~~SECRET//NOFORN~~

2014-11718-IG
18 July 2014

(U) REPORT OF INVESTIGATION

(U//FOUO) Agency Access to the SSCI Shared Drive on RDINet

CENTRAL INTELLIGENCE AGENCY
Office of Inspector General

David B. Buckley
Inspector General

[redacted]
Assistant Inspector
General for Investigations

[redacted]

NOTICE: The information in this report is covered by the Privacy Act, 5 U.S.C §552a; and should be handled accordingly.

~~SECRET//NOFORN~~

(U) This page has been intentionally left blank.

(U) Executive Summary

(U) On 30 January 2014, the CIA Office of Inspector General (OIG) opened an investigation into allegations that Agency personnel improperly accessed Senate Select Committee on Intelligence (SSCI) staff files and records on the CIA-operated and maintained Rendition, Detention, and Interrogation network (RDINet). On 30 January 2014, in accordance with Title 50 U.S.C. § 3517(b)(5), OIG reported the matter to the Department of Justice (DOJ) for potential violations of Titles 18 U.S.C. § 2511 (Wiretap Act) and 18 U.S.C. § 1030 (Computer Fraud and Abuse Act)[1]. The investigation was predicated on information obtained as part of an OIG review into allegations made by SSCI Chairman Dianne Feinstein to Director of the Central Intelligence Agency (D/CIA) John Brennan that CIA personnel had "conducted one or more searches of the computer network at an offsite facility that the CIA had assigned exclusively to the staff of the [SSCI]." The OIG investigation was limited in scope to review the conduct of Agency officials, and did not examine the conduct of SSCI staff members.

(U) The OIG investigation determined the following:

1. (U) Five Agency employees, two attorneys and three information technology (IT) staff members, improperly accessed SSCI Majority staff shared drives on the RDINet.
   - (U) The three IT staff members who accessed the SSCI Majority shared drive displayed a lack of candor about their activities when interviewed by the OIG.
2. (U) The Agency filed a crimes report with the DOJ, reporting that SSCI staff members may have improperly accessed Agency information on the RDINet. The OIG investigation determined that the factual basis for this referral was unfounded and the author of the letter had been provided inaccurate information on which the letter was based.
3. (U) Subsequent to directive by the D/CIA to halt the Agency review of SSCI staff access to the RDINet, [redacted] Security [redacted]/OS) conducted a limited and incomplete investigation of SSCI activities on the RDINet that included [redacted] and a review of some of the emails of SSCI Majority staff members on that network.

(U) RDINet was built at an Agency facility in June 2009 to support a SSCI review of the Agency's rendition, detention, and interrogation activities. RDINet was created to allow Agency staff to review documents for production to the SSCI, and to provide appropriate documents to the SSCI staff. Separate electronic shared drives were created on RDINet for the use of the SSCI Majority and Minority staffs and for the Agency personnel supporting the review and redaction

[1] (U) On 30 April 2014, the DOJ advised the CIA Inspector General that DOJ had completed its review of the allegations and had no prosecutorial interest.

of documents provided to the SSCI review teams. Following review of relevant documents by the RDI team, responsive documents were then made available to SSCI staff members on their respective shared drives.

(U) As part of the Agency's efforts to review and provide documents to the SSCI, then D/CIA Leon Panetta requested summaries of the documents being provided to the SSCI. These summary/analytical documents were considered and marked as internal and privileged by the Agency. The Agency holds that the documents were outside the scope of the data which the Agency agreed to provide for the SSCI review. The creation of such summaries was halted in early 2010 when the DOJ began an inquiry (led by Assistant United States Attorney John Durham) into RDI matters.

(U) While there was no signed memorandum of understanding between the Agency and SSCI regarding access to the RDINet, correspondence between then D/CIA Panetta and Chairman Feinstein established a common understanding between the parties that the SSCI shared drives would be a walled-off area that would only be accessible to CIA IT administrators for the sole purpose of IT network administration. In addition to the common understanding, the SSCI staff were provided a warning at each login that their "use of this system may be monitored and you have no expectation of privacy."

(U) Improper Agency Access to SSCI files on RDINet

(U) On or before 9 January 2014, personnel from the Agency's RDI team theorized that SSCI staffers had improperly obtained copies of the privileged intelligence summaries created by the Agency, and that these documents were stored on the SSCI Majority staff shared drive. On 9 January, members of the RDI team used the IT system administrator access to the SSCI Majority shared drive to prove this theory. The Office of General Counsel (OGC) attorney [redacted] unilaterally concluded that [redacted] had the legal authority to task members of [redacted] to access the SSCI shared drive and conduct a search for copies of the privileged documents. A second OGC attorney, [redacted] tasked three members of the RDI IT team to use their administrative rights to access and view documents on the SSCI Majority shared drive on three separate occasions between 9 and 12 January 2014.

(U) As a result of their review, the two OGC attorneys [redacted] concluded that copies of the intelligence summaries were present on the SSCI Majority shared drive, and that the Agency had not provided those documents to the SSCI staff as part of regular provisioning of RDI documentation. The attorneys therefore believed the SSCI staff had improperly accessed portions of the RDINet that were restricted to Agency staff, and through this access moved the intelligence summaries onto the SSCI Majority staff shared drive.

(U) On 9 January, following their tasking to the IT team, the OGC attorneys also tasked the Agency's internal IT monitoring component with obtaining further information on the activities

of SSCI staffers on RDINet, using data previously collected by the Agency on the system. Both attorneys informed the monitoring team that the tasking was directed by the D/CIA; however, the OIG investigation showed no evidence that the D/CIA ordered the tasking or was even aware of the tasking at the time it was made. Based upon this tasking, the monitoring team staff performed a limited review of SSCI staff activity, using the previously collected data.

(U) Office of Security Review of SSCI Staff Activity

(U) On 14 January 2014, the D/CIA became aware that the monitoring team had been engaged to review the questioned activities of the SSCI staff on RDINet, and immediately ordered a standdown on any and all investigative activities. The D/CIA briefed SSCI Chairman Feinstein on 15 January that, based upon information provided to him by the attorneys, SSCI staff members had improperly accessed Agency documents. The D/CIA recommended to the SSCI Chairman and Vice Chairman a joint forensic review of the activities of SSCI staffers and Agency personnel on the SSCI shared drive. The OS was then asked by the Office of the D/CIA to prepare to conduct a joint forensic review with SSCI. Prior to the commencement of this joint review, the SSCI Security Officer informed OS that, per Chairman Feinstein, the SSCI was on standdown for any joint review. Despite this notice that SSCI was no longer interested in a joint review, OS requested concurrence from the D/CIA's office to proceed with a unilateral review of Agency and SSCI activity on the SSCI shared drive. Without waiting for concurrence from D/CIA /OS directed an investigation by staff that resulted in the generation of a report of SSCI activity on the SSCI Majority shared drive, which included forensically reconstructed some RDINet emails between SSCI staffers. The review was also based, in part, on information previously collected by the monitoring team.

(U) Agency Crimes Report On Alleged Misconduct by SSCI Staff

(U) On 7 February 2014, the then-Acting General Counsel, who had previously recused himself from RDI-related matters and was therefore largely unaware of programmatic details, filed a crimes report with the DOJ, as required by Executive Order 12333 and the 1995 Crimes Reporting Memorandum between the DOJ and the Intelligence Community based on inaccurate information provided to him by OS. The crimes report stated that SSCI staffers may have exploited a software vulnerability on RDINet to obtain access to the intelligence summaries created by the Agency, in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. The report was solely based on inaccurate information provided by the two OGC attorneys to OS and was not supported by, or consistent with, the results of the limited investigation conducted by OS team. The OIG investigation determined that there was no factual basis for the allegations made in the CIA crimes report.

(U) Lack of Candor by Certain RDI Staff

(U) The OIG determined that RDINet IT officers responsible for assisting in conducting the search of the SSCI Majority shared drive were not forthcoming in their initial interviews with OIG, in that they failed to disclose to the OIG the activities they conducted, at the attorneys' direction, to access the SSCI Majority staff shared drive. When interviewed a second time and confronted with evidence of their actions, two of the officers admitted to their conduct. The third officer declined a second interview.

(U) This page has been intentionally left blank.

I. (U) Predication

1. (U//FOUO) On 29 January 2014, the Office of Inspector General (OIG) initiated a special review into the activities of CIA personnel related to the access of Senate Select Committee on Intelligence (SSCI) files and records on the Rendition, Detention, and Interrogation network (RDINet) located at the [redacted] building, an Agency facility in the [redacted] On 30 January 2014, OIG opened an investigation based on information discovered in the special review. In accordance with Title 50 U.S.C. § 3517, OIG reported the matter to the Department of Justice (DOJ) on 30 January 2014 for potential violations of Title 18 U.S.C. § 2511 (Wiretap Act) and 18 U.S.C. § 1030 (Computer Fraud and Abuse Act).

2. (U//FOUO) On 23 January 2014, SSCI Chairman Dianne Feinstein sent a letter to the Director, Central Intelligence Agency (D/CIA) John Brennan alleging that CIA personnel had "conducted one or more searches of the computer network at an offsite facility that the CIA had assigned exclusively to the staff of the [SSCI]." The letter detailed several questions Chairman Feinstein had regarding the conduct of CIA personnel and alleged violations of the 4th Amendment, the Speech and Debate Clause of the Constitution, the Computer Fraud and Abuse Act, and Executive Order 12333.

3. (U//FOUO) OIG investigation was limited to the alleged access of SSCI data on RDINet by Agency personnel (Exhibit A) in January 2014 and the subsequent actions taken. OIG investigation covered the issues of Agency personnel engaging in unauthorized access or exceeding authorized access to the RDINet, Agency monitoring of the RDINet, and whether a formal agreement had been made between the CIA and the SSCI regarding the use of RDINet. The activities of SSCI staff members were deliberately excluded from the investigation. No attempt was made to interview SSCI staff members, and digital forensics on RDINet and the associated [redacted] performed by OIG was limited in scope to avoid obtaining information related to the activities of SSCI users beyond that provided as part of the predication for the investigation. The U.S. Senate arranged for a specific review of the alleged misconduct by U.S. Senate staff to be conducted by the U.S. Senate Sergeant-at-Arms.

II. (U) POTENTIAL STATUTORY OR REGULATORY VIOLATION(S)

- *(U) Title 18 United States Code § 2511 Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited (Wiretap Act)*
- *(U) Title 18 United States Code § 1030 Fraud and Related Activity in Connection with Computers (Computer Fraud and Abuse Act)*

III. (U) BACKGROUND

(U) Review of the Rendition, Detention, and Interrogation Program

4. (U//FOUO) On 26 March 2009, the SSCI informed the CIA that the SSCI planned to conduct a thorough review of the CIA's RDI Program[1]. On 22 June 2009, the SSCI staff began their review. The review necessitated access by SSCI staff to a large volume of sensitive, classified, and compartmented CIA documents. In order to provide the documents to the SSCI staff and ensure pertinent information was provided, the CIA established a review process. Initially, the SSCI staff provided search terms to the CIA RDI Review Team ("RDI team")[2] to identify responsive documents. The RDI team tasked Agency components with searching their databases for the requested material and collected the potentially responsive documents. The CIA tasked components of the Agency to conduct additional searches of their holdings for potentially responsive documents that were then provided to the RDI team. The RDI team reviewed the documents for responsiveness, removed information designated as Executive Privilege information, and provided the SSCI staff with access to the documents via the RDINet.

5. (U//FOUO) In an effort to understand the information the Agency had released and continued to release to the SSCI staff, the RDI Special Review Team (SRT) was created in May 2009. The SRT created documents known as Weekly Case Reports (WCRs), among other documents, at the request of then D/CIA Leon Panetta for the purpose of summarizing for CIA management the information being produced to the SSCI. In approximately February or March 2010, WCR production was halted by members of the Agency staff in response to a Department of Justice investigation led by Assistant U.S. Attorney John Durham.[3] Agency staff interviewed by CIA OIG interpreted the "Panetta Review" (a.k.a. Panetta Report) as a compilation of the WCRs.

(U) RDINet System

6. (U//FOUO) To facilitate SSCI staff access to the large number of released documents, the CIA created a computer network called RDINet. RDINet was established in a secure CIA vault in the [redacted] of the CIA's [redacted] building, with separate physical locations for CIA analysts to review and redact responsive documents and a physical "reading room" for SSCI staff to review responsive documents. The SSCI Majority and Minority staffs

[1] (U//FOUO) The Senate has historically referred to this as a study on the CIA's Detention and Interrogation Program. The study was launched following then D/CIA Michael Hayden's disclosure of the program to the SSCI in September 2006. On 5 March 2009, the SSCI voted to initiate a comprehensive review of the program.

[2] (U//FOUO) The RDI Review Team has had several historical names, including the Director's Review Group and the Office of Detainee Affairs. The team included attorneys from the Office of General Counsel that oversaw the RDI review performed by SSCI and an information technology team that supported the RDI system used for review.

[3] (U//FOUO) In January 2008, Assistant U.S. Attorney John Durham was appointed by the DOJ to lead an investigation into the destruction of videotapes of the interrogation of detainees. In mid-2009, the Durham task force was expanded to include a review of the detention and the use of various interrogation techniques by the Agency.

were later physically separated into two secure reading rooms at the request of the SSCI. Each of these offices included secure CIA-provided computer workstations for the review of materials released by the CIA and for the creation of individual work product.

7. (U//FOUO) RDINet is a standalone network that has a limited connection to the Agency Data Network (ADN) for administration purposes, including the ingestion of system software patches and updates and for routine network monitoring (Exhibit B). The SSCI and CIA were provided shared storage areas on RDINet that physically reside on the same hard drive array. Separate electronic storage drives were established for both the CIA and the SSCI to save documents and their respective reports. The SSCI was also provided additional storage drives further segregated between the Majority and Minority staff. Access to data was restricted through the use of access control lists and logical rules associated with the software. This virtual separation was intended to control access by the various parties to the RDINet, e.g., to prevent general CIA RDINet users from observing or accessing SSCI data, and to prevent SSCI users from observing or accessing CIA data that had not been released to them. Lotus Notes was installed on the network to provide an internal RDINet email capability. The email server allowed for communication among all RDINet users, both CIA and SSCI, and had no connectivity to the ADN.

8. (U//FOUO) From inception, the Office of General Counsel (OGC) was charged by the Agency with overseeing and supporting the RDI Program review.

9. (U//FOUO) In October 2013, when General Counsel Stephen Preston departed, was appointed the Acting General Counsel. Because had previously recused from any RDI matters,

Because of recusal regarding the RDI matter, was unsupervised by the Office of General Counsel pertaining to this matter.

10. (U//FOUO) On 22 June 2009, SSCI staff members began their review of RDI materials at the secure facility.

11. (U//FOUO) In November 2012, the RDI team learned of a vulnerability with the Google appliance, related to configuration settings that had been in place since the initial installation in November 2009. OIG reviewed an April 2013 email between members of the RDINet IT staff detailing the existing settings, which indicated an access control deficiency for search results. The RDI IT team updated the Google appliance in April 2013 to reflect this change. Prior to this update, the settings provided to OIG showed that the Google appliance was not configured to enforce access rights or search permissions within RDINet and its holdings.

12. (U//~~FOUO~~) On 1 November 2012, SSCI emailed of the RDI IT staff, and others to inform them that the new Google appliance was indexing the Majority staff work product on a shared drive. requested that the IT staff configure the tool to stop indexing the shared drive. OIG found that the Agency did not take action to address request.

(U) Memorandum of Understanding Regarding the Operation of RDINet

13. (U//~~FOUO~~) During the course of this investigation, OIG determined that a signed and finalized Memorandum of Understanding (MOU) between the SSCI and the CIA on the RDI review, including access controls, did not exist. Nevertheless, multiple interviewees referred to the existence of a signed MOU. In this regard, OIG found that that a series of written letters were exchanged between SSCI (Chairman Feinstein, then Vice Chairman Bond and then and CIA (then D/CIA Panetta and then) detailing the desires of each side with regard to the use of CIA space and systems, and SSCI access to documents (Exhibit C). These letters were found to contain some common language with regard to the use of the CIA facilities and computer systems.

14. (U//~~FOUO~~) The last letter OIG found on the topic from then D/CIA Panetta to Chairman Feinstein, dated 12 June 2009, described that "an agreement was reached between CIA and SSCI staff personnel regarding operating procedures for the SSCI review of material related to the CIA's detention and interrogation programs." The standard operating procedures (SOPs) referenced appeared to be detailed in a document titled "Standard Operating Procedures for SSCI Review,"[4] a three-page, 18-point document produced to OIG by the Office of General Counsel (Exhibit C.e). Point five of the document discussed the Committee's need to "create work product on a walled-off network share-drive" accessible only by the SSCI, and "CIA access to the walled off network shared drive will be limited to CIA information technology staff, except as authorized by the Committee or its staff." Point eight stated that all Committee staff granted access to the Reading Room were required to receive a security briefing. OIG reviewed a document titled "Security Briefing," dated "May 2009," but found no evidence that the briefing was ever provided to SSCI staff participating in the RDI review.

15. (U//~~FOUO~~) A separate document, titled "Memorandum of Understanding Senate Select Committee on Intelligence's Review of CIA's Detention and Interrogation Program"[5] (Exhibit C.a), dated 28 May 2009, stated in point "C." that,

> A specially designed share-drive will be provided on the Agency's stand-alone network. As SSCI requires, the share-drive can be segregated with only SSCI access and walled-off CIA IT administrators, except as otherwise authorized by SSCI [sic].

[4] (U) Author unknown. The OIG did not find evidence that this document was provided to the SSCI.
[5] (U) Agency author. The OIG did not find evidence that this document was provided to the SSCI.

OIG found no evidence that this document was provided to the SSCI staff involved in the review or signed by either party. An email provided to OIG in relation to this document, from then [redacted] to several CIA officers on 27 May 2009, stated that the document was a "proposed MOU that we will attempt to finalize with the SSCI staff." The email made reference to having SSCI staff sign a Nondisclosure Agreement (NDA) as well. OIG was not able to find any documentation that SSCI staffers signed an Agency NDA.

(U) Monitoring

16. (U//~~FOUO~~) The RDINet desktops were built as modified versions of the standard Agency workstations. At the time of inception, software security measures were put in place by the CIA to protect classified information from exploitation, including the [redacted] and a logon warning banner. Both were standard features that were part of any Agency workstation.

17. ~~(S//NF)~~ [redacted] (Exhibit D). [redacted] OIG found no evidence that SSCI members had been briefed on monitoring specific to RDINet.

18. (U//~~FOUO~~) The RDINet warning banner is the standard Agency warning banner. It consists of an advisement that all users are exposed to at the time of each login, which included any SSCI user who logged onto the RDINet. The warning is located in a dialogue box that the user has to acknowledge prior to logging in. The dialogue box consists of the following text:

> This is a U.S. Government system and shall be used for authorized purposes only. All information on this system is the property of the U.S. Government and may not be accessed without prior authorization. Your use of this system may be monitored and you have no expectation of privacy. Violation of system security regulations and guidance may result in discipline by the Agency, and violators may be criminally prosecuted.

(U) Acting General Counsel Department of Justice Crimes Report

19. (U//~~FOUO~~) On 7 February 2014, CIA Acting General Counsel [redacted] wrote to Attorney General, Eric Holder, to report the matter of potential violation of Title 18 USC § 1030 (Fraud and Related Activity in Connection With Computers) by members of the

SSCI on the RDINet[6] (Exhibit E). The report detailed that in the November 2010 timeframe, a member of the SSCI staff conducted a search on the RDINet that appeared intended to access a part of the system to which the member did not have authorized access.

IV. (U) INVESTIGATIVE FINDINGS

(U) Executive Summary of Investigative Findings

20. (U//FOUO) OIG investigation found support for allegations that CIA staff intentionally accessed the SSCI shared drive without authorization and exceeded authorized access. Additionally, three members of the RDINet IT team were not candid with OIG when interviewed and initially failed to disclose their recent investigative access to the SSCI shared drive. The investigation did not find support for the allegation that CIA performed real-time interception of SSCI communications for its review of the matter in question, however, CIA did review stored information that included and a review of some of the emails of SSCI Majority staff members on that network. The investigation found that D/CIA Brennan did not authorize the access or know the extent of the access, and OIG obtained conflicting testimony regarding whether or not D/CIA Brennan had any knowledge of a review performed on the SSCI shared drive until after it was completed. OIG investigation further found that the Director of Security authorized a review of the SSCI activities, including the reconstruction of the emails of SSCI staffers, following a stand-down order by the D/CIA and a request to withdraw authorization by the SSCI security officer. Finally, OIG investigation found that the CIA referral of criminal conduct by SSCI staffers was predicated on inaccurate information provided to the then-Acting General Counsel.

(U) Absence of a Formal Memorandum of Understanding Regarding the Operation of RDINet

21. (U//FOUO) OIG did not find evidence that a final document was agreed upon by both the SSCI and CIA, nor any documentation that an agreement was signed by the CIA or the SSCI. OIG did find, however, that there was a common understanding reached between the CIA and the SSCI. Several letters between SSCI Chairman Feinstein, then SSCI Vice Chairman Bond, and then D/CIA Panetta were exchanged in 2009 that contained enough similar language to define a working agreement. The common understanding between the SSCI and CIA did contain language regarding a walled-off network shared drive for exclusive SSCI use, except when IT staff required access for maintenance or troubleshooting. In addition to the working agreement, the SSCI staff were provided a warning at each login that their "use of this system may be monitored and you have no expectation of privacy." OIG found that the installed at the outset of RDINet by CIC/ was connected in the normal course of business and was collected in a manner consistent with the administration of

[6] (U) Pursuant to Section 1.6(b) of Executive Order 12333, as amended, and Sections VI.B, VII.A.4, and VIII.A of the 1995 Crimes Reporting Memorandum of Understanding between the Department of Justice and the Intelligence Community, the CIA is required to the report to the DOJ information concerning federal crimes.

Agency information systems. Additionally, OIG did not find documentation that NDAs or security briefings were provided to or signed by the SSCI staff.

(U) Unauthorized CIA Access to RDINet and Related Taskings

22. (U//~~FOUO~~) During the course of the investigation, OIG found that in January 2014, five Agency officers exceeded authorized access or directed such access to the SSCI side of RDINet. These accesses were not conducted as part of IT administration or routine Agency monitoring, but as part of a CIA investigation into how SSCI staffers obtained copies of documents referred to as WCRs.

23. (U//~~FOUO~~) the OGC attorney told OIG that became suspicious of an apparent security breach on the RDI system in December 2013. suspicions stemmed from letters from SSCI Chairman Feinstein and Senator Udall requesting copies of the "Panetta Review," the latter of which Senator Udall used to explain the reason for delaying Caroline Krass' confirmation hearing as CIA General Counsel. supposed that the "Panetta Review" referred to SRT documents or WCRs that were created at the behest of then D/CIA Panetta. As a result, told OIG began to consider the circumstances of how SSCI could have obtained access to CIA documents considered to be inappropriate. Between late December 2013 and early January 2014, expressed suspicions to and informed that the RDINet logs should be reviewed to determine how SSCI obtained access to the WCRs. OIG review of titled "Memorandum for the Record re: partial timeline of events surrounding discovery of SRT documents on RDI NET," ("MFR") (Exhibit F) which contained a timeline of events from perspective. In this document unilaterally reached the legal conclusion that had the legal authority to task members of to access the SSCI shared drive and look for Agency documents to which believed the SSCI staffers were not entitled. stated that tasked the IT team to look for SRT documents on the SSCI staff side on 9 January 2014.[7]

(U) RDI IT Team Review

24. (~~C//NF~~) On 9 January 2014, after a discussion with directed RDINet IT, to set up a user profile on RDINet that was configured with the same privileges as a SSCI Majority staff user. requested this access in order to run Google queries with the same permissions as a SSCI staffer to see what they were able to view in their search results. identified the presence of WCR reports on the SSCI Majority shared drive through a review of the Google search results. After identifying the documents, mapped to the folder where the documents resided and used "dummy account" with SSCI-like permissions to

[7] (U//~~FOUO~~) was initially interviewed by OIG prior to the discovery of the MFR. Following the discovery of the MFR, declined to be interviewed about its contents.

open the folder. recognized the documents as likely WCR reports based on their filenames and folder structure, and opened "a few" of the documents to view the first page, where observed a disclaimer and format similar to the WCR documents. informed of the findings. briefed and on the findings.

25. (U//~~FOUO~~) On 10 January 2014, tasked to search the RDINet database to verify whether the SSCI had been provided access to the restricted documents. search of the database revealed that the documents were not located in the database and they concluded that they had therefore not been produced by the CIA to the SSCI for review. Following search, conducted a search on the root of the RDINet shared drive, which contains all user profiles, user accounts, and shares used by both CIA and SSCI users. search indicated that the restricted documents were located on the SSCI Majority shared drive and one SSCI user's personal drive. navigated directly to the locations of interest on the SSCI Majority shared drive as well as to the SSCI user's personal drive.

26. (U//~~FOUO~~) During the course of the investigation, OIG received conflicting statements from regarding additional accesses to the SSCI shared drive and subsequent screenshots taken during those accesses. According to following confirmation that the restricted documents were present on the SSCI Majority shared drive, specifically requested access to the drive so that could look at the documents granted this access, associating the drive as workstation, for approximately 20 minutes. stated that, during this time, captured screenshots of the SSCI Majority shared drive file structure. emailed the screenshots to requesting the screenshots be transferred to the ADN. According to however, requested that come to office, where provided access to the SSCI Majority shared drive from workstation. when interviewed, was unsure of the methods used to grant the access and stated that helped take screenshots of folders and sub-folders of interest on the SSCI Majority shared drive on behalf.

27. (U//~~FOUO~~) OIG review of activity associated with RDINet user account on 10 January 2014 showed attempts were made to access Next, activity showed usage of followed by a Lotus Note to ADN. A review of personal storage drive on the ADN found a folder named which contained related to searches of the SSCI Majority shared drive, home page, and "not authorized" messages.

28. (U//~~FOUO~~) provided the screenshots to and tasked to determine if the restricted documents had been accessed by SSCI staffers. On 10 January 2014,

tasked by email to obtain The email acknowledged that this was a SSCI shared drive.

29. (U//~~FOUO~~) On 12 January 2014, sent an email to the RDINet IT team requesting new versions of the screenshots that showed Q:\ as the mapped drive letter vice Y:\. SSCI user access to the drive was mapped as requested these updated screenshots in order to "provide the optic" (e.g. display more accurately) that the folder was located on the SSCI Majority shared drive. Both complied with the request and emailed responses on 13 January 2014.

30. (~~C//NF~~) At OIG's request, provided OIG an email and attachments dated 13 January 2014 from to and copying The email documented the RDINet IT team's response to 12 January tasking and contained snapshots of the contents of the folder properties and security settings for a document titled "WCR MJA," and a capture of the virtual folder "My Computer", showing the drive Q:\ labeled as "Share Majority Data." also responded to a series of questions from regarding the number of files in and in its subfolders, as well as information regarding SSCI privileges on RDINet.

31. (U//~~FOUO~~) Between 5 June and 13 June 2014, OIG and Senate Sergeant-at-Arms conducted a joint forensic review of the RDINet log data. The review determined that relevant logs containing file access and security information were not retained appropriately[8]. A review of file meta-data did not show any CIA users as having altered the WCR documents contained in the Q:\ drive, but did not contain sufficient information to assess access by CIA users.

32. (~~C//NF~~) During the course of the investigation, OIG determined that RDINet IT officers were not forthcoming in their initial interviews with OIG, having failed to disclose the assistance they provided to in the searches of RDINet between 9 and 13 January 2014. As a result, OIG requested second interviews with each officer. complied with the second interview requests and admitted to the conduct when confronted with the information from the emails; declined a second interview.

(U//~~FOUO~~) *Review*

33. (~~S//NF~~) OIG investigation found that on 10 January 2014, tasked to conduct a review of activity on the SSCI side of RDINet. As a part of the review requested by ran queries against previously archived RDINet data to determine whether the documents in question had been accessed by SSCI staff. The date

[8]

range of the review focused on the 2010 to 2013 time period. as a part of any of the activities in question during the January 2014 time frame. all data reviewed by at the request of the RDI team was historically logged information.

34. ~~(C//NF)~~ In multiple communications with stated that the requests for review were being made on behalf of D/CIA Brennan. On 9 January 2014, called CIC alerting to a forthcoming "D/CIA tasking". tasked by email on the morning of 10 January 2014, requesting that the team provide contained in the folder of RDINet for the period 1 March 2009 to 31 December 2013. replied to the email, stating that the D/CIA wanted the results of the review that afternoon. provided a response in the form of an Excel spreadsheet on the afternoon of 10 January 2014. Following receipt of this information, emailed and stated that the D/CIA had requested for the same folder and requested a response by Monday, 13 January 2014. On 13 January, provided with an Excel spreadsheet of the requested On the afternoon of 13 January 2014, tasked with determining the provenance of the documents contained in the aforementioned folder. This task was not completed, as D/CIA Brennan directed that no further work be performed by at a meeting on 14 January 2014.

35. ~~(U//FOUO)~~ Despite representations by CIC that D/CIA Brennan directed the aforementioned taskings to OIG did not find evidence to support any such direction.

36. ~~(U//FOUO)~~ Due to conflicting information obtained by OIG through the course of the investigation, OIG could not determine whether any of D/CIA Brennan's senior staff, much less the D/CIA himself, approved any of the taskings made to In mentioned consulting with and and informing them that would be tasking to determine if the documents were accessed by SSCI users. Neither nor recalled approving any tasking, and OIG did not identify documentary evidence confirming any approvals.

37. ~~(U//FOUO)~~ D/CIA Brennan told OIG that he first learned of the concerns regarding documents on RDINet from on the evening 9 January 2014. D/CIA Brennan stated that he recalled referring to a review of but that he did not recall if explained how anyone knew the location of the documents. Subsequently, D/CIA Brennan spoke to on 10 and 11 January 2014. According to D/CIA Brennan tasked to "use whatever means necessary" to find out how the documents had ended up on the SSCI shared drive. D/CIA Brennan told OIG that he only asked "are we sure" that the documents were CIA documents and that he wanted to better understand the RDINet system architecture.

38. (U//~~FOUO~~) OIG presented D/CIA Brennan with an excerpt from the "MFR" document found on [redacted] D/CIA Brennan told OIG that there appeared to be a difference in emphasis between what he had told [redacted] and what [redacted] documented. In response to whether he told [redacted] to proceed by "whatever means necessary," D/CIA Brennan stated that he would never use those words and had not stated that to [redacted] D/CIA Brennan further stated that he was only interested in gaining knowledge of the system because he was unsure if it was a closed system. D/CIA Brennan stated that he had "tremendous respect" for [redacted] and added that he counted on [redacted] action to be consistent with legal authority. D/CIA Brennan reiterated that he had understood that CIA documents were found via [redacted] D/CIA Brennan stated that he wanted to know how the documents got to the SSCI side but did not direct anyone to review SSCI systems.

39. (U//~~FOUO~~) A meeting was held in the Director's conference room in the afternoon of 14 January 2014, attended by D/CIA Brennan, [redacted] CIC), Neal Higgins (Chief/Office of Congressional Affairs), [redacted] Executive Director Meroe Park, and others. At this meeting, D/CIA Brennan expressed surprise and concern at the presence of CIC officers. Several witnesses told OIG that D/CIA Brennan was upset that CIC had been engaged in the inquiry, and was concerned about the optic of the counterintelligence arm of the Agency investigating the activity of SSCI staffers. D/CIA Brennan stated he was surprised at the work that had already been performed, and explicitly told everyone at the meeting not to do anything else on the "tech or forensic side." D/CIA Brennan told OIG that he did not task the [redacted] review, and that there should not have been any other work performed after the meeting on the 14 January 2014. D/CIA Brennan confirmed with OIG that he was surprised when he learned CIC [redacted] was involved in the review.

(U) Office of Security Cyber Blue Team Review

40. (U//~~FOUO~~) During the meeting on 14 January, D/CIA Brennan gave the order to "stand down" on any further reviews until he could brief the SSCI on the Agency's concerns and the actions taken to date. On 15 January, D/CIA Brennan briefed the SSCI and proposed a joint review between the Agency and SSCI Security [redacted] D/CIA Brennan stated that he did not think that Chairman Feinstein explicitly agreed to a joint review that day, but did not explicitly say no or dismiss the conversation. D/CIA Brennan thought that Chairman Feinstein wanted to talk to [redacted] about it and consider the idea further. D/CIA Brennan stated that he did not task anything after this meeting with the SSCI, and that it should have been abundantly clear after the meeting on 14 January in his conference room that all work should have stopped.

41. (U//~~FOUO~~) Between 16 and 17 January 2014, the CIA Office of Security Cyber Blue Team[9] conducted a review of the RDINet [redacted] in [redacted] holdings and produced

[9] (U//~~FOUO~~) The Cyber Blue Team, established in February 2013, identifies vulnerabilities and risks, quantifies impacts to make educated decisions, and partners with other organizations in order to mitigate risks, among other duties.

a report dated 17 January 2014. Office of Security, told OIG that first became aware of the SSCI events on 15 January 2014, when contacted at home to inquire what it would take to conduct a security review. OIG confirmed that was not present at the 14 January 2014 meeting with D/CIA Brennan, and was not aware of the standdown order. stated that spoke to who explained to that SSCI staff accessed data they were not authorized to access. stated that spoke to on 15 January 2014, and that was planning to work with on a joint security review of the RDINet. On 16 January 2014, emailed to request concurrence on the plan of action developed by the Office of Security. Also on 16 January, received an email from stating that they were on "stand down" for a joint security review. On 17 January 2014, responded to request for concurrence "…there has been a new development" and requested, "If you can come to the Director's Office around 8am that would be ideal." OIG did not find any response to request for concurrence.

42. (U//~~FOUO~~) sent an email to Higgins and copied on 16 January 2014 and stated that SSCI Chairman Feinstein would be sending a letter to the D/CIA the following day requesting that no forensic examination of the SSCI "network" proceed. On 17 January 2014, Chairman Feinstein wrote to D/CIA Brennan and requested suspension of access to the computers and networks used by the SSCI and any forensic investigation planned by the CIA. Chairman Feinstein explicitly stated in the letter that until she could consider the matter further, D/CIA Brennan did not have her agreement for any investigative activity.

43. (U//~~FOUO~~) told OIG that on 16 January instructed the Cyber Blue Team to review the RDINet stated that did not seek approval because it was CIA information on a CIA network. further stated that this was a normal function for the Cyber Blue Team, capable of performing such a review. stated that did not feel that was out of coordination with CIA leadership at any time. On 16 January 2014 emailed and advised that the SSCI Chairman was drafting a letter to the Director of the CIA requesting to stop the entire plan of action for the joint review. described the "full plan of action" to OIG as the imaging of RDINet and a full forensic review and stated that interpreted this as a request to stop the joint forensic investigation. did not believe that the request applied to the review of or that the Cyber Blue Team review was akin to forensic activity.

44. ~~(S//NF)~~ On 17 January, the Cyber Blue Team met with to review the forensic generated by the SSCI staff, including reconstructed emails between SSCI staff on the SSCI side of RDINet. The Cyber Blue Team Report, detailed the team's evaluation of RDINet system data surrounding the documents in question. The report stated that a "Congressional user" was able to navigate directly to a "shared directory" and access documents never intended for dissemination to "Congressional users." The report stated that the user first accessed the directory on 9 November 2010, and copied the data contained

within to another shared directory. The report detailed further activity performed by a "Congressional user" on 24 June 2011 including copy/paste, keyword searches, and communication between "Congressional users" that directed them to review specific documents. As mentioned previously, OIG did not investigate the activity of the SSCI staff.

(U) Department of Justice Crimes Report

45. (U//~~FOUO~~) On 7 February 2014, then Acting General Counsel [redacted] sent the Department of Justice a Crimes Report (Exhibit E) that detailed a "limited security investigation." [redacted] wrote that a search tool installed on the system in question had a vulnerability that was exploited by SSCI staff members to view and retrieve documents on a part of the system to which they did not have access. Further, [redacted] explained that the file path to a document discovered while using the search tool could be copied and pasted into a browser access bar as a URL, which would give the user access to that document. The explanation stated that the user could bring a copy of the document across the system's firewall and paste it into a folder on the other side of that firewall. [redacted] wrote that the information made available to [redacted] indicated that a "non-employee" copied a URL, pasted it into the browser's access bar, and accessed the document, repeating this process numerous times. [redacted] told OIG that information provided by [redacted] was the sole source of information for the 7 February 2014 report.

46. (U//~~FOUO~~) OIG did not identify a factual basis to support [redacted] Department of Justice Crimes Report. OIG found tha[redacted] had been provided inaccurate information on which the report was based.

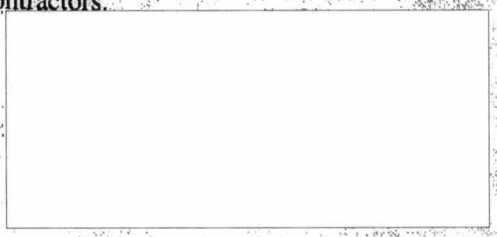
47. (U//~~FOUO~~) [redacted] told OIG that the information [redacted] provided to [redacted] was predicated on the Cyber Blue Team Report that stated that a Congressional user was able to navigate directly to a shared directory not intended for access to Congressional users. However, the Cyber Blue Team report did not identify the vulnerability stated in [redacted] letter as the source of the documents. The source of the information cited by [redacted] was information provided to [redacted] orally by [redacted] was unable to verify the accuracy of the information provided by [redacted] or to review [redacted] legal conclusions regarding the authority to view the SSCI shared drive because he was recused from matters relating to RDI, including the Cyber Blue Team Report. In fact, [redacted] told OIG that he did not read the Cyber Blue Team report a[redacted] was informed that the report contained details of SSCI communication, which made [redacted] wary.

V. (U) DOJ COORDINATION

48. (U//~~FOUO~~) On 3 February 2014, Title 50 U.S.C. § 3517, OIG reported the matter of potential CIA officer violations of Titles 18 USC § 1030 (Fraud and Related Activity in Connection with Computers) and 2511 (Authorization for Interception of Wire, Oral, or Electronic Communications) to the Department of Justice. On 8 July 2014, DOJ wrote to inform the OIG that DOJ had completed its review of the allegations and had no prosecutorial interest.

VI. (U) PRIVACY ACT AND FREEDOM OF INFORMATION ACT NOTICE

49. (U//FOUO) This report is the property of the Office of Inspector General and is for ~~OFFICIAL USE ONLY~~. Appropriate safeguards should be provided for the report and access should be limited to CIA officials who have a need-to-know. Public disclosure is determined by the Freedom of Information Act, Title 5, U.S.C. 552, and the Privacy Act, Title 5, U.S.C. 552a. The report may not be disclosed outside the CIA without prior written approval of the Office of Inspector General, including distribution to contractors.



VII. (U) EXHIBITS

A. (U) Personnel background descriptions.

B. (U) Conceptual diagram of RDINet Architecture, undated.

C. (U) Letters comprising a Memorandum of Understanding and Standard Operating Procedures, various dates.

a. (U) Memorandum of Understanding (*Agency author*), Senate Select Committee on Intelligence's Review of CIA's Detention and Interrogation Program, dated 28 May 2009.

b. (U) Letter from Senate Select Committee on Intelligence (SSCI) Chairman Dianne Feinstein and Vice Chairman Christopher Bond to then Director, Central Intelligence Agency Leon Panetta, dated 2 June 2009.

c. (U) Letter from then [redacted] to SSCI [redacted] and then [redacted] dated 8 June 2009.

d. (U) Letter from then Director, Central Intelligence Agency Leon Panetta to SSCI Chairman Feinstein, dated 12 June 2009.

e. (U) Standard Operating Procedures for SSCI Review (*author unknown*), undated.

D. (U) Other Related RDINet Events.

E. (U) [redacted] Crimes Report to the Department of Justice, untitled, dated 7 February 2014.

F. (U//~~FOUO~~) [redacted] document, titled *"Memorandum for the Record re: partial timeline of events surrounding discovery of SRT documents on RDI NET,"* dated 17-27 January 2014.

EXHIBIT A

(U) Personnel Background Descriptions

(U) **John Brennan.** Current Director of the Central Intelligence Agency since 8 March 2013.

(U) Former Acting General Counsel for the CIA

~~(C//NF)~~

~~(C//NF)~~

(U) **Neal Higgins (SIS).** The Chief of the Office of Congressional Affairs from June 2013 through the present who reported to the D/CIA and Deputy D/CIA.

(U)

~~(C//NF)~~

~~(C//NF)~~

(U)

~~(C//NF)~~

(U)

(U) ***Leon Panetta.*** *Former Director of the Central Intelligence Agency from February 2009* through June 2011. Panetta negotiated the terms of the RDI review with SSCI Chairman Feinstein.

(U) **Meroe Park (SIS).** Current Executive Director of the CIA since May 2013. Reported to D/CIA and DD/CIA.

(U)

(U)

(U)

(U)

(U)

EXHIBIT C (a)

(U) Memorandum of Understanding (*Agency author*), Senate Select Committee on Intelligence's Review of CIA's Detention and Interrogation Program, dated 28 May 2009.

Memorandum of Understanding
Senate Select Committee on Intelligence's Review of
CIA's Detention and Interrogation Program[1]

28 May 2009

1. (S) On 26 March 2009, the Senate Select Committee on Intelligence (SSCI) informed the Central Intelligence Agency (CIA or Agency) that it plans to conduct a thorough review of the CIA's detention and interrogation program. Included with the SSCI notification were detailed terms of reference and a document request. It is CIA's estimation that compliance with SSCI's requests will involve making available millions of highly sensitive and compartmented Agency responsive documents.

2. (S) As SSCI is aware, in order to further safeguard and compartmentalize intelligence sources, methods, personnel, and liaison relationships, CIA planned on redacting the names of our officers, cryptonyms, pseudonyms, liaison provided intelligence, information originated from other US government organizations, and the identity of black-site locations. SSCI informed the Agency that this very information was critical to a number of SSCI terms of reference and SSCI's overall review. Accordingly, SSCI advised that they were prepared to subpoena the information underlying these proposed redactions.

3. (U//FOUO) In order to avoid protracted litigation over subpoenas and in the spirit of cooperation, CIA has agreed to provide in unredacted form the above-referenced information that we previously sought to redact, under the following conditions:

A. (U//FOUO) Consistent with obligations set forth by Executive Order and Agency policy, CIA will provide responsive information to the minimum number of people who have the requisite need-to-know the information to perform the review. Accordingly, pursuant to discussions between SSCI and CIA about SSCI's anticipated staffing requirements, CIA will afford up to 10 SSCI personnel access to unredacted responsive information.

[1] This Memorandum of Understanding relates to responsive documents regarding the SSCI review. As the SSCI review proceeds, additional MOUs may be required to establish agreed upon procedures for non-documentary aspects of the review.

B. (C) CIA will make all responsive information available at a secure Agency electronic Reading Room facility which will permit SSCI personnel electronic search, filing, and print capability.

C. (C) All notes, documents, draft and final recommendations, reports, and other materials generated by SSCI must be prepared and stored in the Reading Room on the CIA approved stand-alone computer system provided. A specially designed share-drive will be provided on the Agency's stand-alone network. As SSCI requires, the share-drive can be segregated with only SSCI access and walled-off CIA IT administrators, except as otherwise authorized by SSCI. CIA will also provide SSCI with lockable cabinets and safes, as required. No outside computer systems or electronics will be authorized to be brought into the Reading Room.

D. (U//FOUO) No CIA generated classified information may be removed from the Reading Room.

E. (S) Should SSCI personnel request to remove any SSCI generated notes, documents, draft and final recommendations, reports, or other materials, CIA will perform a classification review and will redact the above-referenced categories of information from the materials. SSCI will be mindful of the fact that classification review is a careful process and thus requires sufficient time to perform accurately. Accordingly, SSCI will seek classification review at the earliest possible time and CIA will endeavor to expedite all such reviews. SSCI and CIA will work out further storage arrangements of any redacted, though likely still classified, materials produced as a result of the above-referenced classification/redaction review.

F. (U//FOUO) Should SSCI prepare any notes, documents, draft and final recommendations, reports, or other materials outside of the secure Reading Room based on information accessed in the Reading Room, all such materials must be prepared and stored on CIA approved TS//SCI systems and carry the highest classification of any of the underlying source materials. To the extent that SSCI desires any such materials to be produced outside of the approved TS//SCI system – to include publicly – CIA will conduct a classification review and will redact the appropriate information from the materials. Again, as noted above, SSCI will be mindful of the timing of such classification/redaction reviews.

G. (U//FOUO) The Reading Room will be available from 0700 to 1900 hours, official government business days, Monday through Friday. If SSCI requires additional time or weekend work is required,

arrangements must be made with sufficient advance notice to CIA, ideally with no less than 24 hours notice.

H. (U//FOUO) In order to avoid any confusion about the scope and nature of any future SSCI requests related to this review, SSCI will memorialize all requests in writing and CIA will respond in writing.

I. (U//FOUO) All SSCI personnel will be required to receive and acknowledge receipt of a CIA security briefing prior to beginning the review and will be required to review and sign a standard Sensitive Compartmented Information (SCI) non-disclosure agreement relating to classified information obligations.

J. (S) CIA expects that the responsive materials will contain information that has been the subject of previous unauthorized disclosures. Due to SSCI's access to this classified official US government information SSCI personnel will be in a position to either confirm or deny the accuracy of those unauthorized disclosures. Such confirmation or denial would itself constitute an unauthorized disclosure and would violate this agreement and the non-disclosure agreement.

4. (S) SSCI personnel understand by their acknowledgement below and through execution of their non-disclosure agreement that the responsive information will be highly classified, compartmented, and is extremely sensitive in nature. Any disclosure, whether intentional or inadvertent, to unauthorized individuals – including TS//SCI cleared but not compartment cleared individuals – is reasonably likely to cause exceptionally grave damage to national security. CIA anticipates that such disclosures could likely physically harm officers and their families as well as could seriously harm otherwise cooperative liaison relationships that provide critical force-multiplier capabilities to counterterrorism operations. Accordingly, SSCI will make all diligent efforts to properly safeguard this information.

_____ _____

SSCI Officer Date

_____ _____

Central Intelligence Agency Date

EXHIBIT C (b)

(U) Letter from Senate Select Committee on Intelligence (SSCI) Chairman Dianne Feinstein and Vice Chairman Christopher Bond to then Director, Central Intelligence Agency Leon Panetta, dated 2 June 2009.

SECRET

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510-6475

June 2, 2009

The Honorable Leon Panetta
Director
Central Intelligence Agency
Washington, D.C. 20505

Dear Director Panetta:

In a letter dated March 26, 2009, the Senate Select Committee on Intelligence (the Committee) informed the Central Intelligence Agency (CIA) of its intention to conduct a thorough review of the CIA's detention and interrogation program. The letter included terms of reference approved by the Committee, as well as a document request.

To conduct our work in a comprehensive and timely matter, the Committee requires access to unredacted materials that will include the names of non-supervisory CIA officers, liaison partners, black-site locations, or contain cryptonyms or pseudonyms. We appreciate the CIA's concern over the sensitivity of this information. Our staff has had numerous discussions with Agency officials to identify appropriate procedures by which we can obtain the information needed for the study in a way that meets your security requirements. We agree that the Committee, including its staff, will conduct the study of CIA's detention and interrogation program under the following procedures and understandings:

1. Pursuant to discussions between the Committee and CIA about anticipated staffing requirements, the CIA will provide all Members of the Committee and up to 15 Committee staff (in addition to our staff directors, deputy staff directors, and counsel) with access to unredacted responsive information. In addition, additional cleared staff may be given access to small portions of the unredacted information for the purpose of reviewing specific documents or conducting reviews of individual detainees. These Committee staff have or will have signed standard Sensitive Compartmented Information non-disclosure agreements for classified information in the [redacted] compartment.

2. CIA will make unredacted responsive operational files, as that term is defined in Section 701(b) of the National Security Act of 1947 (50 U.S.C. 431(b)), available at a secure Agency electronic Reading Room facility (Reading Room) which will permit Committee staff electronic search, sort, filing, and print capability.

3. If responsive documents other than those contained in operational files identify the names of non-supervisory CIA officers, liaison partners, or black-site locations, or contain cryptonyms or pseudonyms, CIA will provide unredacted copies of those documents at the Reading Room.

4. Responsive documents other than those contained in operational files that do not identify the names of non-supervisory CIA officers, liaison partners, or black-site locations, or contain cryptonyms or pseudonyms will be made available to the Committee in the Committee's Sensitive Compartmented Information Facility (SCIF), unless other arrangements are made.

5. CIA will provide a stand-alone computer system in the Reading Room with a network drive for Committee staff and Members. This network drive will be segregated from CIA networks to allow access only to Committee staff and Members. The only CIA employees or contractors with access to this computer system will be CIA information technology personnel who will not be permitted to copy or otherwise share information from the system with other personnel, except as otherwise authorized by the Committee.

6. Any documents generated on the network drive referenced in paragraph 5, as well as any other notes, documents, draft and final recommendations, reports or other materials generated by Committee staff or Members, are the property of the Committee and will be kept at the Reading Room solely for secure safekeeping and ease of reference. These documents remain congressional records in their entirety and disposition and control over these records, even after the completion of the Committee's review, lies exclusively with the Committee. As such, these records are not CIA records under the Freedom of Information Act or any other law. The CIA may not

integrate these records into its records filing systems, and may not disseminate or copy them, or use them for any purpose without the prior written authorization of the Committee. The CIA will return the records to the Committee immediately upon request in a manner consistent with paragraph 9. If the CIA receives any request or demand for access to these records from outside the CIA under the Freedom of Information Act or any other authority, the CIA will immediately notify the Committee and will respond to the request or demand based upon the understanding that these are congressional, not CIA, records.

7. CIA will provide the Committee with lockable cabinets and safes, as required, in the Reading Room.

8. If Committee staff identifies CIA-generated documents or materials made available in the Reading Room that staff would like to have available in the Committee SCIF, the Committee will request redacted versions of those documents or materials in writing. Committee staff will not remove such CIA-generated documents or materials from the electronic Reading Room facility without the agreement of CIA.

9. To the extent Committee staff seeks to remove from the Reading Room any notes, documents, draft and final recommendations, reports or other materials generated by Committee Members or staff, Committee staff will ensure that those notes, documents, draft and final recommendations, reports or other materials do not identify the names of non-supervisory CIA officers, liaison partners, or black-site locations, or contain cryptonyms or pseudonyms. If those documents contain such information, Committee staff will request that CIA conduct a classification review to redact the above-referenced categories of information from the materials or replace such information with alternative code names as determined jointly by the Committee and the CIA.

Any document or other material removed from the reading room pursuant to paragraphs 8, 9, or 10 will be stored in the Committee SCIF or transferred and stored on Committee TS//SCI systems, under Committee security procedures.

10. Any notes, documents, draft and final recommendations, reports or other materials prepared by Committee Members or Staff based on information accessed in the Reading Room will be prepared and stored on TS//SCI systems. Such materials will carry the highest classification of any of the underlying source materials. If the Committee seeks to produce a document that carries a different classification than the underlying source material, the Committee will submit that document to CIA, or if appropriate to the DNI, for classification review and, if necessary, redaction.

11. The Reading Room will be available from 0700 to 1900 hours, official government business days, Monday through Friday. If Committee staff requires additional time or weekend work is required, Committee staff will make arrangements with CIA personnel with as much advance notice as possible. .

12. The Committee will memorialize any requests for documents or information in writing and CIA will respond to those requests in writing.

13. All Committee staff granted access to the Reading Room shall receive and acknowledge receipt of a CIA security briefing prior to reviewing CIA documents at the Reading Room.

We anticipate that agreement to these conditions will address your concerns about Committee access to unredacted materials responsive to the Committee's document request. We look forward to immediate staff access to those materials.

In addition, we expect that the discussions and agreements over access to the study information are a matter restricted to the Congress and the Executive branch. As such, neither this letter nor derivative documents may be provided or presented to CIA's liaison partners.

Sincerely,

Dianne Feinstein
Chairman

Christopher S. Bond
Vice Chairman

EXHIBIT C (c)

(U) Letter from then [redacted] to SSCI [redacted] and then [redacted] dated 8 June 2009.

8 June 2009

TO:

FROM:

1. In reference to our discussion last week, we obviously differ on a few issues, but only a few. I would like to engage in an informal dialogue with your office in an effort to try to resolve these issues. Nothing in our dialogue should be considered the official position of the Agency until such time as you receive it in an official letter from our Director. For now, this is an informal discussion between us. I have chosen to put this in writing so that you have something in front of you to work with, not notes from a discussion that may or may not convey our position accurately. I think we will both agree that time is of the essence and I have no plans to draw this out in a lengthy dialogue. I would like to come up with an agreement or an acknowledgement that we are at an impasse, no later than Friday of this week (12 Jun), preferably sooner, if possible.

2. From our conference call last week, it was obvious that the most important issue appeared to be the following passage from paragraph three of our Director's 4 Jun 2009 letter:

"First, given that we will be providing the Committee with full, un-redacted access to millions of our most sensitive operational materials, we will review the notes, draft, and final reports, and other material generated from the Committee's review of the materials – **wherever prepared**- prior to removing this material from the Reading Room or **SSCI secure spaces**."

3. From our discussion, the terms of most concern to the SSCI were, "wherever prepared" and "or SSCI secure spaces." For us, the heart of this issue rests with the draft and your final report. That is the primary item that will be created outside of the Reading Room and likely to leave SSCI secure spaces. I noticed in the letter from Senator Feinstein dated 2 Jun 2009, there was no provision for allowing the CIA to review the final SSCI report prior to publication. So I guess our first question is: Does the SSCI plan to allow the CIA to review the SSCI final report before publication? The answer to this question is important to us and goes a long way in helping us address paragraph three of the D/CIA's letter.

4. Our position is this, we are giving the SSCI unprecedented access to our operational material We are aware of all of the previous studies you have cited as a precedent; however, at no time has CIA ever provided the SSCI with the volume of unredacted operational material as we have agreed to do in this case. Exposure of the names of CIA personnel involved in detentions and interrogations carries considerable costs to our officers professionally and personally. It is something we are taking very seriously. Officers who have had their names exposed in the press have had their lives impacted significantly through constant inquiries from the press, threats, phone calls from

international organizations, and limitations on travel. Additionally, and most significantly, their identities are now known to Islamic terrorists bent on revenge. With that in mind, we believe that it is appropriate to review documents regardless of where they are prepared before publication to ensure that it excludes the names of our officers. By the very nature of possessing a security clearance, we each bear the responsibility of protecting classified information; but, at the end of the day, it is the responsibility of CIA to protect its officers from potential harm.

5. Similarly, our relationships with foreign liaison services and agreements that we make with them are also of concern to us. In some instances, foreign liaison services have shared information with us and agreed to take action on things that they have not even discussed with their own governments. Additionally, we have agreements with some liaison partners that specifically prohibit the release of intelligence information outside our Executive Branch of government. If any of this information becomes public, it erodes our ability to do business with these services and they are subsequently reluctant to do things for us and share information with us. This too, is why we feel it is necessary to review a draft of your final report.

6. We realize that some issues involving liaison services may be directly relevant to the Terms of Reference and of importance to the conclusions and recommendations of your final report. We do not wish to hinder or change this, but we do expect you to work with us to convey what you wish to convey while at the same time protecting our relationship with our liaison partners. Perhaps not identifying the specific country being referenced and rewording intelligence provided by foreign liaison services so that it still conveys your message while distorting where the information may have derived from may be the answer. Again, our intent is not to change the meaning or tone of your report, just ensure that it is done in a way that protects our liaison equities. We would expect that both of us would be in agreement on this issue and partner with each other to ensure that you can convey whatever you wish and we can ensure that our liaison equities are protected.

7. In regard to our redaction of third Agency information, we will simply draft a letter from our Director informing the other agencies that we are providing the information to you. Another solution may be to have the DNI draft a letter to the USG Agencies. The main point is, we can resolve this issue without further discussion or debate.

8. In regard to the issue of notes leaving the Reading Room, I'm a little puzzled by this. Any notes that you take in the Reading Room are subject to review by our redactors if you want to remove them. If our building is one stop of several, and you have notes from previous meetings, then perhaps you can leave them in your vehicle or take other simple practical measures to avoid commingling your notes. If you are taking notes relative to issues not pertinent to this review while in the Reading Room, perhaps the solution is for us to remove all non-relevant material from the Reading Room and make it available at OCA spaces.

9. I think we are all in agreement on the computer issue. In a nutshell, you will have a walled off hard drive on our network. No CIA personnel with the exception IT support will have access to the hard drive. The only reason for IT access to the hard drive is for IT maintenance and support. This includes adding material to your hard drive for your review. The SSCI retains ownership of anything created on this drive, it is SSCI property and will be handled accordingly vis-à-vis the FOIA..

10. I think that covers the main issues of our discussion. Please get back to me as soon as possible. I am interested in coming to a resolution, one way or another, as quickly as we can. Please do not send me anything "official" until we can work this out offline.

Regards

[redacted]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

THE DIRECTOR
CENTRAL INTELLIGENCE AGENCY
WASHINGTON, D.C. 20505

JUN 12 2009

The Honorable Dianne Feinstein
Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

Dear Madam Chairman:

(U/FOUO) I have been informed by my staff that as of 10 June 2009, an agreement was reached between CIA and SSCI staff personnel regarding operating procedures for the SSCI review of material related to the CIA's detention and interrogation programs. My understanding is that your staff is now reviewing unredacted material responsive to your 26 March 2009 request.

(U/FOUO) We have established an electronic database that will contain records relevant to the Terms of Reference as we are able to collect them. Thus far, we have more than 100,000 pages of unredacted material available for review. Per your request, we are in the process of downloading materials related to Khalid Shaykh Mohammad into the database.

(U/FOUO) The purpose of these negotiations was to protect the equities of the Committee and the Agency. I am grateful for the cooperation of your staff in this important matter. We look forward to working with the Committee to assist in the completion of your review.

(U) An original of this letter is being sent to Vice Chairman Bond.

Sincerely,

Leon E. Panetta

EXHIBIT C (e)

(U) Standard Operating Procedures for SSCI Review (*author unknown*), undated.

STANDARD OPERATING PROCEDURES FOR SSCI REVIEW

1. The CIA will provide all Members of the Committee and up to 15 Committee staff (in addition to our staff director, deputy staff directors, and counsel) with access to unredacted responsive information. In addition, additional cleared staff may be given access to small portions of the unredacted information for the purpose of reviewing specific documents or conducting reviews of individual detainees. These Committee staff have or will have signed standard Sensitive Compartmented Information non-disclosure agreements for classified information in the [redacted]ompartment. (Ref A)

2. CIA will make unredacted responsive operational files, as that term is defined in Section 701(b) of the National Security Act of 1947 (50 USC 431(b)), available at a secure Agency electronic Reading Room facility which will permit Committee staff electronic search, sort, filing, and print capability. (Ref A)

3. If responsive documents other than those contained in the operational files identify the names of non-supervisory CIA officers, liaison partners, or black site locations, or contain cryptonyms, or pseudonyms, CIA will provide unredacted copies of those documents at the Reading Room. (Ref A)

4. Responsive documents other than those contained in operational files that do not identify the names of non-supervisory CIA officers, liaison partners, or black site locations, or contain cryptonyms or pseudonyms will be made available to the Committee in the Committee's Sensitive Compartmented Information Facility (SCIF), unless other arrangements are made. (Ref A)

5. CIA also recognizes the Committee's need to create work product on a walled-off network share-drive as discussed in paragraph 5 of your letter. Therefore, CIA access to the walled off network share drive will be limited to CIA information technology staff, except as authorized by the Committee or its staff. CIA would like to clarify, however, that unlike the walled-off network share drive, the stand alone network must be accessed by CIA staff assigned to this effort to perform a variety of tasks, including, for example, loading and organizing the raw responsive data requested by the Committee and review or redaction of material sought to be removed from the Reading Room. (Ref B)

6. Any documents generated on the network drive referenced in paragraph 5, as well as any other notes, documents, draft and final recommendations, reports, or other materials generated by the Committee staff or Members, are the property of the Committee and will be kept at the Reading Room solely for secure safekeeping and ease of reference. These documents remain congressional records in their entirety and disposition and control over these records, even after completion of the Committee's review, lies exclusively with the Committee. As such, these records are not CIA records under the Freedom of Information Act or any other

law. The CIA may not integrate these records into its records filing systems, and may not disseminate or copy them, or use them for any purpose without the prior written authorization of the Committee. The CIA will return the records to the Committee immediately upon request in a manner consistent with paragraph 11. If the CIA receives any request or demand for access to these records from outside the CIA under the Freedom of Information Act or any other authority, the CIA will immediately notify the Committee and will respond to the request or demand based upon the understanding that these are Congressional, not CIA, records. (Ref A)

7. CIA will provide the Committee with lockable cabinets and safes, as required, in the Reading Room. (Ref A)

8. If Committee staff identifies CIA-generated documents or materials made available in the Reading Room that staff would like to have available in the Committee SCIF, the Committee will request redacted versions of those documents or materials in writing. Committee staff will not remove such CIA-generated documents or materials from the electronic Reading Room facility without the agreement of CIA. (Ref A)

9. CIA intent is to keep all of the operational cables at the Reading Room. If Members or staff wish to remove any of the operational cables from the Reading Room, we will consider those requests on a case by case basis, and we will work to accommodate your requirements. (Ref B)

10. SSCI Members or staff will not remove from the Reading Room any notes, work product, operational files, or other documents that contain unredacted names or pseudonyms of non-supervisory CIA personnel; locations of detention facilities or cryptonyms or information directly identifying such sites, or names of individual assets, contacts, foreign government officials, or foreign intelligence officials or services. (Ref C)

11. Prior to leaving the Reading Room with any materials containing operational information covered in the preceding paragraph or references to such information, Committee staff will provide those materials to CIA personnel for redaction or replacement with a designator or for CIA's review of the Committee staff redaction or replacement. CIA's review of Committee information for redaction and replacement will be "walled off" from all other CIA activities. (Ref C)

12. It will not be the Committee's general practice to recreate such sensitive information when writing memoranda or report materials in the Committee's office spaces or other locations. (Ref C)

13. The Committee will not provide information gained from the review of materials at the Reading Room to anyone not a Member or cleared staffer of the Committee prior to providing that information to the CIA for a classification review. No

information resulting from the Committee's study will be publicly released prior to determination by the CIA, or if applicable the DNI, that such information is unclassified. (Ref C)

14. Any notes, documents, draft and final recommendations, reports or other materials prepared by Committee members or staff based on information accessed in the Reading Room will be prepared and stored on TS/SCI systems. Such materials will carry the highest classification of any of the underlying source materials. If the Committee seeks to produce a document that carries a different classification than the underlying source material, the Committee will submit that document to CIA, or if appropriate to the DNI, for classification review, and if necessary, redaction. (Ref A)

15. Except for materials stored at the Reading Room, notes and documents created by the Committee based on information provided at the Reading Room will be stored in the Committee's SCIF except during appropriate transit between secure facilities. (Ref C)

16. The Reading Room will be available from 0700 to 1900 hours, official government business days, Monday through Friday. If Committee staff requires additional time or weekend work is required, Committee staff will make arrangements with CIA personnel with as much advance notice as possible. (Ref A)

17. The Committee will memorialize any requests for documents or information in writing and CIA will respond to the requests in writing. (Ref A)

18. All Committee staff granted access to the Reading Room shall receive and acknowledge receipt of a CIA security briefing prior to reviewing CIA documents at the Reading Room. (Ref A)

REFERENCES

A. Letter from Senators Feinstein and Bond to D/CIA Panetta dated 2 Jun 2009
B. Letter from D/CIA Panetta to Senators Feinstein and Bond dated 4 Jun 2009
C. Memo from [redacted] and [redacted] to [redacted] dated 9 Jun 2009

(U) Other Related RDINet Events

1. (U//FOUO) The OIG learned of several historical incidents related to RDINet during the course of this investigation. The incidents were cited by multiple interviewees as demonstrating that SSCI users were previously aware of Agency monitoring of SSCI activity on RDINet.

2. (U//FOUO) In January 2010, the CIA RDI team removed 874 documents from the virtual Reading Room and an additional set of 52 documents on 11 May 2010. The CIA staff interviewed by the OIG stated that these documents were "Executive Privilege" documents that had been unintentionally comingled on the RDINet with documents intended for production to the SSCI. When it was discovered that these documents had been added to the virtual Reading Room in error, the RDI team removed the documents. On or about 11 May 2010, the RDI team informed SSCI that documents were removed from the virtual Reading Room. SSCI staffer sent an email to on 12 May 2010, stating that "Our understanding of the agreement we reached with you last year was that the computer systems on which the Committee would be working would only be accessed by CIA personnel for purely administrative, IT actions. CIA's actions in removing documents from our system are unequivocally not administrative." The RDI leadership then informed the relevant CIA employees that no further documents should be removed from the Reading Room prior to consulting with the SSCI staff.

3. (U//FOUO) In December 2009, the detected that a the SSCI staff In January 2010, the same individual also reported having a camera in the secure facility to the facility's gate guard but did not provide the camera for review. The individual was identified as on RDINet in November and December 2010. The matter was referred to the CIA Counterintelligence Center's Counterespionage Group (CEG), and the employee was removed from the team.

4. (U//FOUO) On 6 May 2010, a SSCI staffer requested from the Agency the ability to print a sensitive document from the RDINet. The SSCI staff member attempted to bypass the print restriction by CIC reviewed the incident and recommended removing the possibility of SSCI staffers utilizing but because the capability was it could not be removed or disabled. The RDI team discussed this issue with the SSCI staff and reminded them of the need for security of the sensitive documents.

5. (U//FOUO) In 2013, a number of detainee videos not provided to the SSCI by the CIA were requested by SSCI staff. The RDI review team evaluated the request and determined the videos to be outside of the scope of the SSCI review. According to the SSCI staffer asserted his request, saying he had a document that defined the location of the videos and that they were from responsive detainee sites. The staffer presented a hardcopy spreadsheet that recognized as a working copy produced by the SRT team. confirmed with the SRT analysts that the requested videos were not responsive, and that all of the responsive videos from the spreadsheet had already been provided. The

RDI IT team reviewed ways the SSCI staff could have accessed the spreadsheet and hypothesized that there may have been a Google search appliance vulnerability. The team discovered that the Google search appliance was capable of searching both the SSCI side as well as the RDI team's side of the Spartan Gate database. The results of Google searches showed documents from both the SSCI and Agency sides of RDINet and included a link to cached versions of the documents. When clicked, the cache link presented the text of the document in question. The RDI IT Team implemented a fix for this vulnerability in April 2013. The CIA requested that the document be destroyed in both paper and electronic format and the SSCI staffer agreed to do so.

CENTRAL INTELLIGENCE AGENCY
Washington, D.C. 20505

General Counsel

7 February 2014

The Honorable Eric Holder
Attorney General
Department of Justice
Washington, D.C. 20530

ATTENTION: Mr. George Toscas
Deputy Assistant Attorney General
National Security Division

Re: Crimes Referral

Dear Mr. Attorney General:

(U//FOUO) I am writing to you pursuant to Section 1.6(b) of Executive Order 12333, as amended, and Sections VI.B, VII.A.4, and VIII.A of the 1995 Crimes Reporting Memorandum of Understanding between the Department of Justice and the Intelligence Community pertaining to the reporting of information concerning federal crimes ("the MOU").

(U//FOUO) The Central Intelligence Agency (CIA) has information relating to possible violations of a specified Federal criminal law by one or more individuals not employed by the CIA. Since the computer system on which these possible violations occurred contains highly classified information, I am reporting in accordance the procedure set forth in Section VIII.C of the MOU.

(U//FOUO) The following information provides a reasonable basis to conclude that a violation of 18 U.S.C. § 1030(a)(2)(B), a specified Federal criminal law, has occurred. This information derives from a limited security investigation that was suspended before completion; only a completed investigation would determine whether or not a violation occurred. There is a computer system or network ("system") located in a CIA facility. Certain non-employees have authorized access to a portion of that system. A "firewall" exists between the portion to which those non-employees have authorized access and the portion to which they do not have authorized access. There is a search tool on the system that allows the non-employees to conduct

The Honorable Eric Holder,

searches to retrieve documents on their portion of the system. That search tool had a security vulnerability, now remedied, that could be exploited to allow non-employees to breach the firewall and retrieve documents on the part of the system to which they were not authorized access. An incomplete audit indicates that at least one non-employee exploited that vulnerability to retrieve a number of CIA documents on the portion of the system to which he or she did not have authorized access.

(U//~~FOUO~~) The information made available to me indicates that in the November 2010 timeframe, the non-employee conducted a search that appeared intended to reach into part of the computer system to which the non-employee did not have authorized access. In such a circumstance, the system was designed to bring up on the workstation screen a page that advised the non-employee was not authorized to access that document. This page, however, had the security vulnerability that has since been discovered and remedied. The security vulnerability was that the page also contained a "URL" that indicated where the document was located on the system and if an individual copied the URL and pasted it into the browser's address bar, the individual could gain access to the document, copy it, bring that copy across the firewall, and paste it into a folder on his or her side of the firewall. The information made available to me indicates the non-employee copied the URL, pasted it directly into the browser's address bar, and accessed the document.

(U//~~FOUO~~) The information made available to me further indicates that this non-employee repeated this activity numerous times in order to access, copy, and bring across the firewall CIA documents to which he or she did not have authorized access. If the system worked as designed, on each occasion, the non-employee would have received on the workstation screen a page informing him or her that he or she did was not authorized to access the document. This non-employee copied all of these documents into a file or folder on the portion of the system to which he or she had authorized access. Thereafter, at least four other non-employees accessed and printed these CIA documents on multiple occasions. It is not clear whether any of these other four non-employees may also have exploited the security vulnerability.

The Honorable Eric Holder,

(U//~~FOUO~~) Some or all of the documents accessed by exploiting the security vulnerability contained the following banner:

(U//~~FOUO~~) This classified document was prepared by the CIA Director's Review Group for Rendition, Detention, and Interrogation (DRG-RDI) for DRG-RDI's internal discussion purposes and should not be used for any other purpose, nor may it be distributed without express permission from DRG-RDI or CIA's Office of General Counsel. This document contains classified information derived from sensitive sources and methods, which may include, but may not be limited to, HUMINT, SIGINT, intelligence assets, other US Government agencies, and/or foreign governments and liaison services, and must be handled accordingly. This document also contains material protected by the attorney-client and attorney work-product privileges. Furthermore, this document constitutes deliberative work product, protected by the deliberative-process privilege, and is not a final, conclusive, complete, or comprehensive analysis of DRG-RDI or CIA. Rather, it was created to suit the needs of DRG-RDI, in support of informing senior Agency officers about broad policy issues. While every effort was made to ensure this document's accuracy, it may contain inadvertent errors. For this reason, and because this document selectively summarizes, draws inferences from, or omits information from the sources it cites, it should not be relied upon by persons outside DRG-RDI.

(U//~~FOUO~~) At the request of the Director of the CIA, the CIA Inspector General (IG) opened a review into the actions of CIA employees who discovered the above information. On 30 January 2014, representatives of the IG discussed with the Criminal Division's Computer Crimes and Intellectual Property Section (CCIPS), information concerning possible violations of Title 18 U.S.C. §§ 1030 and 2511 by CIA employees. On 3 February 2014, the CIA IG's office issued crimes referral 2014-11718 to CCISP based in part on those discussions. The IG did not include in his crime referral any information regarding the potential criminal violation by the non-employees, deferring to the Agency to determine whether the information available met the standard to issue a crimes report on the non-employees.

(U//~~FOUO~~) As the Acting General Counsel, that determination was my responsibility under the MOU. As noted above, I have determined there is a reasonable basis to conclude

The Honorable Eric Holder,

that a violation of 18 U.S.C. § 1030(a)(2)(B), a specified Federal criminal law, has occurred.

Sincerely

[redacted]

Acting General Counsel

copy to: Inspector General

UNCLASSIFIED/DRAFT
ATTORNEY-CLIENT PRIVILEGED

January 15-27, 2014

Memorandum for the Record re: partial timeline of events surrounding discovery of SRT documents on RDI NET

The following is an outline, and does not purport to be complete.

By Jan. 9, 2014, I had developed reason to believe that the SSCI staff performing the RDI review had obtained unauthorized access to classified, draft, pre-decisional, privileged documents resident on the Agency "side" of RDI Net. I was aware of explicit admissions from staff that they "knew something" about the documents (including a comment made by staff member at Caroline Krass' confirmation hearing to the effect that he "have seen [the Agency's] real response" to the SSCI RDI Study), as well as public statements by members of the SSCI to the effect that they had seen the documents.[1] Moreover, I was reminded by my staff that there had once been a "hole" or breach in the firewall dividing the SSCI side from the CIA side of RDI Net (discovered in 2012). At that time, when confronted with a document that should not have been in their possession, SSCI staff members had assured me that they did not inappropriately access any other documents on the Agency side. By January 9, my staff had conducted a check of our logs that chronicle documents the Agency had appropriately provided to the SSCI and found no SRT documents referenced within them. As a result, I had good reason to believe that Committee staffs' 2012 assurance was a misrepresentation.

I am ultimately responsible for ensuring the security of RDI Net system—a CIA owned and operated system, located in a CIA facility and subject to CIA regulations and applicable US laws regarding classified information—and for maintaining the safety of sensitive CIA records placed upon it. As a consequence, I asked IT professionals within the Office of Detainee Affairs (ODA) to determine whether the SRT documents were present on the SSCI side of the system. In so doing, I carefully considered what was known to me regarding the Agency's historical representations to and agreements with the SSCI concerning the general principle of refraining from accessing the SSCI side of the system. Those representations included an explicit reservation of authority for Agency IT officers to access the SSCI side to address precisely these sorts of situations. I was aware that SSCI staff had been briefed on the fact that the Agency would conduct security monitoring of the system. I also was aware that Agency IT officers had repeatedly utilized this authority to confirm that documents had been appropriately placed on the SSCI side of the system, a practice that SSCI had knowledge of and fully and repeatedly consented to. I was mindful that Director Panetta, and others, had clearly stated to the SSCI that our respect for their substantive privacy did not mean that we were abandoning our right to administrative access or an audit capability to ensure the security of the system and to protect CIA information, the latter an obligation imposed by statute. As a consequence, I did not interpret any representation to SSCI as requiring that we turn a blind eye to possible violations of Agency regulations or federal law. To the contrary,

[1] SSCI referred to the documents as the "Panetta Review," but the Agency has historically referred to them as WCRs ("weekly case reports") or SRT (Strategic Review Team) documents.

my understanding from my first days with the Agency, when I was provided with briefings on the SSCI review process by Agency officers, including security officers, was that I have an affirmative obligation to take steps—including [redacted] of the system--to ensure the integrity of that system and to protect classified materials.

Perhaps most importantly, it was my understanding of agreements between the Committee and the Agency that restrictions on Agency access to the SSCI side were intended to preclude the Agency from conducting substantive reviews of the Committee's work product, not from conducting normal administrative and security-related functions. I ensured that this particular administrative action would be extremely narrow, limited to a simple identification of the presence of particular *CIA documents*, not SSCI materials. I explicitly directed that no content was to be read, altered, moved, or examined in any fashion. I gave explicit directions that the officers were to search only for the SRT documents. They were not to search for or access any other documents, nor read or review the SRT documents, but simply to determine whether they were present on the system. The review was purely in the manner of an audit, with no substantive review of any document or Committee work product.

Later that day, I was informed that our IT officers had determined the Agency's documents were indeed present on the SSCI side of the system. I immediately informed [redacted] and [redacted] We discussed next steps, and I informed them that we could take the inquiry into this matter one step further, by asking CIA's [redacted] —which, under the direction of CIC, [redacted] —to [redacted] regarding whether the documents had been accessed by SSCI staffers. They concurred, and I asked ODA to contac[redacted] to request the necessary support. Again, I gave specific direction that the effort was to be closely circumscribed, and should involve only the identified documents. No other documents were to be accessed or reviewed and, again, no substantive review of the SRT documents was to occur. That admonition was delivered via e-mail to [redacted]

On the same day [redacted] informed me that [redacted] had discussed this issue with the Director, and the Director had instructed that we needed to be "completely sure" that the documents on the SSCI side of the system were actually the SRT documents. I asked my colleague[redacted] to attempt to verify the nature of the documents, and [redacted] quickly reported tha[redacted] had looked at the first page of a handful of the documents and confirmed that they were the privileged, draft documents in question, the documents SSCI had not been authorized to receive. [redacted] nformed me that [redacted] did not read any of the documents, but merely looked at the front page format of a few to see if they possessed the same warning banner, draft designation, format, etc., as the SRT documents. I informed [redacted] of this confirmation.

Late in the afternoon of Jan. 10, 2014, I received a report of findings from [redacted] indicating that five SSCI staff members had accessed the documents, beginning in the fall of 2010 and concluding in the fall of 2012, about the time the "hole" in the RDI Net firewall had been discovered. The staff members had accessed the documents thousands

of times. I reported this finding to [redacted] and the DCIA. I advised the Director of the importance of determining the full facts surrounding this matter before discussing it with the Committee or the WH, and he directed me to pursue all available options to determine how the documents came to be on the SSCI side of the system, as a necessary predicate to any broader discussions. I noted for him that I did not run an investigative organization, but that I could ask the ODA team to try and explore how SSCI could have achieved access to the documents.

Saturday afternoon, Jan. 11, I took a call at home from the Director, who informed me that he had discussed the possible security breach with WH COS Denis McDonough. The Director reiterated his desire to inform the Hill of the breach as soon as possible, and emphasized that I was to use whatever means necessary to answer the question of how the documents arrived on the SSCI side of the system so that his communication with the Hill could occur. I viewed those instructions as authorizing me to gather the necessary Agency personnel and components who would normally be involved in such an effort. He also tasked me to generate a set of draft talking points for that meeting with Committee leadership. I cautioned that discussing this matter with the WH, at this stage, was problematic, as it could later be viewed as WH interference in a potential criminal investigation. He thanked me for my efforts, and reiterated that he wanted answers as soon as possible…meaning days, not weeks.

On the morning of Jan. 13, 2014, after informing elements of Agency leadership of the issue, I was called to a meeting chaired by the EXDIR. Also in attendance was [redacted] /CIC, [redacted], D/OPA, D/OCA, and others. [redacted] attended briefly. During the meeting I described the events to date and the Director's instructions. I indicated that neither I nor ODA had any capability to conduct the sort of forensic work necessary to answer the DCIA's question concerning the provenance of the SRT documents. [redacted] CIC explained how [redacted] would be able to perform the work. No one in attendance voiced any objection to [redacted] taking on the assignment; indeed, there were unanimous expressions of support for the proposition that the Agency needed to determine whether the documents had been intentionally taken or if there was some more innocent explanation for their presence on the SSCI side, prior to discussing the matter with the SSCI. I advised that the matter should be placed under the control of the Office of Security. I also stressed that this work should be done without reference to the content of any documents on the SSCI side; that no substantive review of any document had been performed, should not be performed, and need not be performed in order to conduct this [redacted] activity.

Later that evening, the aforementioned group met with the Director to discuss status of efforts to determine the provenance of the documents. Before we could begin a substantive discussion, the Director expressed irritation that CIC was involved in the effort, stating that the "optic" of CIC performing the [redacted] work was poor. Several attendees attempted to explain that [redacted] but the Director continued to focus on the "optics." I informed the Director of my view that the conduct in question could be criminal, and that the Agency—based solely on its current understanding, that unauthorized documents existed

on the SSCI side of the system and had been repeatedly accessed—had an obligation to answer the question of whether there had been a security violation or a potential violation of law that should be referred to the Department of Justice. Nevertheless, he ordered a "pause" in the [redacted] work being conducted by [redacted] and stated that it was necessary to consult with the WH on next steps. Moreover, he expressed his intention to discuss the matter with Committee leadership the next day.

I repeatedly counseled the Director, as well as [redacted] and D/OCA, that it was unwise to ask the WH for direction as to a possible criminal investigation. If the WH were to order the inquiry stopped, it could constitute an act in furtherance of obstruction of justice. At the least, it could be interpreted that way by Congressional critics and the press. Merely consulting with the WH would place the Director in a bad light, making it appear that he was politicizing a potential criminal matter. I also repeatedly counseled that informing Committee leadership of the potential breach at this stage would result in the potential targets of the investigation—SSCI staff—being informed of the investigation, and would permit them to "get their story straight" prior to being interviewed by Agency security officers or law enforcement, a practice that would not be viewed as appropriate by criminal investigators. I again recommended that the matter be placed under the auspices of the Office of Security and that [redacted]OS determine next steps, be they to continue the review or to refer the matter to the Department of Justice.

Following these events, I received an e-mail on AIN from [redacted] praising my work, and asking me to come see the Director so he could tell me how much he appreciated my efforts. I attempted to decline, noting that it wasn't necessary, but [redacted] insisted.

At 5:30 on January 16, I was asked to come to the Director's office. The Director said he understood I was concerned about events relating to this matter. Referencing the meeting on the evening of January 13, he said he could come off as "brusque" but that he hoped he hadn't offended me. He went on to say this was a difficult matter, but he was the Director and had to make a decision about the proper way to proceed. He said he appreciated my advice, fully supported all my actions in this matter, and urged me to be proactive in coming to him with future concerns—directly if necessary, rather than through staff. I thanked him for his consideration in bringing me in, but noted that any discomfort I had concerning this matter was not related to his demeanor at the January 13 meeting, but rather stemmed from a concern that I had not adequately or with sufficient force conveyed what I perceived as the legal risks inherent in his chosen course of action.

He asked me what he should do going forward and I made three recommendations: Provide [redacted]OS with written instructions to carry out a review of this matter using all available means at her disposal, and to arrive at a recommendation "without fear or favor"; to refrain from further discussions with the WH until such time as the facts were known; and to contact FBI to let them know of the potential breach—noting that the facts are incomplete and that it could turn out to be a matter of little consequence—but to inform the Bureau of the actions that had been taken and to accept help in conducting the forensic work if offered. The Director thanked me and noted that these all seemed to be

good ideas, and that he would pursue them. I again thanked him for his thoughtfulness. The conversation was cordial throughout.

Addendum re Feinstein letter of January 23, 2014

I share a few thoughts about Sen. Feinstein's letter—in particular, it's most important implicit assertion, that the Agency is not permitted to access the SSCI side of the CIA system for purposes of security monitoring and to ensure the safety of classified materials.

That assertion is simply incorrect. Throughout the life of the SSCI review CIA has in fact performed security monitoring and exerted compliance control over RDI Net, including on the SSCI side of the system. The Agency monitors the entire system as it does all CIA systems, and SSCI awareness of this fact is reflected in the security warnings and disclaimers that SSCI staffers see as they access their side of the system. The security briefing provided to SSCI staffers makes it clear that such monitoring / was to be expected.

Of course, it must be so. After all, SSCI has never attempted to exert any sort of security protocols or monitoring over the system. To my knowledge, no SSCI security officer has ever accessed the system or requested permission to do so. If SSCI is right in claiming that CIA lacks the authority to maintain security of the system and its compliance with Agency regulations and applicable law, then we have created a system in which no one has that responsibility. Even the Director lacks the authority to establish a system for maintaining extremely sensitive, classified documents and exempt it from all security monitoring and compliance.

In point of fact, of course, DCIA Panetta did not purport to do so here. While SSCI asserted the right to complete hegemony over its side of the system, the Agency did not accept that demand. The Committee cannot establish otherwise by repeatedly citing its unacknowledged and unapproved assertion of complete control. I am told that like many issues of contention between the Agency and the Committee (such as the ultimate ownership of the documents being provided to the SSCI, which the Committee still claims should be given over for permanent storage on the Hill following conclusion of the Review) Agency leadership at the time chose to defer "open warfare" over the issue of security by not making it an explicit provision in letter exchanges between the Agency and Sen. Feinstein. But at no point did the Agency abdicate its responsibility to maintain security over the system—and my own view is that, in any event, it could not have lawfully done so.

Finally, and perhaps of greatest significance, the "stand alone" nature of the system was only important, as the letter from Sen. Feinstein explicitly admits, "because it was recognized to contain SSCI work product." The preliminary audit conducted in this instance, which took place because there was a reasonable basis to believe that a violation of regulation or law had occurred, did not involve the review of any work product. It was

solely focused on determining whether CIA documents—resident on a CIA owned and operated system, housed in a CIA facility and entrusted to CIA officers for management and security--which had not been authorized for passage to the Committee had been accessed by the SSCI staff. No substance was reviewed, no documents were moved or altered, and no substantive information was gained.

[redacted]