told Mr. Lindsey he was not aware of any missing documents and that there must be some mistake; statements he knew to be untrue. Later that day, the defendant contacted an Archives staff member and advised that he did indeed have documents, and that he must have inadvertently removed them, which he also knew to be untrue. Arrangements were made for the defendant to return the documents to Archives staff. On

October 5, 2003, Archives staff retrieved from the defendant the remaining email print-out the defendant removed on October 2nd and the copy of the final version the defendant removed on September 2nd.

Upon review of the returned documents, Archives staff contacted Berger and advised him that documents were still missing. After initially denying any knowledge of additional documents, which the defendant knew was false, the defendant advised Archives staff that he did have additional documents but that he had discarded them in the trash and that upon search of the trash, could not locate them. After the defendant retained counsel, arrangements were made to return the notes that the defendant had removed from the Archives, and on October 10, 2003, the defendant provided his notes to Archives staff.

Sentencing Guidelines

The parties agree that the appropriate Guideline for Unauthorized Removal and Retention of Classified Documents is U.S.S.G. § 2X5.1. The parties further agree that because there is not ~~a sufficiently analogous guideline to the charged offense, the provisions of 18 U.S.C. § 3553(b)~~ shall control" the defendant's sentence. U.S.S.G. § 2X5.1 Section 3553(b) provides that the sentence imposed reflect the seriousness of the offense, promote respect for the law, provide just punishment for the offense, afford adequate deterrence to criminal conduct, protect the public from further crimes of the defendant and provide the defendant with any needed educational or vocational training, medical care or other correctional treatment in the most effective manner. 18 U.S.C. § 3553 (a)(2) (A)-(D).

The defendant's crime in this case was to breach the great trust given to him in his review of highly classified documents and to disregard the laws and rules governing the safeguarding of

those classified documents for his own convenience. The defendant was entitled to review the documents any time he wished to, at the secure location, but he decided that was too burdensome and so he chose to break the law. The defendant also falsely denied his conduct when confronted by Archives staff. The defendant's conduct falls squarely within the ambit of 18 U.S.C. § 1924. The 9-11 Commission received copies of each of the documents the defendant removed in the normal course of the production of documents. There is also no evidence that any unique document was destroyed or lost. The defendant only removed copies of documents which did not contain any handwritten or other notes. The defendant did not share any of the documents with any other person. Ultimately, the defendant accepted responsibility for his actions and fully cooperated with the United States in its investigation of this matter.

Conclusion

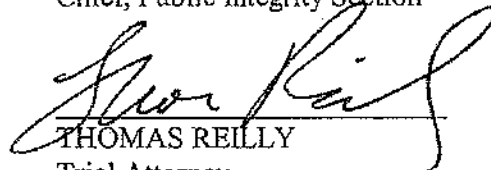
The United States submits that an appropriate sentence in this case would be at least one year of probation, a \$10,000 fine, and a period of community service.

Respectfully submitted,

FOR THE UNITED STATES

JOHN J. DION
Chief, Counterespionage Section

NOEL L. HILLMAN
Chief, Public Integrity Section



THOMAS REILLY
Trial Attorney
U.S. Department of Justice
Criminal Division
Counterespionage Section




DANIEL PETALAS
Trial Attorney
U.S. Department of Justice
Criminal Division
Public Integrity Section

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a copy of the foregoing Government's Sentencing Memorandum was served by fax and first class mail this 6th day of September, 2005 on the following:

Lanny A. Breuer
Covington & Burling
1201 Pennsylvania Avenue N.W.
Washington, DC 20001-2401
202-662-5538
202-662-6291



Thomas Reilly
U.S. Department of Justice

Office Of The Inspector General
National Archives and Records Administration
Evidence Control Form

Custodian Log Number

Case File Number 04-001-6C

Receiving Office and Location: SIG - ARCHIVES II
College Park MD (Secured @ Arch I)

Receiving Special Agent/Official:

(b) (6), (b) (7)(C)

Property Obtained By: SA (b) (6), (b) (7)(C)

Address:
8601 Adelphi Road
College Park, Maryland 20740

Location Obtained (b) (7)(E)

Date Obtained:
10/14/03

Purpose For Which Obtained: EVIDENCE / REQUEST BY Holder of Documents

Item No.	Quantity	Description of Articles (Include Model, Serial #, Identifying Marks, Conditions, and Value)
1	1	MANILA ENVELOPE w/ CONTENTS (b) (7)(E) ARCHIVES II

Chain Of Custody

Item #	Date	Relinquished By	Received By
1	10/14/03	Printed Name (b) (6), (b) (7)(C) Signature (b) (6), (b) (7)(C)	Printed Name (b) (6), (b) (7)(C) Signature SA [redacted]
1	10/14/03	Printed Name (b) (6), (b) (7)(C) Signature (b) (6), (b) (7)(C)	Printed Name (b) (6), (b) (7)(C) Signature (b) (6), (b) (7)(C)

Purpose Of Change Of Custody: TO STORE IN ARCHIVES FACILITY

Chain Of Custody

Item #	Date	Relinquished By	Received By
1	1/28/04	Printed Name (b) (6), (b) (7)(C) Signature (b) (6), (b) (7)(C)	Printed Name (b) (6), (b) (7)(C) Signature (b) (6), (b) (7)(C)
		Printed Name Signature	Printed Name Signature
		Purpose Of Change Of Custody	
		Printed Name Signature	Printed Name Signature
		Printed Name Signature	Printed Name Signature
		Purpose Of Change Of Custody	
		Printed Name Signature	Printed Name Signature
		Printed Name Signature	Printed Name Signature
		Purpose Of Change Of Custody	
		Printed Name Signature	Printed Name Signature
		Printed Name Signature	Printed Name Signature
		Purpose Of Change Of Custody	

9/2 On vacation -> participated in prep for the visit but out of office

10/2 @ my desk or in our vault most of day
 while in vault, got call re 217 -> ~~put~~
 put in same search terms for just the three months surrounding the gap (gap was when) is there anything that should have been incl.?
 this doc should have (no guarantee it was) but ~~pointed out for review in any case~~
~~turned over to colleagues~~ reported findings -
 left for the day - saw in hallway - colleague pointed out to show to NKS

11/3 told to look for 217 - could not find -
 colleagues joined me - still couldn't find
 noticed 323 gone
 looked at time period on computer,
 found Samela doc. that should have been incl.

took files to NKS for her check/review - she confirmed that the #s weren't there, & discovered 150 was not in the run either

checked copies that had been made for Xfer to NSC for S+ below email copy set matched set we had - should not have - our set should have had one more document - not copied b/c being specifically held for review (@ front of folder)

- 5k
 had to go back
 to get the
 documents

Office Of The Inspector General
National Archives and Records Administration
Evidence Control Form

Custodian Log Number

Case File Number 04-001-62

Receiving Office and Location: OIG - Archives II
College Park, MD

Receiving Special Agent/Official:

(b) (6), (b) (7)(C)

Property Secured at Archives I
Property Obtained By: SA (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

Address:
8601 Adelphi Road
College Park, Maryland 20740

Location Obtained

(b) (7)(E)

Date Obtained:

10/10/03

Purpose For Which Obtained: Evidence / Request by Holder of Documents

Item No.	Quantity	Description of Articles (Include Model, Serial #, Identifying Marks, Conditions, and Value)
1	1	Manila Envelope w/ contents (b) (7)(E) Archives I

Chain Of Custody

Item #	Date	Relinquished By:	Received By
1	10/10/03	Printed Name SAMUEL A.K.A. "SANDY" Signature BERGER	Printed Name (b) (6), (b) (7)(C) Signature (b) (6), (b) (7)(C)
	WITNESSED BY	Printed Name SA (b) (6), (b) (7)(C) Signature (b) (6), (b) (7)(C)	Printed Name (b) (6), (b) (7)(C) Signature (b) (6), (b) (7)(C)

Purpose Of Change Of Custody: TO STORE IN ARCHIVES FACILITY

Chain Of Custody
Obtained via FOIA by Custody Watch, Inc.

Item #	Date	Relinquished By	Received By
1	10/14	Printed Name (b) (6), (b) (7)(C)	Printed Name (b) (6), (b) (7)(C)
		Signature [Redacted]	Signature [Redacted]
		Printed Name	Printed Name
		Signature	Signature
Purpose Of Change Of Custody			
<i>for review & photocopy</i>			
1	1/27/04	Printed Name (b) (6), (b) (7)(C)	Printed Name (b) (6), (b) (7)(C)
		Signature (b) (6), (b) (7)(C)	Signature (b) (6), (b) (7)(C)
		Printed Name	Printed Name
		Signature	Signature
Purpose Of Change Of Custody			
		Printed Name	Printed Name
		Signature	Signature
		Printed Name	Printed Name
		Signature	Signature
Purpose Of Change Of Custody			

Obtained via FOIA by Judicial Watch, Inc.

ONE HUNDRED EIGHTH CONGRESS
Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (203) 225-3074
Facsimile (202) 225-3974
MINORITY (203) 225-6021
TTY (202) 225-6352

www.house.gov/gform

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER
TON LANTOS, CALIFORNIA
MAJORA D. DWYER, NEW YORK
EDOLPHUS TOMPA, NEW YORK
PAUL E. KAMBOURIS, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. DUNNING, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN P. TIERNEY, MASSACHUSETTS
W. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH KUPPERICOPEL
MAYMI AND
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
BETTY MCCOLLUM, MINNESOTA

BERNARD SANDERS, VERMONT,
INDEPENDENT

August 5, 2004

The Honorable John W. Carlin
Archivist of the United States
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, DC 20403

Dear Mr. Carlin:

As you know, the Committee is conducting an investigation into recent news accounts that allege the removal of highly classified documents by former National Security Advisor Samuel R. Berger from the National Archives and Records Administration (NARA). According to news reports, although the documents were restricted under both national security laws pertaining to classified documents and the Presidential Records Act, Mr. Berger was granted access to review the documents on behalf of former President Bill Clinton to respond to special access requests made by the National Commission on Terrorist Attacks Upon the United States (9/11 Commission). The unauthorized removal of such documents raises serious questions as to NARA procedures and policies in place to protect such important records and raises specific questions as to whether the 9/11 Commission received all relevant requested documents.

In accordance with our responsibility to review and ensure proper security operations at NARA and pursuant to Rules X and XI of the U.S. House of Representatives, please provide the following information to the Committee by Friday, August 13, 2004:

1. On July 21, 2004, NARA staff supplied Committee staff with the *current* security measures taken to protect classified documents that are reviewed in NARA research rooms. Please also provide all NARA policies and guidance in place prior to March 31, 2004, that addressed access to materials containing classified information in NARA research rooms by non-governmental persons.
2. A copy of the Special Access Request from the White House, sent on behalf of the 9/11 Commission, for which Mr. Berger was conducting an executive privilege review.

Obtained via FOIA by Judicial Watch, Inc.

The Honorable John W. Carlin
August 5, 2004
Page 2

3. A copy of the letter identifying Mr. Berger as an official representative of former President Bill Clinton for the purpose of conducting executive privilege reviews.
4. All written and electronic communications within NARA entities concerning the collection of responsive documents, the consultation process between NARA and the White House in narrowing the identified responsive documents, and the identification of the final set of responsive documents.
5. All written and electronic communications between NARA and the agency of equity, and NARA Inspector General, pertaining to the alleged security breach of classified documents by Mr. Berger.
6. All internal NARA written or electronic communications pertaining to the alleged removal of documents by Mr. Berger.

If you have any questions about this request, please contact Jennifer Safavian, Chief Counsel for Oversight and Investigations, at (202) 225-5074.

Sincerely,



Tom Davis
Chairman

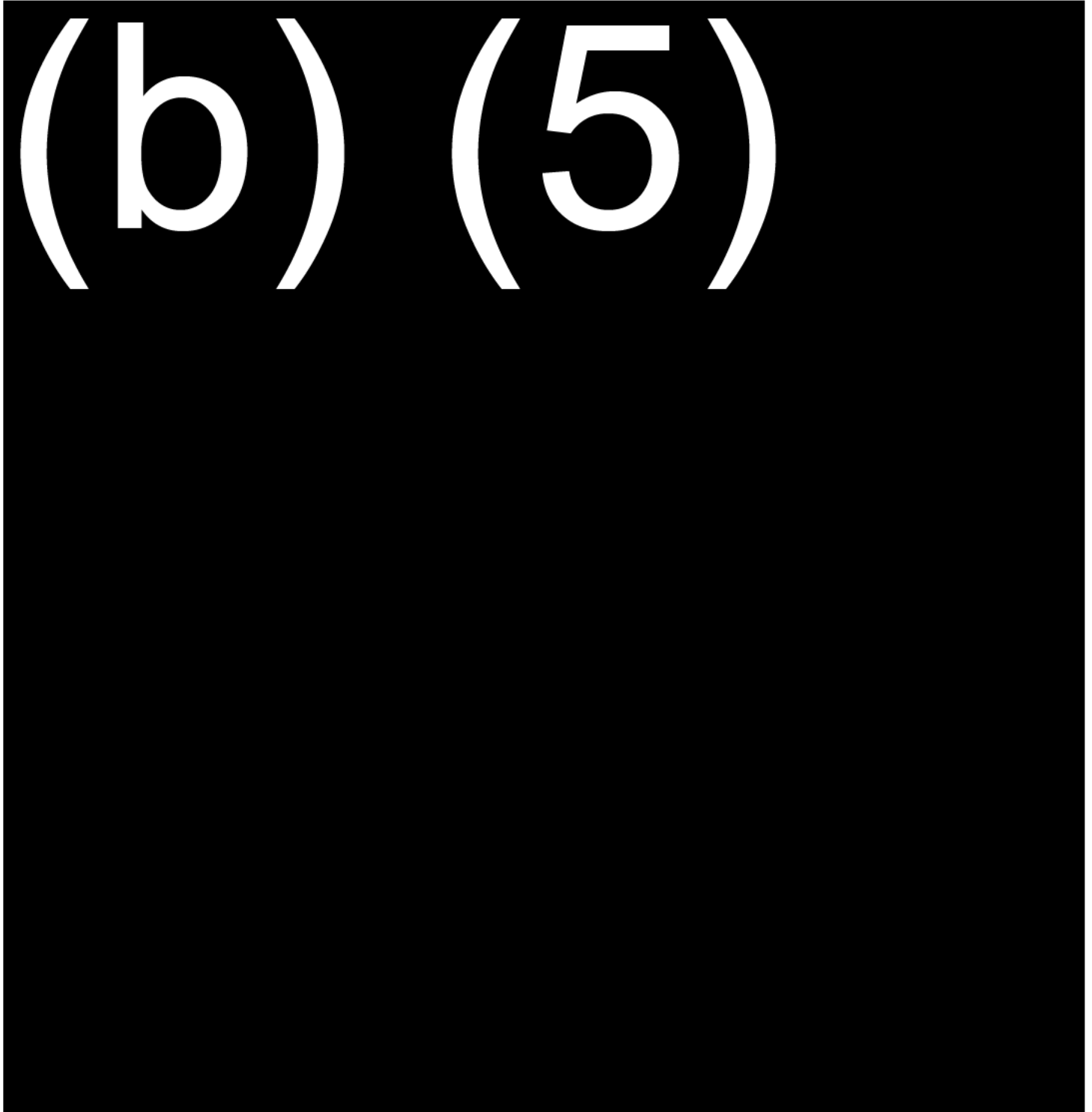
cc: Honorable Henry Waxman, Ranking Member



Obtained via FOIA by Judicial Watch, Inc.
National Archives and Records Administration

*8601 Adelphi Road
College Park, Maryland 20740-6001*

NARA documents potentially responsive to the August 5, 2004, request by Chairman Davis:



(b) (5)



Obtained via FOIA by Judicial Watch, Inc.
National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Documents potentially responsive to the August 5, 2004, request by Chairman Davis.

(b) (5)

(b) (5)

Obtained via FOIA by Judicial Watch, Inc.

TOL DAVID, VIRGINIA
CHAZWALK
DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LENTINI, FLORIDA
JOHN M. MURPHY, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LATTIQUETTE, OHIO
GORD OSE, CALIFORNIA
HOWARD COOPER, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATT, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM W. PUTNAM, FLORIDA
EDWARD W. ZEBROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
MATTHEW GEAL, GEORGIA
DANIEL HILL, MISSISSIPPI
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
MARGARET CLACKSON, TENNESSEE
PATRICK J. TICHEN, OHIO
KATHERINE HARRIS, FLORIDA

ONE HUNDRED EIGHTH CONGRESS
Congress of the United States
House of Representatives

COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

MAILROOM (202) 225-4678
FACSIMILE (202) 225-1974
RECORDS (202) 225-5251
TTY (202) 225-1822

www.house.gov/rtf/jam

HENRY A. WADSWORTH, CALIFORNIA
BANKING AND FINANCIAL SERVICES
TOM LAMTOS, CALIFORNIA
MAX BAER, NEW YORK
EDDIE BROWN, CALIFORNIA
PAUL E. HASTINGS, CALIFORNIA
CHRISTOPHER H. SMITH, NEW YORK
BLAKE FLYNN, MARYLAND
DANNY K. DAVIS, ILLINOIS
JOHN F. TUNNEY, MASSACHUSETTS
W. LARRY CLAY, MISSOURI
DANIEL E. WATSON, CALIFORNIA
STEPHEN F. LYNN, MASSACHUSETTS
CHRIS VAN HOLEN, MARYLAND
LINDA T. BIRCHBAUM, CALIFORNIA
C.A. DUTCH BOURKE, CALIFORNIA
MARYLAND
FRANK HOLMES, NEWTON
DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
BETTY MCCOLLUM, MINNESOTA
EDWARD SANDERS, VERMONT
INDEPENDENT

FACSIMILE TRANSMISSION

Date: 8/30/04

To: Gary Stein

From: Jennifer Safavian

Phone: (301) 837-3026

Fax: (301) 837-0293

There will be a total of 3 pages, including cover page.

Comments: _____

*If there are any questions or problems regarding this transmission,
please call the sender at 202-225-5074*

Please Note: The information on this facsimile is confidential and is intended only for the use of the person named above. If this facsimile has come to you in error, please call the sender at the number given above. Any distribution of this facsimile is strictly prohibited.

TOM DAVIS, VIRGINIA, CHAIRMAN
GAIL BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. BOEHNER, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
DOLG OSC, CALIFORNIA
RON LUIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL BLATTZ, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM K. RUTY, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DINGENY, JR., TENNESSEE
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN B. CARTER, TEXAS
MARSHA BLACKBURN, TENNESSEE
PATRICK J. TIBERI, OHIO
KATHERINE HARRIS, FLORIDA

ONE HUNDRED EIGHTH CONGRESS
Congress of the United States
House of Representatives

COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

MAJORITY (203) 225-6374
FACSIMILE (202) 225-4274
MINORITY (202) 225-8351
TTY (202) 225-4852
www.house.gov/taform

HENRY A. WAXMAN, CALIFORNIA, RANKING MEMBER
TOM LANTOS, CALIFORNIA
MAJORITY
EDDOLPHUS TOMAS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CLUMMINES, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WILL LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH BUMPERS, ARIZONA
MARYLAND
ELEANOR HOLMES NORTON, DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
BETTY MCCOLLUM, MINNESOTA
SHIRAZO BANERJEE, VERMONT, INDEPENDENT

August 30, 2004

The Honorable John W. Carlin
Archivist of the United States
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, D.C. 20403

Dear Mr. Carlin:

We are in receipt of the National Archives and Records Administration's (NARA) August 13, 2004 letter and partial response to our document request of August 5, 2004. The letter sets forth that NARA sought guidance from the Department of Justice (DOJ) in responding to our request. DOJ advised NARA to defer production of any documents responsive to requests 5 and 6, as well as any documents responsive to request 4 created after October 2, 2003, because production of these documents, according to an August 12, 2004 letter from DOJ to NARA, "could adversely impact the pending investigation." In accordance with DOJ's request, you did not produce any responsive documents to requests 5 and 6, while producing documents responsive to request 4, including a document dated October 7, 2003, per DOJ's authorization. While we have asked DOJ how production of these documents could harm the investigation, we have not received an adequate explanation of their concerns.

To be clear, we do not seek any documents that refer, discuss, or reflect any action taken by DOJ. We do not seek any documents created after the initiation of DOJ's criminal investigation, which, according to DOJ's letter, appears to be October 2, 2003. Therefore, we cannot understand how production of the documents we have requested could harm the criminal investigation.

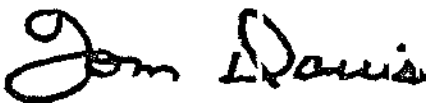
We strongly believe that it is our responsibility to examine how such highly classified documents could be removed from NARA, and whether there is a need for Congress to take legislative action to ensure the security of such documents at NARA. Accordingly, please provide all responsive documents to requests 4, 5, and 6, to the Committee by Tuesday, September 7, 2004. As an alternative to producing the

The Honorable John W. Carlin
August 30, 2004
Page 2

documents, Committee staff could review them at a NARA facility and take notes of their contents, if this would be preferable to DOJ. Please let us know if this arrangement would be satisfactory by Friday, September 3, 2004.

If you have any questions regarding the above, please contact Jennifer Safavian, Chief Counsel for Oversight and Investigations, at (202) 225-5074.

Sincerely,



Tom Davis
Chairman

cc: Honorable Henry Waxman, Ranking Member

From: (b) (6)
To: (b) (6)
Date: Tue, Oct 14, 2003 2:02 PM
Subject: Flow Chart

Nancy,

Here is a flow chart that (b) (6) and I put together. Please let me know if it is not what you want or you need additional information.

(b) (6)

**Mr. Berger's Visit to review his records in preparation for Congressional Testimony
- May 2002**

NLMS-held numbered documents (originals) that met the terms of his permission letter

Folders of material from NLMS-held files (originals) that met the terms of his permission letter

EOP 2 - July 2003

NLMS-held numbered documents deemed responsive to by NARA (originals)

Folders of material from NLMS-held files in which potentially responsive documents had been tabbed (originals)

EOP 3 - 1st Visit, September 2

Mr. Berger was shown Xerox copies of all materials except the responsive numbered documents from NLMS. The materials were arranged in one box in the following order:

- folder of 8 items NSC deemed responsive to EOP 2 from NLMS holdings - just incase you or Mr. Berger would like to review
- folder with 1 Clinton SCI item NR from EOP 2 but responsive to EOP 3
- folder with 1 Clinton Top Secret item NR from EOP 2 but responsive to EOP 3
- folder with NLMS - Staff Member Office Files responsive to EOP 3 - these are copies, Kate has written your note on each cover sheet - to assist Mr. Berger, these are arranged in chron order
- folder with NLMS - Numbered Documents - these are **originals** - your tabs are still on them with your notes - to assist Mr. Berger, these are arranged in document number order
- folder of NLCP Secret and below textual documents - to assist Mr. Berger, these are arranged in chron order
- folder of NLCP TC-SCI textual documents - to assist Mr. Berger, these are arranged in chron order
- folder of NSC email responsive to para 2 - 1998-2001
- folder of NSC email responsive to para 3 - 1998
- folder of NSC email responsive to para 3 - 1999

- folder of NSC email responsive to para 3 - 2000-2001

Mr. Berger completed the review of all the textual records and the 1st part of the folder entitled "NSC email responsive to Para 2 - 1998-2001"

EOP 3 - Visit by Mr. Naplan - September ? (I think his notes say September 4-8, which includes a weekend, and so would be parts of three days reviewing. Does that sound right to you?)

Mr. Naplan was provided with the Secret and Below emails segregated from the following folders:

- folder of NSC email responsive to para 2 - 1998-2001

- folder of NSC email responsive to para 3 - 1998

- folder of NSC email responsive to para 3 - 1999

- folder of NSC email responsive to para 3 - 2000-2001

These were all emails and therefore not original records.

Mr. Naplan took detailed notes and left those for Mr. Berger to review on his next visit.

EOP 3 - 2nd Visit by Mr. Berger October 2nd

Mr. Berger was provided with the following materials:

- The Secret and Below materials provided to Mr. Naplan and Mr. Naplan's Notes.
- The Top Secret email responsive to Para 2 and 3
- Copies of NLCP and NLMS textual records which NARA deemed responsive to EOP3 out of materials that NARA had previously deemed responsive to EOP 2 and provided to NSC/WH but which NSC/WH in turn deemed non-responsive

From: (b) (6)
To: (b) (6)
Date: Wed, Oct 15, 2003 4:33 PM
Subject: TerrorF1.doc

How is this?

<p>May 2002</p> <p>Mr. Berger's Visit to review his records in preparation for Congressional Testimony –</p>	<p>Originals - NLMS-held numbered documents that met the terms of his permission letter</p> <p>Originals - Folders of material from NLMS-held files that met the terms of his permission letter</p>
<p>EOP 2 – July 2003</p> <p>Mr. Berger</p>	<p>Originals - NLMS-held numbered documents deemed responsive to by NARA</p> <p>Originals - Folders of material from NLMS-held files in which potentially responsive documents had been tabbed</p>
<p>EOP 2 – July 2003</p> <p>Nancy Soderberg</p>	<p>Copies of TS records from Little Rock</p>
<p>EOP 3 – 1st Visit, September 2</p> <p>Mr. Berger</p>	<p>Originals - NLMS Numbered Documents</p> <p>Copies of SMOFS from NLMS, and NLCP</p> <p>Copies of Memcon's from NLCP</p> <p>Copies of Email</p> <p>***(For additional information please see below)</p>
<p>EOP 3 – September</p> <p>Mr. Naplan</p>	<p>Copies of Email at the Secret Level and Below</p>
<p>EOP 3 – 2nd Visit October 2nd</p> <p>Mr. Berger</p>	<p>These copies were all numbered sequentially:</p> <p>The Secret and Below materials provided to Mr. Naplan and Mr. Naplan's Notes.</p> <p>The Top Secret email responsive to Para 2 and 3</p> <p>Copies of NLCP and NLMS textual records which NARA deemed responsive to EOP3 out of materials that NARA had previously deemed responsive to EOP 2 and provided to NSC/WH but which NSC/WH in turn deemed non-responsive</p>

*** EOP 3 – 1st Visit, September 2

Mr. Berger was shown Xerox copies of all materials except the responsive numbered documents from NLMS. The materials were arranged in one box in the following order:

- folder of 8 items NSC deemed responsive to EOP 2 from NLMS holdings - just incase you or Mr. Berger would like to review
- folder with 1 Clinton SCI item NR from EOP 2 but responsive to EOP 3
- folder with 1 Clinton Top Secret item NR from EOP 2 but responsive to EOP 3
- folder with NLMS - Staff Member Office Files responsive to EOP 3 - these are copies, Kate has written your note on each cover sheet - to assist Mr. Berger, these are arranged in chron order
- folder with NLMS - Numbered Documents - these are **originals** - your tabs are still on them with your notes - to assist Mr. Berger, these are arranged in document number order
- folder of NLCP Secret and below textual documents - to assist Mr. Berger, these are arranged in chron order
- folder of NLCP TC-SCI textual documents - to assist Mr. Berger, these are arranged in chron order
- folder of NSC email responsive to para 2 - 1998-2001
- folder of NSC email responsive to para 3 - 1998
- folder of NSC email responsive to para 3 - 1999
- folder of NSC email responsive to para 3 - 2000-2001

Mr. Berger completed the review of all the textual records and the 1st part of the folder entitled "NSC email responsive to Para 2 -- 1998-2001"

From: (b) (6)
To: (b) (6)
Date: 7/23/04 9:26AM
Subject: Re: Gary's email

(b) (5), (b) (6)

>>>(b) (6) 07/23/04 09:20AM >>>

(b) (5)

My two cents.

K.

From: GaryM Stern
To: Constance, John; Fawcett, Sharon; Smith, Nancy
Date: 7/23/04 8:51AM
Subject: Re: 'Procedures for Special Access for Designated Representatives of Former President under the PRA

(b) (6), (b) (5)

>>> Nancy Smith 7/22/04 5:31:43 PM >>>
Gary, Sharon and John:

(b) (5)

Thank you,

(b) (6)

cc:

(b) (6)

From:

(b) (6)

To:

Date:

7/23/04 9:20AM

Subject:

Gary's email

(b) (5)

My two cents.

K.

cc:

(b) (6)

From: (b) (6)
To: Constance, John; Fawcett, Sharon; Stern, GaryM
Date: 7/23/04 10:00AM
Subject: Re: 'Procedures for Special Access for Designated Representatives of Former President under the PRA

Gary and John:

(b) (5)

(b) (5) The former President or his designated representative have a legal right to review for privilege records being requested. They can also have copies of this material if it is not classified and if classified they could if they asked as long as they have a classified storage facility. A designated representative is the same as the former President looking at his records.

There are no set procedures for how we have treated the former President's at their Libraries. For example, Lyndon Johnson got originals all the time when he was writing Vantage Point in his office or wherever he wanted them and he certainly was not being watched.

I think again the procedures we have described follow what has been in place since 1989.

(b) (6)

cc:

(b) (6)



National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

August 13, 2004

Ms. Jennifer Safavian
Chief Investigative Counsel
Committee on Government Reform
House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515-6143

Dear Ms. Safavian:

This letter is in response to the August 5, 2004, letter from Chairman Davis to John Carlin, Archivist of the United States, requesting documents. As you are aware, in responding to this request, we sought guidance from the Department of Justice.

Attached is a letter to the Archivist dated August 12, 2004, from Bruce Swartz, Deputy Assistant Attorney General for the Criminal Division. Mr. Swartz's letter advises NARA to defer production of any documents responsive to items 5 and 6 of Chairman Davis's letter, as well as any documents responsive to item 4 created after October 2, 2003, because of the ongoing criminal investigation into this matter. In addition, Mr. Swartz's letter requests that interviews with NARA employees be deferred. Accordingly, enclosed with this letter are documents that are responsive to items 1, 2, 3, and 4 of Chairman Davis's request, as limited by Mr. Swartz's letter. As noted in his letter, please contact the DOJ Office of Legislative Affairs if you have any questions about this guidance.

As we have also discussed, NARA greatly appreciates your sensitivity to and respect for the privacy of NARA employees who are involved in this matter. To that end, we have redacted all such names and identifiers from these documents.

As we have already explained with respect to document request number 1, NARA did not have specific written procedures for special access privilege reviews of classified information under the Presidential Records Act. Such access is governed by the PRA itself, the implementing regulations, and the standard practices for accessing and handling classified information, including NARA's Information Security Manual. In response to this request, we have included the relevant portions of these authorities, as well as a description of the process that was recently prepared by NARA staff.

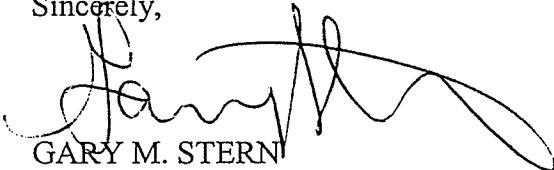
With respect to document request number 2, we have enclosed the two requests that the White House received from the 9/11 Commission for relevant Presidential records, including Clinton Presidential records that are held by NARA. Mr. Berger was involved in conducting the privilege review on behalf of former President Clinton for both of these requests. One of these 9/11 Commission requests contains classified information, which has been redacted.

With respect to document request number 3, attached is a letter of April 12, 2002, from former President Clinton establishing Mr. Berger as his representative for reviewing NSC records. NARA relied on this designation for the subsequent special access review conducted by Mr. Berger in 2003.

In our phone conversation of August 12, 2004, concerning document request number 4, you indicated that this request essentially seeks information on what was produced by NARA to the White House in response to the two requests (responsive to item 2, above), such as cover letters that accompanied the documents and/or any inventories or logs describing the documents. Based on our conversation, enclosed are the cover letters that accompanied the documents that were responsive to the two 9/11 Commission requests; because NARA kept a complete copy set of what was produced, we did not create an inventory or description of the documents themselves. Please note that even though Mr. Swartz's letter limits our production to documents created on or before October 2, 2003, DOJ has authorized us to include in this production the final cover letter, dated October 7, 2003.

Please let me know if you have any questions.

Sincerely,



GARY M. STERN
General Counsel

Cc: David Rapallo, Minority Counsel

Enc.

AUG-12-2004 15:23

DOJ/CRIMINAL DIV/ISS
Obtained via FOIA by Judicial Watch, Inc.

202 514 2836

P.02



U.S. Department of Justice

Criminal Division

*Office of the Deputy Assistant Attorney General**Washington, D.C. 20530*

AUG 12 2004

The Honorable John W. Carlin
Archivist of the United States
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, DC 20408

Dear Mr. Carlin:

This responds to your request for guidance regarding your response to the letter, dated August 5, 2004, from Chairman Davis of the House Government Reform Committee, which requested documents from the Archives related to Mr. Samuel R. Berger's review of documents at the Archives. As you are aware, there is currently an ongoing criminal investigation regarding this matter and we are concerned that the production of some of the requested documents, as well as congressional interviews of certain Archives employees, at this time could compromise the investigation.

In light of these concerns, we request that the Archives defer production of any documents responsive to items 5 and 6 of Chairman Davis's letter because their disclosure at this time could adversely impact the pending investigation. We also request that your production of documents responsive to item 4 of the letter be limited to documents that were created on or before October 2, 2003. Documents that were created after that date may relate to the ongoing investigation and should not be produced. We do not have any objection to the production of documents responsive to the other portions of Chairman Davis's letter.

Additionally, we request that the Archives defer any requests by the Committee staff to interview Archives employees Nancy Smith, Kathleen Dillon McLure, Billy John Laster, and Elizabeth Fidler because they are central to our ongoing investigation and congressional interviews of them at this time could adversely impact our law enforcement efforts.

We make these requests with due respect for the Committee's interests in this matter based upon our substantial concern that the provision of the above described documents and interview witnesses would complicate and/or compromise our criminal investigation. We

understand that you may wish to share this letter with the Committee and we are available to confer through our Office of Legislative Affairs with Committee staff if there are further questions about our views. Please do not hesitate to contact me if you would like additional assistance regarding this matter.

Sincerely,



Bruce C. Swartz
Deputy Assistant Attorney General

AUG-12-2004 15:23

DOJ/CRIMINAL DIV/ISS

202 514 2836

P.22

Obtained via FOIA by Judicial Watch, Inc.

U.S. Department of Justice



Criminal Division

Office of the Deputy Assistant Attorney General

Washington, D.C. 20530

AUG 12 2004

The Honorable John W. Carlin
Archivist of the United States
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, DC 20408

Dear Mr. Carlin:

This responds to your request for guidance regarding your response to the letter, dated August 5, 2004, from Chairman Davis of the House Government Reform Committee, which requested documents from the Archives related to Mr. Samuel R. Berger's review of documents at the Archives. As you are aware, there is currently an ongoing criminal investigation regarding this matter and we are concerned that the production of some of the requested documents, as well as congressional interviews of certain Archives employees, at this time could compromise the investigation.

In light of these concerns, we request that the Archives defer production of any documents responsive to items 5 and 6 of Chairman Davis's letter because their disclosure at this time could adversely impact the pending investigation. We also request that your production of documents responsive to item 4 of the letter be limited to documents that were created on or before October 2, 2003. Documents that were created after that date may relate to the ongoing investigation and should not be produced. We do not have any objection to the production of documents responsive to the other portions of Chairman Davis's letter.

Additionally, we request that the Archives defer any requests by the Committee staff to interview Archives employees [redacted] because they are central to our ongoing investigation and congressional interviews of them at this time could adversely impact our law enforcement efforts.

We make these requests with due respect for the Committee's interests in this matter based upon our substantial concern that the provision of the above described documents and interview witnesses would complicate and/or compromise our criminal investigation. We

understand that you may wish to share this letter with the Committee and we are available to confer through our Office of Legislative Affairs with Committee staff if there are further questions about our views. Please do not hesitate to contact me if you would like additional assistance regarding this matter.

Sincerely,



Bruce C. Swartz
Deputy Assistant Attorney General

Responsive to Paragraph #1

Former President's Privilege Review of Classified Presidential Records in the Custody of the Archivist of the United States

As there was no single directive for this type of access, the procedures followed in allowing a former President and/or his designated legal representative to conduct a privilege review of classified records were drawn from the statutory authority of the Presidential Records Act, 44 U.S.C. §§ 2201-2207, and NARA's required operating framework governing the access to and handling of classified information.

Procedures

1) NARA receives a request under 44 U.S.C. § 2205(2) for access to records that are not otherwise available to the public. Presidential records shall be made available in response to one of the following: a subpoena or other judicial process issued by a court of competent jurisdiction, a request by the incumbent President for on-going government business, or a request from either House of Congress or from a committee or subcommittee if such records are needed for the conduct of Congressional business.

2) If NARA locates documents responsive to the special access request, NARA will provide a notification of that fact to the former President and/or his designated legal representative. The PRA and E.O. 13233 allows for the review of those records for privilege concerns. The former President must designate in writing to NARA any individual he wants to conduct such a privilege review on his behalf. Further, 44 U.S.C. § 2205(3) states that "the Presidential records of a former President shall be available to such former President or his designated representative."

3) The PRA and NARA's implementing regulations at 36 C.F.R. § 1270.44(c) are the only authorities governing a privilege review by the former President and/or his designated representative. However, if the responsive Presidential records contain classified information, any privilege review must occur in accordance with Executive Order 12958, as amended, and NARA's Information Security Manual 202. This manual has no specific procedures for granting a former President and/or his designated representative access to classified information for a privilege review. However, NARA followed those procedures that were most appropriate, specifically those that apply to access for research by former Presidential appointees, historical researchers and safekeeping and storage of classified information. These are outlined below.

NARA Information Security Manual 202

Chapter 2, Part 1 – Access

4. Former Presidential Appointees.

Access is permitted when:

- a. The person has a current security clearance at the appropriate level and completes an SF 312, Classified Information Nondisclosure Agreement.
- c. The person seeking access agrees to:
 - (1) Safeguard the information (Accomplished by the SF 312);

- (2) Authorized review of his or her notes to make sure that they do not contain classified information; and
- (3) Make sure that the classified information to which he or she received access is not further disseminated or published.

5. Historical Researchers and Contract Historians.

- b. Verification in writing of the accessing individual's security clearance.
 - (2) The written verification must be provided by an official, other than the visitor, who is in a position to verify the visitor's security clearances
- c. Verification (orally or in writing), that the contractor/researcher has completed and filed with the contracting or authorizing agency a classified information nondisclosure agreement.

Chapter 4, Part 1 – Safekeeping and Storage

7. Custodial Precautions

- b. Care during working hours. Each person must take precautions to prevent access to classified information by unauthorized persons. The following precautions are to be observed:
 - (4) When classified information is to be made available to research, properly cleared employees move the material to a research room, supervise its use, return it to storage, and make sure that unauthorized persons do not have access to it. Notes taken from classified information in records or documents by researchers are to be safeguarded the same as the classified documents.

44 USC

§ 2205. Exceptions to restricted access

Notwithstanding any restrictions on access imposed pursuant to section 2204--

(1) the Archivist and persons employed by the National Archives and Records Administration who are engaged in the performance of normal archival work shall be permitted access to Presidential records in the custody of the Archivist;

(2) subject to any rights, defenses, or privileges which the United States or any agency or person may invoke, Presidential records shall be made available--

(A) pursuant to subpoena or other judicial process issued by a court of competent jurisdiction for the purposes of any civil or criminal investigation or proceeding;

(B) to an incumbent President if such records contain information that is needed for the conduct of current business of his office and that is not otherwise available; and

(C) to either House of Congress, or, to the extent of matter within its jurisdiction, to any committee or subcommittee thereof if such records contain information that is needed for the conduct of its business and that is not otherwise available; and

(3) the Presidential records of a former President shall be available to such former President or his designated representative.

§ 2206. Regulations

The Archivist shall promulgate in accordance with section 553 of title 5, United States Code, regulations necessary to carry out the provisions of this chapter. Such regulations shall include--

(1) provisions for advance public notice and description of any Presidential records scheduled for disposal pursuant to section 2203(f)(3);

(2) provisions for providing notice to the former President when materials to which access would otherwise be restricted pursuant to section 2204(a) are to be made available in accordance with section 2205(2);

(3) provisions for notice by the Archivist to the former President when the disclosure of particular documents may adversely affect any rights and privileges which the former President may have; and

(4) provisions for establishing procedures for consultation between the Archivist and appropriate Federal agencies regarding materials which may be subject to section 552(b)(7) of title 5, United States Code.

§ 1270.44

36 CFR Ch. XII (7-1-03 Edition)

Nati

§ 1270.44 Exceptions to restricted access.

(a) Notwithstanding any restrictions on access imposed pursuant to section 2204 or these regulations, and subject to any rights, defenses, or privileges which the United States or any agency or person may invoke, Presidential records shall be made available in the following instances:

(1) Pursuant to subpoena or other judicial process properly issued by a court of competent jurisdiction for the purposes of any civil or criminal investigation or proceeding;

(2) To an incumbent President if the records sought contain information which is needed for the conduct of current business of his office and is not otherwise available;

(3) To either House of Congress, or, to the extent of matter within its jurisdiction, to a Congressional committee or subcommittee if the records sought contain information which is needed for the conduct of business within its jurisdiction and is not otherwise available.

(b) Requests by an incumbent President, a House of Congress, or a Congressional committee or subcommittee pursuant to paragraph (a) of this section shall be addressed to the Archivist. All requests shall be in writing and, where practicable, identify the records sought with reasonable specificity.

(c) Presidential records of a former President shall be available to the former President or his designated representative upon request.

§ 1270.46 Notice of intent to disclose Presidential records.

(a) The Archivist or his designee shall notify a former President or his designated representative(s) before any Presidential records of his Administration are disclosed.

(b) The notice given by the Archivist or his designee shall:

(i) Be in writing;

(ii) Identify the particular records with reasonable specificity;

(iii) State the reason for the disclosure; and

(iv) Specify the date on which the record will be disclosed.

(2) In the case of records to be disclosed in accordance with § 1270.44, the notice shall also:

(i) Identify the requester and the nature of the request;

(ii) Specify whether the requested records contain materials to which access would otherwise be restricted pursuant to 44 U.S.C. 2204(a) and identify the category of restriction within which the record to be disclosed falls; and

(iii) Specify the date of the request.

(c) If, after receiving the notice required by paragraph (a) of this section, a former President raises rights or privileges which he believes should preclude the disclosure of a Presidential record, and the Archivist nevertheless determines that the record in question should be disclosed, in whole or in part, the Archivist shall notify the former President or his representative of this determination. The notice given by the Archivist or his designee shall:

(1) Be in writing;

(2) State the basis upon which the determination to disclose the record is made; and

(3) Specify the date on which the record will be disclosed.

(d) The Archivist shall not disclose any records covered by any notice required by paragraph (a) or (c) of this section for at least 30 calendar days from receipt of the notice by the former President, unless a shorter time period is required by a demand for Presidential records under § 1270.44.

(e) Copies of all notices provided to former Presidents under this section shall be provided at the same time to the incumbent President.

Subpart E—Presidential Records Compiled for Law Enforcement Purposes

§ 1270.50 Consultation with law enforcement agencies.

(a) For the processing of Presidential records compiled for law enforcement purposes that may be subject to 5 U.S.C. 552(b)(7), the Archivist shall request specific guidance from the appropriate Federal agency on the proper treatment of a record if there is no general guidance applicable. If the record is particularly sensitive, or if

the
wid-
the
req-
sect
app-
sion
doc-
foll-
(1
que-
(2
scri



National Archives and Records Administration
Washington, D.C.

January 13, 1989

INFO. SECURITY 202, CHGE 5

Committee that originated classified information, or that transferred its own records containing classified information, may be granted access upon verification in writing of the accessing individual's security clearance and need to know by an authorized agency or Congressional Committee official. Requests should be addressed to the Presidential library director, Federal records center director, or NN division director or branch chief concerned. The written verification must be submitted by an official, other than the visitor, who is in a position to verify the visitor's security clearance. Visit requests normally should include the employee's name, birth date or social security number, position, level of clearance, employing activity of the visitor, date and duration of the proposed visit, purpose of the visit in sufficient detail to establish the need to know, and a description of the records for which access is authorized. Visit requests may remain valid for up to one year. Visitors must present proof of identity before access is granted.

3. Officials of nonoriginating agencies. Access by officials of one executive branch agency to classified records originated by or transferred to NARA by another agency is permitted only under the Interagency Agreement on Access for Official Agency Historians (see app. 2A) or when the proper NARA official receives written authorization from the originating or transferring agency. Any restrictions imposed by access agreements or authorization letters must be strictly enforced. Waivers of access authorization procedures must be approved by the assistant information security manager of the office that has custody of the records. Written verification of clearance requirements are the same as for officials of originating or transferring agencies.

4. Former Presidential appointees. Persons who occupied policymaking positions to which they were appointed by the President may be authorized access to classified information or material that they originated, reviewed, signed, or received while serving as a Presidential appointee. Access is limited to information under the classification jurisdiction of the agency or agencies from which the written decisions required in b, below, are received. Access is permitted when:

a. The person has a current security clearance at the appropriate level and completes an SF 312, Classified Information Nondisclosure Agreement.

b. A written decision is made by an official of the agency or agencies which employed the former Presidential appointee that the access is consistent with the interests of national security.

January 13, 1989

INFO. SECURITY 202, CHGE 5

c. The person seeking access agrees to:

(1) Safeguard the information (accomplished by signing the SF 312);

(2) Authorize a review of his or her notes to make sure they do not contain classified information; and

(3) Make sure that the classified information to which he or she receives access is not further disseminated or published.

5. Historical researchers and contract historians. Persons outside the Federal Government who are engaged in historical research and persons acting as contractors to executive branch agencies may be granted access to classified information in NARA when they fulfill certain requirements. These are:

a. Authorization from the agency with classification jurisdiction.

(1) Receipt by the custodial unit of a written statement of the person's need to know. Normally this will take the form of a letter or memorandum outlining the topic of research and the records or documentary material to which access is being sought in order to perform the historical research or the contract.

(2) The statement will normally be prepared by the agency's historian or contracting officer in a separate letter or memorandum. But it may also be part of the visit authorization form of that agency along with a statement of the researcher's clearance signed by the agency's security officer.

b. Verification in writing of the accessing individual's security clearance.

(1) A statement (usually on a visit authorization form) by an authorized agency official addressed to the Presidential library director, Federal records center director, or NN division director or branch chief concerned.

(2) The written verification must be provided by an official, other than the visitor, who is in a position to verify the visitor's security clearance.

(3) Visit requests normally should include the historical researcher's or contractor's name, birth date or social security number, level of clearance, basis for clearance (i.e., authority granting clearance and date thereof), and name of the employing contractor when relevant,

January 13, 1989

INFO. SECURITY 202, CHGE 5

and other information such as date and duration of visit and description of the records.

c. Verification (orally or in writing) that the contractor/researcher has completed and filed with the contracting or authorizing agency a classified information nondisclosure agreement.

d. NARA custodians will be responsible for enforcing any additional limits or requirements imposed by the authorizing letters.

e. No contractor/researcher will be permitted to remove notes made from classified material or reproductions of classified material from a NARA facility. All notes made from classified material and classified reproductions will be transmitted to the responsible classifying agency, if requested, or directly to the sponsoring government agency for further handling. The accompanying letter should identify the researcher, the name of the contractor (and the contract project number, if relevant), and information about the request and the records involved. Pay particular attention to any special access restrictions which may apply to any of the reproductions.

f. The records or donated historical material to be consulted must be screened and material which the contractor is not authorized to examine must be withdrawn. This may involve withdrawal of special access restricted records (SCI, RD, FRD, CNWDI, NATO); Top Secret items (if clearance is only through the Secret level); documents containing classified information originating in another agency; and otherwise restricted material.

g. Government contractors and other historical researchers are not "official agency historians". Consequently, they are not covered by the interagency agreement. Each agency which originated classified information found in a file requested by a cleared contractor must specifically authorize access to its information. This written authorization should identify that contract employee by name and direct NARA to make the classified information accessible or that agency's classified information must be withdrawn.

6. Access during judicial proceedings. Classified information will not normally be released in the course of any judicial proceeding. Under certain circumstances, however, the introduction of classified information into evidence may be necessary to ensure the administration of justice.

January 13, 1989

INFO. SECURITY 202, CHGE 5

strip cards) do not provide enough protection and may not be substituted for the locks prescribed in par. 2. Cipher and electrically activated locks may be used to admit authorized persons to an occupied area, provided:

(1) The lock is properly installed and screened to prevent unauthorized viewing (screened, recessed, or opaque cover over buttons);

(2) The combination is changed by an authorized person at least once every three months, or when persons who know the combination are separated from the agency; and

(3) The combination is classified as high as or higher than the highest classification of material processed or stored within the area.

d. Repair of damaged security containers. Forcing open locked containers or repairing damage that affects the integrity of a security container approved for storing classified information may be done only by authorized persons who are cleared or who are continuously escorted.

7. Custodial precautions.

a. Responsibilities of custodians.

(1) Custodians are responsible for protecting and accounting for classified information at all times and particularly for locking classified information in security equipment when it is not in use or under the direct supervision of authorized persons. They must follow procedures to prevent unauthorized persons from gaining access to classified information by sight or sound or other means and see that classified information is not left with or left open in the presence of unauthorized persons. Standard Form 701, Activity Security Checklist, must be used by responsible officials to ensure that essential safeguarding steps are taken.

(2) Classified information must not be removed from office or work areas for use during off-duty hours or for other reasons of personal convenience.

b. Care during working hours. Each person must take precautions to prevent access to classified information by unauthorized persons. The following precautions are to be observed:

(1) Classified information in records or documents removed from storage for working purposes must be kept under constant watch and kept face down or covered when not in use.

January 13, 1989

INFO. SECURITY 202, CHGE 5

Records or documents which contain classified information must be covered by the cover sheet for the level of classification applicable to the information contained in the record or document. Standard Form 703, Top Secret; Standard Form 704, Secret; and Standard Form 705, Confidential, shall be affixed to records containing that specific level of classified information. Cover sheets for various SCI programs (available through NND) should be used to protect such documents from unauthorized viewing.

(2) Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, and similar items containing classified information must be either:

(a) Destroyed promptly by the person responsible for preparing them, once they have served their purpose, or

(b) Given the same classification and safeguarded the same as the classified information produced from them.

(3) Typewriter ribbons used in typing classified information must be protected in the same way as the highest level of classification for which they are used. They must be destroyed the same way as classified working papers of that classification. After the upper and lower halves have been cycled through the machine five times in the course of regular typing, fabric ribbons may be treated as unclassified. Carbon and plastic typewriter ribbons and carbon paper used in producing classified information must be destroyed the same as working papers of that classification after one use. An exception to the foregoing, is that a typewriter ribbon that remains substantially stationary in the typewriter until it has received at least five consecutive impressions may be treated as unclassified.

(4) When classified information is to be made available for research, properly cleared employees move the material to a research room, supervise its use, return it to storage, and make sure that unauthorized persons do not have access to it. Notes taken from classified information in records or documents by researchers are to be safeguarded the same as the classified documents.

c. Care after working hours. All units that have custody of classified information must set up a system of security checks to make sure that classified information held by the unit is properly protected at the close of each work day. Custodians of classified information must inspect to make sure that:

Responsive to Paragraph #2

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

June 11, 2003



National Archives and Records Administration
8601 Adelphi Road
College Park, MD 20740

Dear [Redacted]

Enclosed, please find a copy of "EOP Document Request No. 2," dated June 4, 2003 (the "Request"), from the National Commission on Terrorist Attacks Upon the United States ("Commission"). As you will see, item No. 1 of the Request calls for materials produced under the former Administration (dating from January 1, 1998). Pursuant to the Presidential Records Act, I certify that responsive records may "contain information that is needed for the conduct of current business of the [Executive Office of the President] and that [they are] not otherwise available." 44 U.S.C. section 2205(2)(B). As you know, I faxed you a copy of this Request last week. In accordance with your standard procedures, including with regard to notification of the former President, please provide materials you believe may be responsive to the Request to the NSC Directorate of Records and Access Management, to my attention. Please let me know at your earliest convenience whether NARA will be able to meet the requested deadline and, if not, please provide a reasonable estimate of when you might be able to provide us with responsive materials, so that we may advise the Commission. Thank you for your timely assistance in this matter.

Sincerely yours,

William H. Leary
Senior Director
for Records and Access Management

Enclosure



James H. Keen
CHAIR

W. Hamilton
VICE CHAIR

Richard Ben-Veniste

Richard C. Cleveland

W. F. Fielding

W. S. Gorelick

William H. Gordon

Richard L. Lehman

Walter J. Roemer

W. R. Thompson

W. D. Zalkow
VICE DIRECTOR

EOP DOCUMENT REQUEST No. 2

The National Commission on Terrorist Attacks Upon the United States (the "Commission") requests that the Executive Office of the President (the "respondent") provide the Commission with the following documents and information no later than June 25, 2003 (the "production date"). The Commission requests that the respondent inform the Commission promptly if the production date poses a problem for certain categories of documents, such as documents from the previous Administration that may be in the custody of the National Archives and Records Administration, and meet promptly with the Commission staff to set a schedule for the production of those documents.

1. The briefing materials prepared or compiled by NSC staff and distributed to attendees for; any summaries prepared or compiled by NSC staff and distributed to attendees of the discussions held at and/or conclusions emerging from; and any minutes prepared or compiled by NSC staff of Principals and Deputies Committee meetings held from January 1, 1998, through September 20, 2001 that concerned:

- (a) Al-Qa'ida, Usama bin Laden, and/or Afghanistan;
- (b) the policy and budget development, implementation, or review of the overall counterterrorism policies of the United States, including PDD-62 (1998), the Five Year Counterterrorism Plan, and any successor NSPDs; and/or
- (c) counterterrorism issues involving threats to or attacks on the United States or American persons or assets in relations with Malaysia, Pakistan, Saudi Arabia, Sudan, the United Arab Emirates, and Yemen, other than materials that focus only on Palestinian terrorist activities.

Principals meetings include any such meeting whether chaired by the President or by the National Security Adviser. This request applies to principals or deputies level meetings addressing these topics wholly or in part regardless of the title used for the group or whether conducted in person or by SVTS, including meetings of the "Foreign Policy Team," the "Small Group," and the Counterterrorism Security Group (including CSG meetings chaired by the National Coordinator), as well as relevant meetings at Camp David.

2. The President's Daily Diary for September 11, 2001, and logs from the White House Situation Room, the Presidential Emergency Operations Center (PEOC), and the White House Military Office for September 11, 2001.

EOP DOCUMENT REQUEST No. 2
Page 2

3. Contemporaneous notes of individuals present in the PBOC or accompanying the President on September 11, 2001, including notes of White House officials other than the President. (A request for such documents directed to the Office of the Vice President will be submitted separately.)
4. The briefing materials prepared or compiled by White House staff and distributed to attendees for; any summaries prepared or compiled by White House staff and distributed to attendees of the discussions held at and/or conclusions emerging from; and any minutes prepared or compiled by White House staff of meetings at the principals or deputies level, including the Domestic Consequences Principals Committee, from September 11 through September 20, 2001, that concerned domestic policy responses to the terrorist attacks upon the United States.
5. Information sufficient to describe the activation and implementation of continuity of operations and emergency response plans and measures for the White House complex on September 11, 2001.

The Commission requests that the documents requested above be provided as soon as they are available, even though all requested documents may not be provided at the same time, through means of a "rolling" production.

If any requested documents are withheld from production, even temporarily, based on an alleged claim of privilege or for any other reason, the Commission requests that the respondent, as soon as possible and in no event later than the production date, identify and describe each such document or class of documents, as well as the alleged basis for not producing it, with sufficient specificity to allow a meaningful challenge to any such withholding.

If the respondent does not have possession, custody or control of any requested documents but has information about where such documents may be located, the Commission requests that the respondent provide such information as soon as possible and in no event later than the production date.

If the respondent has any questions or concerns about the interpretation or scope of these document requests, the Commission requests that any such questions or concerns be raised with the Commission as soon as possible so that any such issues can be addressed and resolved prior to the production date.

The Commission intends to make further document requests as its work develops and reserves the right to request additional documents and information in the areas addressed in this request.

June 4, 2003

Daniel Marcus
General Counsel



~~CONFIDENTIAL~~

Thomas H. Keas
CHAIR

Lee H. Hamilton
VICE CHAIR

Richard Ben-Veniste

Max Cleland

Fred F. Fielding

Jamie S. Greenlit

Sade Gorman

John Lehman

Timothy J. Roemer

Jane R. Thompson

Philip D. Zelikow
EXECUTIVE DIRECTOR

EOP DOCUMENT REQUEST NO. 3

(U) The National Commission on Terrorist Attacks Upon the United States (the "Commission") requests that the Executive Office of the President (EOP or the "respondent") provide the Commission with the following documents and information, with rolling production to begin no later than August 13, 2003 (the "production date"). The Commission requests that the respondent inform the Commission promptly if the production date poses a problem for certain categories of documents, such as documents from the previous Administration that may be in the custody of the National Archives and Records Administration, and discuss with the Commission staff a schedule for the production of those documents.

1. (U) All presidential directives related to overall national counterterrorism policies and operations, and those concerning Usama bin Laden (UBL), al Qa'ida, Afghanistan (including the Taliban and/or the Northern Alliance), Pakistan, Saudi Arabia, Sudan, and/or the setting of priorities for or national management of U.S. intelligence, from January 1, 1998 through September 20, 2001, including but not limited to:
 - a. Executive Orders (including any classified attachments thereto);
 - b. Presidential Decision Directives (including PDD 39 from 1995); and
 - c. National Security Presidential Directives (including NSPD 26 from 2002).
2. (U) All written communications, questions, notes, or other guidance (including notes of spoken questions, requests, instructions, or other guidance) from January 1, 1998 through September 20, 2001 that the National Coordinator for Terrorism (Richard Clarke) or the National Security Council (NSC) Directorate of Transnational Threats (TNT) staff received from the President, the Vice President, the National Security Advisor, and/or the Deputy National Security Advisor or their assistants, including messages prompted by items in the President's Daily Briefing (PDB), (a) relating to UBL and/or al Qa'ida, and (b) as to Afghanistan (including the Taliban and/or the Northern Alliance), Pakistan, Saudi Arabia, and/or Sudan, relating to terrorism or other matters that could reasonably be expected to affect U.S. policy

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

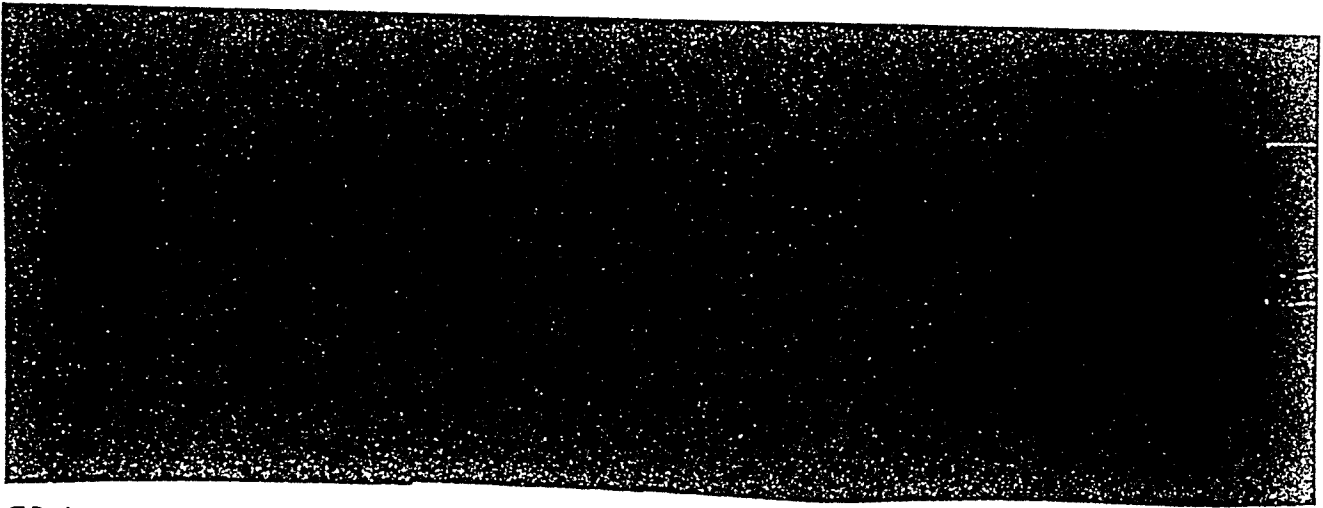
EO? Document Request No. 3
Page 2

on terrorism or cooperation with that country in countering terrorist threats to or attacks on the United States.

3. (U) Any substantive policy memoranda or other written communications (including emails) sent from the National Coordinator for Terrorism (Richard Clarke) or the TNT Directorate staff to the President, Vice President, National Security Advisor and/or the Deputy National Security Advisor, from January 1, 1998 through September 20, 2001, on (a) UBL and/or al Qa'ida, and (b) as to Afghanistan (including the Taliban and/or the Northern Alliance), Pakistan, Saudi Arabia, and/or Sudan, subjects relating to terrorism or other matters that could reasonably be expected to affect U.S. policy on terrorism or cooperation with that country in countering terrorist threats to or attacks on the United States. This request also includes responses to any tasking from the President or the National Security Advisor to the National Coordinator for Terrorism (Richard Clarke) or the TNT Directorate staff on these subjects.

4.

5.



6. (U) Documents summarizing (a) discussions relating to UBL and/or al Qa'ida, (b) discussions concerning Afghanistan (including the Taliban and/or the Northern Alliance) relating to terrorism or other matters that could reasonably be expected to affect U.S. policy on terrorism or cooperation with that country in countering terrorist threats to or attacks on the United States, and (c) discussions relating to counterterrorism issues involving threats to or attacks on the United States, between the President, the Vice President, the National Security Advisor, and/or the Deputy National Security Advisor and senior officials of the United Kingdom, Germany, Pakistan, and/or Saudi Arabia, from January 1, 1998 through September 20, 2001.
7. (U) Any transition briefings, options papers, and other documents prepared by the TNT Directorate staff for incoming officials and staff of the Bush administration from November 2000 through January 18, 2001, related to (a) counterterrorism, (b) UBL and/or al Qa'ida, (c) as to Afghanistan (including the Taliban and/or the Northern Alliance), Pakistan, Saudi Arabia, and/or Sudan, terrorism or other matters that could reasonably be expected to affect

~~CONFIDENTIAL~~

U.S. policy on terrorism or cooperation with that country in countering terrorist threats to or attacks on the United States, and (d) management of the Intelligence Community related to counterterrorism.

8. (U) Excerpts from the annual re-certification of ongoing covert action programs related to counterterrorism prepared by the NSC and signed by the President, from January 1, 1998 through September 20, 2001, sufficient to show the scale and priority of programs and resources devoted to counterterrorism.
9. (U) Classified annexes to the annual report to Congress on counterterrorism funding prepared by the Office of Management and Budget from 1998 through 2003.
10. (U) All official documents from the National Security Advisor and/or the Deputy National Security Advisor, and all documents from the TNT Directorate, setting forth strategy or policy guidance in analyzing, tracking, or disrupting the financing of terrorist activities or the movement of money in support of terrorist operations or groups, from January 1, 1998 through September 20, 2001, and documents sufficient to describe policies on these subjects now in force.
11. (U) Transcripts of all press interviews with President Bush discussing the facts and circumstances surrounding the 9/11/01 attacks and the immediate response of the United States, to the extent they have not already been produced.

(U) The Commission requests that the documents requested above be provided as soon as they are available, even though all requested documents may not be provided at the same time, through means of a "rolling" production.

(U) If any requested documents are withheld from production, even temporarily, based on an alleged claim of privilege or for any other reason, the Commission requests that the respondent, as soon as possible and in no event later than the production date, identify and describe each such document or class of documents, as well as the alleged basis for not producing it, with sufficient specificity to allow a meaningful challenge to any such withholding.

(U) If the respondent does not have possession, custody or control of any requested documents but has information about where such documents may be located, the Commission requests that the respondent provide such information as soon as possible and in no event later than the production date.

(U) If the respondent has any questions or concerns about the interpretation or scope of these document requests, the Commission requests that any such questions or concerns be raised with the Commission as soon as possible so that any such issues can be addressed and resolved prior to the production date.


Daniel Marcus, General Counsel

July 23, 2003

Responsive to Paragraph #3



OFFICE OF
WILLIAM JEFFERSON CLINTON

April 12, 2002

[Redacted]

National Archives and Records Administration
700 Pennsylvania Avenue, N.W.
Washington, DC 20408

Dear [Redacted]

I hereby designate Samuel R. Berger and Nancy Soderberg as agents on my behalf to review relevant National Security Council documents regarding the following topics.

- 1. Osama Bin Laden/Al Qaeda (1993-2000)
- 2. Sudan (1995-2000)
- 3. Presidential correspondence from or to Omar Bashir (1993-2000)

It is anticipated that Mr. Berger, my national security advisor, may be asked to testify in connection with upcoming Congressional hearings on terrorism, including efforts during the Clinton Administration. This review is for the purpose of allowing Mr. Berger to prepare for those hearings.

If you have any questions about this request, please contact Bruce Lindsey at 301-229-6359. Thank you for your attention to this matter.

Sincerely,

William Jefferson Clinton

Responsive to Paragraph #4



National Archives and Records Administration

700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

VIA MESSENGER
(NLMS 2003-035)

July 25, 2003

William H. Leary
Senior Director, Access Management
National Security Council
Room 392, EEOB
Washington, DC 20504

Dear Mr. Leary:

This is in reference to your letter, dated June 11, 2003, to [REDACTED] requesting that NARA provide the incumbent President with copies of Clinton Presidential records that are responsive to the EOP Document Request No. 2 from the National Commission on Terrorist Attacks Upon the United States.

Clinton Presidential records are administered in accordance with the Presidential Records Act (PRA), 44 U.S.C. §§2201-2207. Because the White House Counsel's Office has determined that these records are needed by the current Administration for the conduct of business and are not otherwise available, the request meets the requirement for exceptions to restricted access, 44 U.S.C. § 2205(2)(B). NARA has located 1,191 pages of Clinton Presidential records that are responsive to this request. In accordance with the PRA and section 6 of Executive Order 13233, NARA notified Bruce Lindsey, former President Clinton's legal representative, of our intent to provide these records to the incumbent President. We have been advised that the former President has agreed to authorize access to these records. Therefore, copies of these records are now being provided to you, on behalf of the incumbent President.

While the former President has raised no objection to providing these documents to the Commission, Mr. Lindsey notes that 58 pages represent direct communications between President Clinton's National Security Advisor, Samuel Berger, and President Clinton. (Copies of these documents have been flagged in the production set provided to the White House.) If the current Administration intends to assert executive privilege or determines that certain documents are not responsive, Mr. Lindsey requests that NARA be advised as to these specific documents. While this material is being produced to the incumbent President with the intention that the information in these documents will be provided to members of the Commission, these records should retain their status as Clinton Presidential records in accordance with the provisions of the PRA.

Please note that this is an interim response. NARA has completed its search in response to EOP Document Request #2 and is currently coordinating with the former President's representative on the review of the remaining records that will be the final response to this request.

If you have any questions regarding this request, please do not hesitate to contact me [REDACTED]
[REDACTED]

Sincerely,
[REDACTED]

Enclosure

cc: [REDACTED]

John Bellinger
General Counsel, National Security Council
Bruce R. Lindsey
[REDACTED]



National Archives and Records Administration

700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

VIA MESSENGER
(NLMS 2003-035)

August 1, 2003

William H. Leary
Senior Director, Access Management
National Security Council
Room 392, EEOB
Washington, DC 20504

Dear Mr. Leary:

This is the second production of Clinton Presidential records in reference to your letter, dated June 11, 2003, to [REDACTED] requesting that NARA provide the incumbent President with copies of Clinton Presidential records that are responsive to the EOP Document Request No. 2 from the National Commission on Terrorist Attacks Upon the United States.

Clinton Presidential records are administered in accordance with the Presidential Records Act (PRA), 44 U.S.C. §§2201-2207. Because the White House Counsel's Office has determined that these records are needed by the current Administration for the conduct of business and are not otherwise available, the request meets the requirement for exceptions to restricted access, 44 U.S.C. § 2205(2)(B). NARA has located 1,973 pages of Clinton Presidential records that are responsive to this request. In accordance with the PRA and section 6 of Executive Order 13233, NARA notified Bruce Lindsey, former President Clinton's legal representative, of our intent to provide these records to the incumbent President. We have been advised that the former President has agreed to authorize access to these records. Therefore, copies of these records are now being provided to you, on behalf of the incumbent President.

While the former President has raised no objection to providing these documents to the Commission, Mr. Lindsey notes that 8 pages represent direct communications between President Clinton's National Security Advisor, Samuel Berger, and President Clinton. (Copies of these documents have been flagged in the production set provided to the White House.) If the current Administration intends to assert executive privilege or determines that certain documents are not responsive, Mr. Lindsey requests that NARA be advised as to these specific documents. While this material is being produced to the incumbent President with the intention that the information in these documents will be provided to members of the Commission, these records should retain their status as Clinton Presidential records in accordance with the provisions of the PRA.

With this production, NARA has completed its search of Clinton Presidential records in response to EOP Document Request #2.

If you have any questions regarding this request, please do not hesitate to contact me [REDACTED]

Sincerely,

[REDACTED]

Enclosures

cc:

[REDACTED]

John Bellinger
General Counsel, National Security Council
Bruce R. Lindsey

[REDACTED]



National Archives and Records Administration

700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

VIA MESSENGER
(NLMS 2003-050)

September 12, 2003

William H. Leary
Senior Director, Access Management
National Security Council
Room 392, EEOB
Washington, DC 20504

Dear ^{Bill} Mr. Leary:

This is in reference to the request that the National Archives and Records Administration (NARA) provide the incumbent President with copies of Clinton Presidential records that are responsive to the EOP Document Request No. 3 from the National Commission on Terrorist Attacks Upon the United States.

Clinton Presidential records are administered in accordance with the Presidential Records Act (PRA), 44 U.S.C. §§2201-2207. Because the White House Counsel's Office has determined that these records are needed by the current Administration for the conduct of business and are not otherwise available, the request meets the requirement for exceptions to restricted access, 44 U.S.C. § 2205(2)(B). NARA has located 407 pages of Clinton Presidential records that are responsive to this request. In accordance with the PRA and section 6 of Executive Order 13233, NARA notified Bruce Lindsey, former President Clinton's legal representative, of our intent to provide these records to the incumbent President. We have been advised that the former President has agreed to authorize access to these records. Therefore, copies of these records are now being provided to you, on behalf of the incumbent President.

While the former President has raised no objection to providing these documents to the Commission, Mr. Lindsey notes that 115 pages represent direct communications between President Clinton's National Security Advisor, Samuel Berger, and President Clinton. (Copies of these documents have been flagged in the production set provided to the White House.) If the current Administration intends to assert executive privilege over these documents, or any other documents, Mr. Lindsey requests that NARA be advised of that development. In addition, if the current Administration determines that any of the documents are not responsive to the request, Mr. Lindsey requests that NARA be advised of that fact as well. Finally, please note that NARA is producing documents in their entirety even in instances when a portion of the information is non-responsive. If the current administration chooses to redact any information as non-responsive before producing this material to the Commission, Mr. Lindsey requests that a copy of those redacted documents be provided to NARA.

*

While this material is being produced to the incumbent President with the intention that the information in these documents will be provided to members of the Commission, these records should retain their status as Clinton Presidential records in accordance with the provisions of the PRA.

Please note that this is an interim response. NARA has completed its search in response to EOP Document Request #3 and is currently coordinating with the former President's representative on the review of the remaining records that will be the final response to this request.

If you have any questions regarding this request, please do not hesitate to contact me [REDACTED]

Sincerely,

[REDACTED]

Enclosure

cc:

[REDACTED]
John Bellinger
General Counsel, National Security Council
Bruce R. Lindsey
[REDACTED]



National Archives and Records Administration

700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

VIA MESSENGER
(NLMS 2003-050)

September 16, 2003

William H. Leary
Senior Director, Access Management
National Security Council
Room 392, EEOB
Washington, DC 20504

Bill
Dear Mr. Leary:

This is in reference to the request that the National Archives and Records Administration (NARA) provide the incumbent President with copies of Clinton Presidential records that are responsive to the EOP Document Request No. 3 from the National Commission on Terrorist Attacks Upon the United States.

Clinton Presidential records are administered in accordance with the Presidential Records Act (PRA), 44 U.S.C. §§2201-2207. Because the White House Counsel's Office has determined that these records are needed by the current Administration for the conduct of business and are not otherwise available, the request meets the requirement for exceptions to restricted access, 44 U.S.C. § 2205(2)(B). NARA has located an additional 155 pages of Clinton Presidential records that are responsive to this request. In accordance with the PRA and section 6 of Executive Order 13233, NARA notified Bruce Lindsey, former President Clinton's legal representative, of our intent to provide these records to the incumbent President. We have been advised that the former President has agreed to authorize access to these records. Therefore, copies of these records are now being provided to you, on behalf of the incumbent President.

While the former President has raised no objection to providing these documents to the Commission, Mr. Lindsey notes that 21 pages represent direct communications between President Clinton's National Security Advisor, Samuel Berger, and President Clinton. (Copies of these documents have been flagged in the production set provided to the White House.) If the current Administration intends to assert executive privilege over these documents, or any other documents, Mr. Lindsey requests that NARA be advised of that development. In addition, if the current Administration determines that any of the documents are not responsive to the request, Mr. Lindsey requests that NARA be advised of that fact as well. Finally, please note that NARA is producing documents in their entirety even in instances when a portion of the information is non-responsive. If the current administration chooses to redact any information as non-responsive before producing this material to the Commission, Mr. Lindsey requests that a copy of those redacted documents be provided to NARA.

While this material is being produced to the incumbent President with the intention that the information in these documents will be provided to members of the Commission, these records should retain their status as Clinton Presidential records in accordance with the provisions of the PRA.

Please note that this is an interim response. NARA has completed its search in response to EOP Document Request #3 and is currently coordinating with the former President's representative on the review of the remaining records that will be the final response to this request.

If you have any questions regarding this request, please do not hesitate to contact me [REDACTED]
[REDACTED]

Sincerely,

[REDACTED]

Enclosure

cc:

[REDACTED]

John Bellinger

General Counsel, National Security Council

Bruce R. Lindsey

[REDACTED]



National Archives and Records Administration

Obtained via FOIA by Judicial Watch, Inc.

700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

VIA MESSENGER
(NLMS 2003-067)

October 7, 2003

William H. Leary
Senior Director, Access Management
National Security Council
Room 5013, New Executive Office Building
Washington, DC 20504

Bill
Dear Mr. Leary:

This is in further reference to the request that the National Archives and Records Administration (NARA) provide the incumbent President with copies of Clinton Presidential records that are responsive to the EOP Document Request No. 3 from the National Commission on Terrorist Attacks Upon the United States. This production constitutes the second and final response to this request. NARA has previously provided 407 pages of Clinton Presidential records on September 12, 2003 and 155 pages of Clinton Presidential records on September 17, 2003 that were also responsive to EOP Document Request #3.

Clinton Presidential records are administered in accordance with the Presidential Records Act (PRA), 44 U.S.C. §§2201-2207. Because the White House Counsel's Office has determined that these records are needed by the current Administration for the conduct of business and are not otherwise available, the request meets the requirement for exceptions to restricted access, 44 U.S.C. § 2205(2)(B). NARA has located an additional 1,199 pages of Clinton Presidential records that are responsive to this request. In accordance with the PRA and section 6 of Executive Order 13233, NARA notified Bruce Lindsey, former President Clinton's legal representative, of our intent to provide these records to the incumbent President. We have been advised that the former President has agreed to authorize access to these records. Therefore, copies of these records are now being provided to you, on behalf of the incumbent President.

While the former President has raised no objection to providing these documents to the Commission, Mr. Lindsey notes that 103 pages represent direct communications between President Clinton's National Security Advisor, Samuel Berger, and President Clinton. (Copies of these documents have been flagged in the production set provided to the White House.) If the current Administration intends to assert executive privilege over these documents, or any other documents, Mr. Lindsey requests that NARA be advised of that development. In addition, if the current Administration determines that any of the documents are not responsive to the request, Mr. Lindsey requests that NARA be advised of that fact as well. Finally, please note that NARA is producing documents in their entirety even in instances when a portion of the information is non-responsive. If the current administration chooses to redact any information as non-responsive before producing this material to

the Commission, Mr. Lindsey requests that a copy of those redacted documents be provided to NARA.

While this material is being produced to the incumbent President with the intention that the information in these documents will be provided to members of the Commission, these records should retain their status as Clinton Presidential records in accordance with the provisions of the PRA.

If you have any questions regarding this request, please do not hesitate to contact me [REDACTED]

Sincerely,

[REDACTED]

Enclosure

cc:

[REDACTED]
John Bellinger
General Counsel, National Security Council
Bruce R. Lindsey

[REDACTED]