REPORT OF INVESTIGATION

Title (Name and address):	Type of Investigation:	Type of Report:
Samuel R. Berger [redacted] b2	Criminal	☒ Final ☐ Supplemental

Social Security Number: NA	☐ Employee ☒ Non-employee ☐ 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: [redacted] b2	Signature of Special Agent Making Report:
Office of Inspector General	1		
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

4. [redacted] b6, b7C
5. [redacted]
6. [redacted]

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, facilitated access to [redacted] b6,b7C 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

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] b6, b7C nor [redacted] reported this incident to any law enforcement entity before conducting an investigation of the incident.

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

[redacted]

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

[redacted] b2, b5, b6, b7C

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

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]. 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]. These documents [redacted] designated as the "W" intelligence files, contain classified information [redacted] material. b6, b7C b2, b5

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], 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

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. [redacted] 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. [redacted] 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] [redacted] b2, b6, b7C

[redacted] pursuant to DCID 6/9: Physical Security

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

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] b2,b5,b6,b7C received a [redacted] classified document from Little Rock, AR, [redacted], in response to an EOP request. [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 [redacted]

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 [redacted]

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 [redacted]

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

[redacted] asked [redacted] staff member [redacted] to buy a soda for Mr. Berger. [redacted] said Mr. Berger stepped out of [redacted] office, out of the suite, and into the hallway headed for the men's room. [redacted] said [redacted] came out of the suite and had to "side step" Mr. Berger. [redacted] said [redacted] saw Mr. Berger bent down, fiddling with something white, which could have been paper, around his ankle. [redacted] said [redacted] continued to the basement to buy the soda. [redacted] said [redacted] attempted to call [redacted] but could not recall [redacted] extension. [redacted] said [redacted] returned to the suite and asked [redacted] [redacted] to step out. [redacted] said [redacted] briefly explained to [redacted] what [redacted] had witnessed. According to [redacted], [redacted] asked [redacted] to write the information down. [redacted] said [redacted] sent an email to [redacted], before Mr. Berger left for the day. [redacted] b2, b6, b7C

[redacted] said [redacted] read the email. According to [redacted], when Mr. Berger stepped out to the men's room, [redacted] discussed with [redacted] if [redacted] was sure enough of what [redacted] saw to confront Mr. Berger. [redacted] said that [redacted] did not believe there was enough information to confront someone of Mr. Berger's stature. [redacted] [redacted] said [redacted] did not mention the email to [redacted] or discuss this matter until after Mr. Berger left. b2, b5, b6, b7C [redacted]

Mr. Berger said he took the first opportunity when [redacted] was out of [redacted] office to remove a document (a facsimile sent from [redacted] 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 [redacted]

On either September 2, 2003, or September 3, 2003, [redacted] contacted [redacted], and advised [redacted] of what occurred. According to [redacted], [redacted] said "we have a problem." [redacted] said [redacted] said [redacted] was worried Mr. Berger might be taking documents out of Archives I and that [redacted] and [redacted] staff were going to watch Mr. Berger closely on his next visit. When asked, [redacted] said [redacted] did not make these statements to [redacted] b2, b6, b7C [redacted]

[redacted] stated [redacted] mentioned the incident to [redacted] supervisor, [redacted], [redacted] [redacted]. According to [redacted], neither [redacted] nor [redacted] provided further guidance to [redacted]. [redacted] said [redacted] does not recall having a conversation with [redacted] about this incident in preparation for Mr. Berger's visit on October 2, 2003. However, [redacted] stated [redacted] approved a more aggressive action to be taken by [redacted] and the [redacted] when Mr. Berger returned but did not give [redacted] specific direction. b2, b6, b7C [redacted]

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. [redacted] 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. [redacted] 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. [redacted] b2, b6, b7C

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

(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.

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.

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.

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.

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.

[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

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]

[redacted] b2, b6, b7C [redacted]

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 [redacted]

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. [redacted], b6, b7C [redacted]

[redacted] stated [redacted] led the investigation [redacted] expanded that [redacted] b2, b6, b7C [redacted]

was on [redacted] leadership team, [redacted] had expertise in Archives' matters, and [redacted] was the [redacted], [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] asked [redacted] to head up this investigation. It was clear to [redacted] and [redacted] that [redacted] was not in charge. b2, b6, b7C [redacted]

[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]

[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]

[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 [redacted]

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]

[redacted] said

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]

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]

[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 [redacted]

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]

[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] 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 [redacted]

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]

[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 [redacted]

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. [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] b2, b5, b6, b7C

[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. [redacted] 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. [redacted] 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] 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. [redacted] b2, b5, b6, b7C

[redacted] said on October 10, 2003, [redacted] met with [redacted], [redacted], [redacted], [redacted], and [redacted], [redacted]. [redacted] said [redacted] shared potentially applicable statutes and executive orders at this meeting. [redacted] 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 [redacted]

The Inspector General (IG) was briefed on this matter on Friday, October 10, 2003. This same date, OI investigators along with [redacted], retrieved documents from Mr. Berger, at his residence, at the request of Mr. Berger's attorney. [redacted] said the documents appeared to be Mr. Berger's hand written notes. These documents were secured [redacted]. b2, b6, b7C

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

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:	Date and Time:
☒ Personal Interview ☐ Telephone Interview ☐ Records Review ☐ Other	May 31 – June 2, 2005
[redacted] b6,b7C [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] b6,b7C 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.

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. b2, A box usually belonged to one person or a directorate. [redacted] b6, b7C 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:	Case Title:
[redacted] b2	Samuel R. Berger [redacted] b2

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.

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. b6, b7C

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]

[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.

[redacted] explained that at this time the [redacted] was not running. Because the [redacted] was not running, a keyword search of the [redacted] database was conducted by [redacted], from the incumbent President's database, and a hard copy list of results, in the form of NSC numbered document numbers was provided to [redacted] staff. [redacted] contained in the correspondence requesting Mr. Berger's access to the records. [redacted].

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

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

[redacted] 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. [redacted] 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 [redacted], 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 [redacted] staff. This was because there were standard "out-cards" left in some files by Clinton staff.

[redacted] 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, [redacted] 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 [redacted] office. One box contained NSC numbered documents and three boxes contained SMOF files. [redacted] had originally pulled 5 boxes worth of SMOF files. Documents deemed responsive were copied and placed in boxes for [redacted]

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

[redacted] pulled the NSC numbered documents. [redacted] used the list [redacted] 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." [redacted] prepared a list of NSC numbered documents [redacted]. [redacted] sent this list, of six digit numbers only, to [redacted]. [redacted] made "out-cards" for the documents [redacted] 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 [redacted] 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.

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

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

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

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

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, [redacted] wrote on the SMOF, in pencil, where the file came from. These documents have not been re-filed in the originating box.

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

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

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].

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.

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.

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].

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. [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] 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].

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

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] b5, b6, took their copy set of what they produced to the White House for EOP 2. This included the documents sent up by [redacted]. [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. 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

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.

[redacted] numbered most of the copies. [redacted] became tired or it was late and [redacted] did not finish numbering the documents. [redacted] provided a note that [redacted] left [redacted] asking [redacted] to complete the numbering the morning of October 2, 2003. [redacted] 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 [redacted] notes first. Really, they were the first items in the box. [redacted] could recall the order documents were served as they were not in the room, with the exception of [redacted]. Then, Mr. Berger was provided one folder at a time for review. b6, b7C

[redacted] reviewed folders given to him by [redacted] 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

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

[redacted] gave [redacted] 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 [redacted] 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. [redacted] located the missing email. [redacted] then left for the day, before printing the missing email [redacted] called back to the office to ensure [redacted] knew what to look for on the email system in order to find the email in question. [redacted] told [redacted] another copy of this email was printed, [redacted] wrote #217 on the back, and provided to [redacted]. b6, b7C

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

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

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:

[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

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.

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.

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.

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.

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].

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 in 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.

[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.

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, b7

[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

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

ENCLOSURE(4)

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 A - SCIF Checklist (approved 27 May 1994)
Annex B - Intrusion Detection Systems (revised 18 November 2002)
Annex C - Tactical Operations/Field Training (approved 27 May 1994)
- Part I - Ground Operation
- Part II- Aircraft/Airborne Operation
- Part III - Shipborne Operation

Annex D - Part I - Electronic Equipment in SCIFs (approved 30 January 1994)
Part II - Handling and Disposal of Laser Toner Cartridges (revised 5 June 1998)
Annex E - Acoustical control and Sound Masking Techniques (approved 30 January 1994)
Annex F - Personnel Access Controls (revised 18 November 2002)
Annex G - Telephone Security (revised 18 November 2002)

---

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.

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

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

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

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

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:

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

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

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:

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.

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

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

(If Yes, Classification: _____, and provide copy of Co-utilization Agreement for SAP oeration 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

11. How is access to the SCIF controlled?

    a. By Guard Force: ____ YES ____ NO Security Clearance Level: _____

    b. By Assigned Personnel: _____ YES _____ NO

    c. By Access Control Device: _____ YES _____ NO
    If yes, Manufacturer _____ Model No _____

12. Does the SCIF have windows? _____ YES _____ NO

    a. 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 _____ NO

    a. 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 _____ NO

        2. Noise Generator: _____ YES _____ NO

        3. Non-Conductive Joints: _____ YES _____ NO

        4. 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 _____ NO
    Are 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 duet 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): _____
_____

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?

___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

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,

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.

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.)

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 though 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

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

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 1¾ 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 1¾ 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:

- 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.]

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)

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

- 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:

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:

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.

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, an 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.

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 Iin 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).

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 he 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 he limited to:

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):

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 surruptitious 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

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 cheeks 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.

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 he 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,

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).

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

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.

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.

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.

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

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] Superceded Annex B dated 27 May 1994.

[5][5] Superceded Annex F dated 5 June 1998.

[6][6] Superceded 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:	Date and Time:
☒ Personal Interview ☐ Telephone Interview ☐ Records Review ☐ Other	July 8, 2005 9:30 a.m.
Activity or Interview of: Samuel R. Berger	**Conducted by:** [redacted] b6, b7C
	Location of Interview/Activity: Washington, DC

Subject Matter/Remarks

On July 8, 2005, [redacted] b6, b7C 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 [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 b6, security called [redacted], office and someone from b7C [redacted] office would escort Mr. Berger to [redacted] office. Mr. Berger always left late in the

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

ENCLOSURE(7)

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] [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

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] [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] [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.]

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 [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.

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.

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.

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.

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

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 though 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

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.

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.

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.

[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.

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]

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

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.

[redacted] told Mr. Berger there was a missing document, one that [redacted] 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 [redacted] said. Mr. Berger disassembled first, then he asked [redacted] if the document could have been misfiled. [redacted] said "No." Mr. Berger asked if they had not produced this document already. [redacted] said it was a different version. b6, b7C

[redacted] gave him another copy of the document. Mr. Berger slid this document under his portfolio also. [redacted] did not ask for it back. If [redacted] 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. [redacted] wanted him to finish the review and said they only had about an hours worth of work left. He understood [redacted] was getting pressure from the White House to provide a response so he agreed. [redacted] 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 [redacted]. 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 [redacted] 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 [redacted] and [redacted] staff would notice that his pockets were bulging. [redacted] b2, b6, b7

If Mr. Berger had been aware [redacted] 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: [redacted] b2	Case Title: Samuel R. Berger [redacted] b2

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] 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

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.

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.

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.

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.

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.

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.

[redacted] 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 [redacted] 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 [redacted] 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.

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(11)

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(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(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:	Date and Time:
☐ Personal Interview ☐ Telephone Interview ☒ Records Review ☐ Other	June 2005
Activity or Interview of: Verification of Documents	**Conducted by:** [redacted] 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, b7

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

ENCLOSURE(17)

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.)

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:

b2

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

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