(U~~//FOUO~~) Final Report of the Rendition, Detention, and Interrogation Network Agency Accountability Board

I. (U) Scope of Review

(U~~//FOUO~~) The CIA Office of the Inspector General (OIG) on 30 January 2014 opened an investigation into potential unauthorized access to the Senate Select Committee on Intelligence (SSCI) shared drive portion of the Rendition, Detention, and Interrogation Network (RDINet) based on information derived from a special review conducted on 29 January 2014. The OIG on 3 February 2014 reported to the Department of Justice (DOJ) the matter of potential CIA officer violations of 18 U.S.C. §§ 1030 (Computer Fraud and Abuse Act) and 2511 (Wiretap Act). The DOJ on 8 July 2014 informed the OIG that the DOJ had no prosecutorial interest in the case and the OIG delivered its completed report to the Director of the Central Intelligence Agency (D/CIA) on 18 July 2014.

~~(C//NF)~~ The OIG Report concluded that Office of General Counsel (OGC) officers [redacted] and [redacted], Agency Information Technology (IT) [redacted] officers [redacted] and [redacted], and [redacted] improperly accessed the SSCI Majority Staff shared drive on RDINet. The OIG found the three IT officers also demonstrated a lack of candor during their first interviews with the OIG because they did not disclose actions they took on behalf of the two OGC officers.

(U~~//FOUO~~) The OIG investigated a crimes report filed by the Agency with the DOJ that reported that SSCI staff members may have improperly accessed Agency information on the RDINet. The OIG found 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.

(U~~//FOUO~~) The OIG also found that subsequent to a directive by the D/CIA to halt the Agency review of SSCI staff access to the

[redacted]

RDINet, [redacted] Security conducted a limited investigation of SSCI activities on the RDINet that included a keyword search of all, and review of some, e-mails of SSCI Majority staff members on that network.

(U~~//FOUO~~) The D/CIA on 6 August 2014 convened an Agency Accountability Board (the Board) in response to the OIG findings. The Board was commissioned to investigate the conduct of the five individuals referenced in the IG report and provide recommendations regarding both their individual accountability and any systemic CIA issues the Board might find. (A summary of the Board membership is found in Tab A.)

(U~~//AIUO~~) The Board held its first meeting on 21 August 2014 and completed its deliberations on 24 November 2014. The Board first sought to establish relevant facts concerning the incidents cited in the OIG report per Accountability Board guidance found in Agency Regulation 4-7. As a result, Board members reviewed the OIG report, OIG's Memoranda of Investigative Activity that summarize OIG interviews, written responses to the OIG report from the five named individuals, and other documents provided by individuals or used by the OIG to make its determinations. The Board also interviewed the five named individuals, the D/CIA, the Executive Director, [redacted] the Office of Security (OS), [redacted] the Counterintelligence Center (CIC), [redacted] OIG's investigative staff, the OIG attorney, and OIG officers who conducted the investigation.

(U~~//FOUO~~) This report represents the Board's summary, analysis, and recommendations based on relevant information that came before the Board and is not intended to be a definitive history of the RDI Network. The Board was directed to limit its investigation only to the conduct of Agency officers, not investigate the conduct of SSCI staff members.

A. (U) The RDI Network

(U~~//FOUO~~) The creation of the RDINet was ground-breaking in that it provided SSCI staff members with full, un-redacted access to millions of the Agency's most sensitive operational materials.

The Agency had to build an information system that enabled the review and release of these documents, provide a secure means to transfer the documents to SSCI staff members, and create electronic partitions to offer some protection of SSCI work product.

(U~~//FOUO~~) Most officers interviewed by the Board noted the unprecedented nature of RDINet with two branches of Government using a shared computer network system to distribute vast amounts of sensitive operational information. Regrettably, none of the documents reviewed by the Board contained guidance on procedures to be used in the event of a suspected security incident.

(U~~//FOUO~~) CIA Had Operational Responsibility for RDINet

(U~~//FOUO~~) The Board received a copy of the 8 February 2011 document *DRG-RDI/SSCIRG Handbook for File Reviews* that contains a summary of the RDINet program history. According to the *Handbook*, the SSCI on 26 March 2009 advised then-CIA Director Panetta that the Committee would conduct a thorough review of how the CIA created, operated, and maintained its detention and interrogation program. Director Panetta on 1 May 2009 issued a preservation order directing CIA personnel to save documents, information, records, and other materials related to CIA's detention and interrogation program. The authorized date range for any data under review to be possibly responsive was set as 11 September 2001 to 22 January 2009.

(U~~//FOUO~~) CIA established RDINet at its [redacted] Building facility in June 2009 to allow the Agency to review and release responsive RDI material to SSCI Staff members. At no time was any equipment associated with RDINet located on Senate property, nor was the equipment itself property of the Senate. The Agency used electronic protocols to provide SSCI staff members with access to specific documents located in a database and separate electronic shared drives were established for SSCI Majority and Minority staffs. SSCI staff could only access RDINet by being physically present in the [redacted] building. No remote access from SSCI offices was possible.

(U~~//FOUO~~) CIA Operated and Maintained RDINet

(U~~//FOUO~~) RDINet was operated by the CIA, maintained by CIA staff and contractor IT officers, and CIA staff officers oversaw the implementation of the system when they led what was designated as the Director's Review Group, the Office of Detainee Affairs, or the RDI Review Team.

(U~~//FOUO~~) In addition to the *Handbook*, the Board received Version 2.8 of the RDINet System Security Plan dated 29 August 2013 and a copy of a 15 June 2011 Statement of Work that covers activities of contractors who perform development work on Counter Terrorism Center document management systems that include RDINet.

(U~~//FOUO~~) Combined with the unsigned Memorandum of Understanding (MOU) (discussed under the *No Written Agreement Governed CIA Access to the SSCI Side of RDINet* section below), these four documents capture how the Agency managed the operation of RDINet. According to an overview in the Statement of Work, the Agency designated the highly customized system as Spartan Gate[1] and retained standard security practices, created inter-office document management workflow, permitted redaction referral and review processes, and used standard information dissemination practices.

(U~~//FOUO~~) CIA was Responsible for the Security of RDINet

(U~~//FOUO~~) RDINet contained millions of documents, where were provided without redaction. Therefore, RDINet contains highly classified and compartmented information about intelligence sources and methods; pseudonyms and true names of Agency personnel, assets, liaison officers, and detainees; details about liaison relationships; and, the locations of black sites. The Agency was responsible for securing this highly sensitive material from unauthorized disclosure. Section 102A(i) of the National Security Act requires the Director of National Intelligence (DNI) to protect intelligence sources and methods from unauthorized disclosure. 50 U.S.C. § 3024(i)(1). To accomplish this imperative, the DNI requires "heads of the IC

[1] (U) The Agency creates names for systems to be used as a common reference or as an unclassified name for a classified system.

elements [to] protect national intelligence, intelligence sources, methods and activities from unauthorized disclosure." Intelligence Community Directive 700(E)(2)(a). Executive Order 12333 contains the same imperative to "protect intelligence, intelligence sources, methods, and activities from unauthorized disclosure." EO 12333 § 1.6(d).

(U~~//FOUO~~) Section 1.5 of the RDINet System Security Plan highlights that the protection level and levels-of-concern for RDINet follow guidance in the 5 June 1999 Director of Central Intelligence Directive (DCID) 6/3 Protecting Sensitive Compartmented Information within Information Systems. The policy section of DCID 6/3 contains the following:

> Intelligence information shall be appropriately safeguarded at all times, including when used in information systems. The information systems shall be protected. Safeguards shall be applied such that (1) individuals are held accountable for their actions; (2) information is accessed only by authorized individuals* and processes; (3) information is used only for its authorized purpose(s); (4) information retains its content integrity; (5) information is available to satisfy mission requirements; and (6) information is appropriately marked and labeled.
>
> * Authorized individuals are those with the appropriate clearance, formal access approvals, and need-to-know.

(U~~//FOUO~~) DCID 6/3 goes on to define a security incident as "an act or circumstance in which there is a deviation from the requirements of the governing security regulations. Compromise, inadvertent disclosure, need-to-know violation, and administrative deviation are examples of security incidents."

(U~~//FOUO~~) Section 7.1 on System Administration in the RDINet System Security Plan requires the system administrator to explain how user notifications will be accomplished on the network. The following text listed in the Plan explains how this requirement is satisfied:

> (U~~//FOUO~~) All users of the RDINet will be informed by the application that they consent to monitoring and recording,

and that unauthorized use is prohibited and subject to criminal and civil penalties. The login splash screen for all users fulfills this requirement.

(U~~//FOUO~~) The OIG, [redacted] the CIC, and various interviewees noted that all SSCI users on RDINet clicked the OK button for the login warning banner that read:

> 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. (emphasis added) Violation of system security regulations and guidance may result in discipline by the Agency, and violators may be criminally prosecuted.

(U~~//FOUO~~) RDINet was Subject to Comprehensive, Continuous Monitoring for Security Purposes

~~(S//NF)~~ The entirety of RDINet, including the SSCI side, was subject to the same [redacted] monitoring by the CIC's [redacted] as any other Agency information system.[2] The monitoring is routinely conducted as a security and counterintelligence measure.[3]

B. (U) Arrangements for Use of the System

(U) Protection of SSCI Work Product

(U~~//FOUO~~) Documents reviewed by the Accountability Board highlight that SSCI work product was to be protected within RDINet. The Board did not receive, nor understand there to have been, a signed agreement between the SSCI and Agency on the definition of work product. The OIG report included an undated document on the Standard Operating Procedures for SSCI Review

---

[2] (U~~//FOUO~~) OIG Report, ¶ 17.

[3] (U) Ibid.

that contains what the Board considers to have been one understanding of SSCI work product:

> (U~~//FOUO)~~ Any documents generated on the network drive (a walled-off network share-drive), 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 the 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.

(U~~//FOUO)~~ No Written Agreement Governed CIA Access to the SSCI Side of RDINet

(U~~//FOUO)~~ The OIG used correspondence between the SSCI and the Agency to establish what the OIG termed a "common understanding" on the implementation of RDINet. The Board agrees that one can discern a general working agreement on the day-to-day operations of RDINet, but there was no final, clear agreement on access limits to the SSCI portion of the network. On the evidence reviewed by the Board it appears that recognizing the difficulties of reaching a full final agreement, the Senate and the Agency proceeded instead to leave the resolution of issues that arose to ad hoc administrative processes.

(U~~//FOUO)~~ The 2 June 2009 letter from the SSCI Chair and Vice Chair requests the Agency to "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."

(U~~//FOUO)~~ Director Panetta responded to the SSCI letter on 4 June 2009 with a clarification that "the stand-alone network must be accessed by the 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." The Director's letter further outlines that "any remaining security or logistical concerns or other issues can be resolved through our respective staffs."

(U~~//FOUO~~) A letter from Director Panetta to the SSCI Chair on 12 June 2009 notes "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 Board could find no further information that would clarify the substance behind this statement and the OIG could not locate a final signed agreement.

(U~~//FOUO~~) The OIG report included a 28 May 2009 unsigned MOU on SSCI's review of CIA's Detention and Interrogation Program. The SSCI had informed the Agency that it would issue a subpoena to gain access to unredacted documents containing true names, cryptonyms, pseudonyms, liaison provided intelligence, information from other US government organizations, and the identity of "black sites." The Agency decided to avoid protracted litigation and agreed to provide the above-referenced information with a series of conditions that included:

- Responsive information will be available at a secure Agency Reading Room facility which will permit SSCI personnel with electronic search, filing, and print capability.
- 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.
- 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.

(U~~//FOUO~~) The Parties Dealt with CIA Access to CIA Documents Transferred to the SSCI Side of RDINet on an Ad Hoc Basis. Sometimes They Agreed. Sometimes They Did Not.

(U~~//FOUO~~) In the absence of a written understanding, ad hoc procedures were created as questions on issues arose. Indeed, the January 2014 RDINet incident was not the first time the Agency searched the SSCI side of RDINet to determine if certain CIA-created documents not yet approved for transfer were inappropriately present on the SSCI side of the network. Such administrative searches were commonplace.[4,5,6] For example, on 10 and 11 January 2011, a SSCI staffer asked a CIA officer to search the SSCI side of the database for documents the staffer thought were missing.[7] Another CIA officer responded by e-mail on 21 January 2011 that the cables the SSCI staffer requested were now accessible to SSCI Staff.[8] While a search could reveal that the requested documents had not been produced for transfer to

---

[4](U~~//FOUO~~) CIA [redacted] AAB Submission, p.3 ("There was nothing unusual about a request to determine the presence of files for which the SSCI staff lacked authorized access on the drives used by the SSCI Majority and Minority Staffs. The efforts I undertook at the direction of [redacted] were entirely consistent with my responsibilities for RDINet security.")

[5](U~~//FOUO~~) [redacted] AAB Submission, p. 2 ("On numerous occasions over four-plus years, CIA IT officers had accessed RDI Net as they did here, for the purpose of determining whether particular documents were resident on the system. They often did so at the urging of the Committee staffers themselves, using administrative procedures that were the same or similar to those used in this case. . .")

[6](U~~//FOUO~~) [redacted] AAB submission, p. 5 ("Throughout the SSCI review, SSCI staff knew the practical necessity of carrying out the document production required the non-IT professional CIA staff routinely access CIA-generated documents on the CIA system for the purpose of administering the document production.")

[7](U~~//FOUO~~) [redacted] AAB submission, tab 6. (E-mail dated 10 January 2011 (06:08 PM) from e-mail dated 11 January 2011 (06:12).

[8](U~~//FOUO~~) Ibid. (E-mail dated 21 January 2011 (12:13 PM).

the SSCI staff, it also could reveal that the documents were in fact already on the SSCI side of RDINet.[9]

(U~~//FOUO)~~ Another example is the May 2010 transactions in which the Agency unilaterally removed 926 documents from the SSCI side of RDINet.[10] CIA removed the documents because they had been erroneously comingled before being screened for privilege concerns.[11]

(U~~//FOUO)~~ A SSCI staffer objected to the removal of the documents, making three assertions about documents on RDINet:

1. Documents made available to SSCI on RDINet have been turned over to the Committee, even if made available erroneously;

2. CIA should not unilaterally access documents on the SSCI side of RDINet; and

3. CIA should not unilaterally remove or alter documents on the SSCI side of RDINet.[12]

(U~~//FOUO)~~ The Agency declined to summarily return these documents to the SSCI side of RDINet, and instead, the White House reviewed them for Executive Privilege.[13] When that review was complete, the Agency returned the majority of the documents

---

[9](U~~//FOUO)~~ Ibid. (E-mail dated 23 March 2011 from CIA officer to SSCI staffer ("I checked the SSCI side of Spartan Gate and it appears that [the document you requested] is already in the system.")).

[10](U~~//FOUO)~~ OIG Report Exhibit D, ¶ 2.

[11](U) Ibid.

[12](U) 12 May 2011 (01:31 PM) e-mail from the SSCI staffer to CIA attorneys.

[13](U~~//FOUO)~~ 13 May 2010 (05:36 PM) e-mail from a CIA attorney to [redacted] and a CIA attorney, and the CIA General Counsel ("The WH is not inclined at this point to ask CIA to categorically replace all the documents that were pulled, in large part because the mistake was clerical in nature ... CIA will continue its ongoing efforts to identify all documents that were pulled from the reading room and to produce all such documents to the WHC for review asap.").

to the SSCI side of RDINet, but withheld those subject to the Privilege.[14] This incident reflects an Agency and White House view, known to the SSCI, that the SSCI side of RDINet was non-inviolable. The CIA officials believed that it was permissible for the Agency to search the SSCI side of the database to determine whether particular Agency documents were present there.[15] [redacted] emphasized at the time that such searches would be "limited to checking to see whether a document is or is not already in the reading room."[16] However, at that time, Senator Feinstein expressed to the White House her strong view that removal of documents was inappropriate, and the White House acknowledged her concerns and agreed that the documents should not have been removed without notice to the Senate and no such removals should occur in the future.

(U~~//FOUO~~) General Conclusion: SSCI staffers were, or should have been aware of, CIA's [redacted] monitoring of RDINet for security purposes. In fact, CIA had previously accessed [redacted] collected from the SSCI side of RDINet when security concerns arose.

(a) (U~~//FOUO~~) The Board determined that while an informal understanding existed that SSCI work product should be protected, no common understanding existed about the roles and responsibilities in the case of a suspected security incident.

(b) (U~~//FOUO~~) The joint desire to begin the review and avoid protracted negotiations on a final agreement led the parties to

---

[14] (U~~//FOUO~~) Memo, "Administrative Document Production Error," 1 June 2010.

[15] (U~~//FOUO~~) 7 June 2010 (10:53 AM) e-mail from a CIA attorney to [redacted] ("Occasionally in the course of the White House's review of EP documents, they will come across a document they believe may already be in the reading room (as part of a different batch) and have asked us to check, so they don't assert EP over a document that has already been produced. Prior to last month's events, the SOP was to check the reading room's holdings (electronically - not physically) and let the WH know. We would like to continue to honor WH requests to check the reading room's holding when they ask about a specific document. Are you ok with our continuing to do so? We currently have several requests outstanding.").

[16] (U~~//FOUO~~) 8 June 2010 (01:51 PM) e-mail from a CIA attorney to the RDI Front Office, another CIA officer, and [redacted]

proceed without a definitive, fully executed agreement, they elected instead to handle issues as they arose.

(c) ~~(TS/[redacted]/NF)~~ The Board concluded SSCI staffers were, or should have been, aware of the [redacted] monitoring by [redacted] because of past [redacted] discoveries of SSCI staffers' misconduct on RDINet:

~~(TS/[redacted]/NF)~~ In December 2009, the [redacted] monitoring [redacted] detected that a SSCI staffer [redacted] 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 [redacted] 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 SSCI team.[17]

~~(TS/[redacted]/NF)~~ In May 2010, a SSCI staff member requested from the Agency the ability to print a sensitive document from RDINet. The SSCI staff member attempted to bypass the print restriction by [redacted] reviewed the incident and recommended removing the possibility of SSCI staffers utilizing [redacted] but because the capability was [redacted] it could not be removed or disabled. The RDI team discussed this issue with SSCI staff and reminded them of the need for security of sensitive documents.[18]

---

[17](U) Ibid. ¶ 3.

[18](U) Ibid.

II. (U) Events of Days in Question, January 2014

(U~~//FOUO)~~ Agency personnel searched the SSCI-side of RDINet or reviewed SSCI-related [redacted] over several days in January 2014. The Board grouped these activities into three separate "looks."

(U~~//FOUO)~~ [redacted] told the IG [redacted] ordered what the Board calls the first and second looks because [redacted] believed there was a security breach on RDINet. [redacted] suspected that privileged Weekly Case Reports (WCRs) could be on the SSCI's side of RDINet and had been accessed by SSCI staff.[19] [redacted] formed this belief because of a November 2013 Senate request for a copy of the "Panetta Review"; because a draft SSCI report contained language remarkably similar to portions of the "Panetta Review"; and because of a statement by a SSCI staffer that the staffer had "seen the real response."[20]

(U) The First Look

(U~~//FOUO)~~ On or about 9 January, [redacted] instructed [redacted] to search RDINet to determine whether particular Agency-created documents not yet cleared for transfer were resident on the SSCI accessible portion of the database.[21] Specifically, [redacted] wanted to know whether the privileged and deliberative draft CIA summary documents known variously as the "Panetta Review," "Special Review Team Documents (SRT)," or WCRs" were inappropriately on the SSCI side of the database.[22] RDI personnel conducted this look on or about 9 and 10 January 2014. [redacted] has maintained that the Agency's obligations under the National Security Act created a

---

[19] (U~~//FOUO)~~ OIG notes of 27 March 2014 [redacted] Interview, ¶ 7 and 15.

[20] (U) Ibid. ¶¶ 7-10, 13.

[21] (U~~//FOUO)~~ OIG notes of 27 March 2014 [redacted] interview, ¶ 15.

[22] (U) Ibid. ¶ 8.

legal duty to search the SSCI side of RDINet for the presence of Agency documents to which SSCI staff should not have access.[23]

(U~~//FOUO~~) The [redacted] RDINet IT employee, [redacted] recalls being instructed by [redacted] on 9 January 2014 to conduct searches of RDINet for the presence of files with "WCR" or "SRT" in their titles.[24] First, [redacted] searched the database containing documents to which the Agency had granted SSCI access[25] and no file with WCR or SRT in its name was present on that portion of RDINet.[26] Next, [redacted] conducted a Google search of RDINet, which by virtue of [redacted] administrator access, searched the entirety of the network.[27] That search disclosed as expected that WCR and SRT files resided on the CIA side of the network, but also that they were present on the SSCI Majority Staff user drive.[28] Finally, [redacted] conducted a root search with the search terms WCR and SRT, which revealed that files with those names were located on one SSCI Majority Staff user drive, and the SSCI Majority shared drive.[29]

(U~~//FOUO~~) When questioned by the IG, [redacted] recalled instructing [redacted] on 10 January to demonstrate how SSCI staff would have looked at the WCR documents on the SSCI side of the network.[30] [redacted] recalled asking [redacted] to help [redacted] take screenshots of the Majority share drive folder and subfolder in which the WCR documents resided, and to demonstrate how SSCI staff could use the Google appliance to locate the documents.[31] [redacted] said [redacted]

[23] (U~~//FOUO~~) [redacted] AAB Submission, p. 6.

[24] (U~~//FOUO~~) [redacted] AAB Submission, p. 2.

[25] (U) Ibid.

[26] (U) Ibid.

[27] (U) Ibid.

[28] (U) Ibid.

[29] (U) Ibid.

[30] (U~~//FOUO~~) OIG Notes of 22 April 2014 [redacted] OIG interview, ¶ 22.

did not recall whether this required [redacted] to adjust [redacted] network permissions.[32]

(U~~//FOUO)~~ There is no evidence that any SSCI work product—e-mails, drafts, or other confidential or deliberative material of any type—were accessed at that time.

~~(C//NF)~~ There is disagreement about the timing of the activity [redacted] recalls as occurring on 9 January, and who participated in the activity. The OIG concluded that [redacted] assisted [redacted] on the 9th,[33] but time and attendance records show [redacted] on leave that day[34] and [redacted] recalled assisting [redacted] on the 9th.[35] [redacted] recalls the RDINet searches being conducted between 6 and 8 January, not 9 and 10.[36] [redacted] recalled that [redacted] had determined that SSCI staff had access to the WCR documents on 7 or 8 January.[37] The OIG Report also says [redacted] opened "a few" of the files on the 9th,[38] but that finding is not corroborated by the OIG interview notes or the various AAB submissions. [redacted] surmises that the OIG confused the activities of the 9th with activities of the 10th.[39]

---

[31](U) Ibid.

[32](U) Ibid. ¶ 23.

[33](U) OIG Report ¶ 24.

[34]~~(C//NF)~~ [redacted] AAB Submission, p. 9 and Exhibit 3.

[35](U~~//FOUO)~~ [redacted] AAB Submission, p. 2.

[36]~~(C//NF)~~ [redacted] AAB Submission, p. 6

[37](U~~//FOUO)~~ OIG Notes of 27 March 2014 [redacted] OIG Interview, ¶ 14.

[38](U) OIG Report ¶ 24.

[39](U~~//FOUO)~~ [redacted] AAB Submission, p. 2.

(U) The Second Look

(U~~//FOUO)~~ The second look commenced on or about 10 January, when [redacted] attempted to learn whether SSCI Staffers had actually accessed or printed the WCR documents.[40] If the documents had not been accessed or copied, the potential security concerns and need to approach SSCI would be more limited. [redacted] stated in [redacted] IG interview that [redacted] reported the results of the first look to the [redacted] and the [redacted] on the 9th,[41] and that "between [redacted] (the [redacted]), and [redacted], they decided to approach the next step as determining whether the files had been accessed by SSCI."[42] [redacted] recollection of this meeting is consistent with the [redacted][43]

~~(S//NF)~~ [redacted] did this by asking [redacted] to task CIC [redacted], which [redacted] believed to be [redacted][44]

(U~~//FOUO)~~ In [redacted] statement, [redacted] says that the [redacted] visited [redacted] on 9 January after briefing the D/CIA about the results of "the first look," and conveyed an explicit instruction to [redacted] that [redacted] determine whether SSCI staff had accessed or printed the documents.[45] Specifically, [redacted] recalled being told by the [redacted] that the D/CIA "wanted to be 'completely sure' that the documents were, in fact, what they appeared to be . . . and also wanted to know if they had been printed, as he was concerned the documents could have been

---

[40](U) Ibid. ¶ 20.

[41](U) Ibid. ¶ 15.

[42](U) Ibid. ¶ 17.

[43](U~~//FOUO)~~ AAB 14 October 2014 [redacted] Interview (When I heard about this, I thought the facts were not correctly developed. I wanted to know of the WCRs were just sitting there, or had they been used, or were taken. If they were accessed, how often and by whom?)

[44](U~~//FOUO)~~ OIG notes of 27 March 2014 [redacted] interview, ¶ 17.

[45](U~~//FOUO)~~ [redacted] AAB Submission, p. 10.

secretly removed from the CIA facility."[46] [redacted] also wrote in [redacted] statement that the D/CIA himself reiterated these explicit instructions to [redacted] on three occasions between 10 and 13 January.[47]

(U~~//FOUO)~~ A misunderstanding between the D/CIA and [redacted] arose because the former did not appreciate what forensic techniques were necessary to answer his questions and the latter did not understand the D/CIA's expectations that no intrusive methods be employed.

~~(S//~~[redacted]~~/NF)~~ On 10 January 2014, [redacted] sought to determine whether SSCI users accessed the WCR documents by tasking [redacted] to [redacted] who accessed documents contained in [redacted] folder of RDI Net for the period 3/1/2009 to 12/31/2013."[48] In a follow-on tasking, [redacted] for the same documents . . . to determine whether staffers would have had the opportunity to take the documents for the Hill in hard copy."[49]

~~(S//NF)~~ In addition to describing the information sought, the [redacted] tasking expressly limited where [redacted] was to look. [redacted] first e-mail to [redacted] carried the following caveat:

> We ask that you provide us ONLY the [redacted] documents in this folder and its component sub-

---

[46](U) Ibid.

[47](U~~//FOUO)~~ Ibid. pp. 10-11 ("First in his office on the night of January 10; second during a call placed to me at home on the afternoon of January 11; and third, in a passing conversation in the doorway of his office on January 13. In the January 11 call, the D/CIA particularly emphasized his desire to confront SSCI leadership immediately with information concerning the matter. As a predicate to doing so, however, he felt the need to have a clear understanding of how the documents came to be accessible by SSCI Staff.")

[48]~~(S//NF)~~ [redacted] AAB Submission, tab 1, 10 January 2014 (09:18 AM) e-mail from [redacted] to [redacted] staff.

[49](U~~//FOUO)~~ 10 January 2014 (07:25 PM) e-mail from [redacted] to CIC [redacted] advisors.

folders. Please **DO NOT** undertake this tasking if it would require that you search and/or provide us [redacted] relating to other contents of the RDI Net Y: drive, as this drive is a SSCI staff drive on the RDI Net system.[50]

~~(S//NF)~~ After [redacted] follow-on tasking, [redacted] repeated this caveat in an e-mail to CIC [redacted] on 13 January 2014,[51] "To follow up on our conversation this morning, please be sure that CIC [redacted] understands that the scope of the documents under review has not/not changed. [redacted] should be told expressly to look ONLY at the provenance of the documents in the [redacted]

(U~~//FOUO~~) [redacted] reiterated the caveat: "I can't stress how important this is. We need to confine this review as narrowly as possible, and make sure everyone understands this is not a fishing expedition into SSCI files (emphasis added)."[52]

(U~~//FOUO~~) When the Executive Director convened a meeting with senior Agency leadership on the morning of 14 January, each person present was either aware of the first and second looks and approved of the action [redacted] had taken to date, or posed no objection.[53, 54, 55, 56] the CIC [redacted] also was present at the

---

[50] ~~(S//NF)~~ [redacted] AAB Submission, tab 1, 10 January 2014 (09:18 AM) e-mail from [redacted] to [redacted] staff (emphasis in original).

[51] ~~(S//NF)~~ [redacted] AAB Submission, tab 3, 13 January 2014 (09:18 AM) e-mail from [redacted] to CIC [redacted]

[52] ~~(S//NF)~~ [redacted] AAB Submission, tab 3, 13 January 2014 (04:57 PM) e-mail from [redacted] to CIC [redacted]

[53] (U~~//FOUO~~) OIG notes of 9 April 2014 EXDIR interview, ¶ 10 (meeting attendees surprised by the D/CIA's decision not to learn how the documents got on the SSCI side and felt that Agency personnel had not exceeded their authority or acted inappropriately regarding the review of RDI events.)

[54] (U~~//FOUO~~) OIG notes of 15 April 2014 the [redacted] interview, ¶ 16 ("he knew [redacted] was having [redacted] IT guys look at it. . . [and] [redacted] actions did not strike him as problematic or in any way untoward").

[55] (U~~//FOUO~~) OIG notes of 2 April 2014 the [redacted] interview, ¶ 18 ("SSCI had documents on their side that were not passed through the firewall. According to the [redacted] all of the information was provided by [redacted] and

meeting and recalled that the "[redacted] repeatedly emphasized that the 'D/CIA wants to GO' on this issue."[57]

(U) The Third Look

(U~~//FOUO~~) The third look, while benign in intent, was characterized by miscommunications, is the source of greatest controversy, and raised the most questions about the scope of the Agency's security review.

~~(S//NF)~~ [redacted] and the Office of Security's Cyber Blue Team (CBT) conducted this third look. [redacted] analyzed activity on the SSCI folder containing the WCRs to determine if any documents were printed from that folder and how the WCR's got onto the SSCI side of RDINet.[58] The CBT review was conducted to determine how SSCI could have gained access to the WCRs, how a SSCI user could discover the WCRs, and how the Agency knew that SSCI acquired access to the WCRs.[59] The Board tried to piece together the communications used to start, stop, modify, and continue these activities.

~~(TS//~~[redacted]~~/NF)~~ In his OIG interview, a [redacted] contractor employee explained that he was tasked "sometime in January 2014" with [redacted] on RDINet, and specifically, the "CIA side."[60] He was

---

[redacted] The [redacted] stated that they knew the files were there through whatever computer action had taken place. He stated that he did not understand fully how they found them.")

[56](U~~//FOUO~~) [redacted] AAB Submission, p. 8. (Also present at the EXDIR meeting the morning of 14 January were the [redacted] Acting General Counsel, Director of the Office of Public Affairs, Director of the Office of Congressional Affairs, [redacted] the Counterintelligence Center (CIC), [redacted] [redacted] CIC, [redacted] to the EXDIR.) No one raised an objection to [redacted] actions.

[57]~~(S//NF)~~ Timeline provided by [redacted] CIC during AAB Interview.

[58]~~(S//NF)~~ OIG notes of 11 March 2014 [redacted] contractor interview, ¶ 2.

[59](U~~//FOUO~~) OIG notes of 20 March 2014 CBT [redacted] interview, ¶ 4.

[60]~~(S//NF)~~ OIG Notes of 12 March 2014 separate [redacted] contractor, ¶ 3.

investigating the possibility that the documents were provided to the SSCI staff by a leaker though "HUMINT."[61] The [redacted] contractor did not have access to the RDINet hard drives, network share drives, or actual RDINet files.[62] Rather, he looked "at [redacted] that had previously been collected by [redacted] as part of 'normal CIA [redacted] on CIA networks.'"[63] The [redacted] contractor explained that, for RDINet, [redacted][64] He found no evidence of a HUMINT leak, and theorized that a misconfiguration of the google appliance may have given SSCI staff access to the document.[65] However, a stand down order from the Director, discussed below, arrived before he could test that theory.[66]

(U~~//FOUO)~~ When the D/CIA was briefed the evening of 14 January 2014 about the foregoing, he ordered the stand down.[67] He then proposed a joint CIA-SSCI review of the matter,[68] which the SSCI shortly thereafter declined to participate in.[69] At no time did the D/CIA order any further forensic work to be undertaken.[70]

~~(S//NF)~~ Upon returning from that evening's meeting with the D/CIA, [redacted] CIC instructed [redacted] "to 'stand down immediately' on any tasking on this issue."[71] Those working the issue had

[61](U) Ibid.

[62](U) Ibid.

[63](U) Ibid.

[64](U) Ibid., ¶ 7.

[65](U) Ibid., ¶ 8.

[66](U) Ibid.

[67](U//FOUO) OIG Notes of 21 April 2014 D/CIA OIG Interview, ¶ 6.

[68](U//FOUO) Ibid., ¶ 8.

[69](U) Ibid., ¶ 10.

[70](U) Ibid., ¶ 9.

[71](U~~//FOUO)~~ Timeline provided by [redacted] CIC during AAB Interview.

departed for the day, and eventually, [redacted] CIC [redacted] was reached at home and instructed to call CIC [redacted] at home with the order to instruct the two [redacted] contractor analysts to stand down immediately.[72]

(U~~//FOUO~~) After the D/CIA briefing, the [redacted] contacted the [redacted] the Office of Security [redacted] OS) at home about the proposed joint review [redacted].[73] The [redacted] asked [redacted] OS if the OS could lead an investigation of an IT issue.[74] [redacted] called [redacted] OS 15 minutes later and said the issue would be discussed at work on 15 January.[75] The SSCI Security [redacted] then called and explained the work would be part of a joint SSCI-CIA review.[76]

~~(S//NF)~~ [redacted] CIC's stand-down order apparently was not delivered in a timely fashion. According to one [redacted] contractor employee, he was ordered on 15 and 16 January by the [redacted] to look into [redacted] that was available for RDINet.[77] There were three tasks: 1) analyze activity on the specified folder; 2) determine [redacted] and, 3) determine the provenance of the documents.[78]

~~(S//NF)~~ On 15 January, several Agency officers met to scope the OS review and effect the turnover from [redacted] to OS.[79] [redacted] OS understood the guidance from the 14 January D/CIA meeting was

---

[72] (U) Ibid.

[73] (U~~//FOUO~~) OIG Notes of 3 April 2014 [redacted] OIG Interview, ¶ 30.

[74] (U~~//FOUO~~) AAB Notes of 8 September 2014 [redacted] OS Interview, p. 1.

[75] (U) Ibid.

[76] (U) Ibid.

[77] ~~(S//NF)~~ OIG notes of 11 March 2014 [redacted] contractor employee Interview, ¶ 2.

[78] (U) Ibid.

[79] ~~(S//NF)~~ Ibid. In attendance were [redacted] OS, [redacted] CIC, [redacted] CIC [redacted] OS [redacted] Officer, and OGC attorneys [redacted] and CIC [redacted]

that CIC would stop its work and that OS would look at [redacted] to determine if a violation occurred.[80] (S//NF) At a meeting also on the 15th [redacted] the Cyber Blue Team (CBT) received a tasking from [redacted] and [redacted] OS.[81] The oral tasking was followed by an e-mail confirmation.[82] The CBT was ordered to review the [redacted] data to determine how SSCI could have gained access to the restricted documents.[83]

~~(S//NF)~~ A [redacted] contractor employee was assigned to help the Office of Security's Cyber Blue Team (CBT) conduct its review.[84] He stated that the CBT's tasks were to verify that unauthorized documents were in a specific location, and if so determine how they got there.[85] According to the employee, the combined team concluded that someone directly navigate to the file path containing the unauthorized documents and copied them to another SSCI accessible location.[86] However, he was unsure of how that individual discovered the folder path that led him or her to the documents.[87]

~~(S//NF)~~ When interviewed by the OIG, [redacted] said the first tasking from [redacted] OS called for a full forensic review of the SSCI systems.[88] However, before CBT accessed any part of the SSCI side of RDINet, [redacted] OS countermanded that order and limited CBT's

---

[80] (U~~//FOUO~~) AAB Notes of Interview with [redacted] OS p.2.

[81] (U~~//FOUO~~) OIG notes of 20 March 2014 [redacted] Cyber Blue Team Interview, ¶ 4.

[82] (U) Ibid.

[83] (U) Ibid.

[84] ~~(S//NF)~~ OIG Notes of 11 March 2014 Interview of [redacted] contractor employee, ¶ 3.

[85] (U) Ibid.

[86] (U) Ibid.

[87] (U) Ibid.

[88] (U~~//FOUO~~) OIG Notes of 13 March 2014 Interview of [redacted] ¶ 2.

review to the [redacted] monitoring of RDINet.[89]

(U~~//FOUO~~) When interviewed by the OIG, a CBT analyst said their review identified by name the SSCI user responsible for originally accessing the unauthorized documents.[90] The SSCI employee accessed at least 166 files. The review also discovered that beginning on November 9, 2010 the restricted documents were later disseminated among four other SSCI staffers and printed.[91] The names of the SSCI staffers were removed from the final CBT report and replaced with IDENs.[92]

(U~~//FOUO~~) Although OIG interview notes mention the CBT's conclusions, they do not describe the facts on which the CBT based its conclusions. The OIG Report's Executive Summary says the CBT report contains some "forensically reconstructed" SSCI staffer e-mails.[93] And the body of the OIG Report describes those e-mails as "communication between 'Congressional users' that directed them to review specific documents."[94] As previously indicated, SSCI communications inappropriately reviewed by Agency staff were limited in number (five) and did not involve discussions of substantive matters in content. The CBT report lists five e-mails made by one staffer:

[redacted]

[89](U) Ibid.

[90](U~~//FOUO~~) OIG Notes of 13 March 2014 CBT analyst Interview, ¶ 3.

[91](U) Ibid.

[92](U~~//FOUO~~) OIG Notes of [redacted] Interview, ¶ 2.

[93](U) IG Report, Executive Summary, p. iii.

[94](U) IG Report, p. 44.

[redacted]

~~(S//NF)~~ The OIG found that [redacted] OS ordered the CBT review under [redacted] own authority as a normal OS function and did not believe [redacted] needed to seek higher approval.[95] [redacted] OS believed [redacted] actions were consistent with the D/CIA's stand down order because [redacted] thought it applied to the joint CIA-SSCI investigation, not to an internal review of [redacted] already had compiled.[96]

(U~~//FOUO)~~ This third look resulted in inappropriate access to SSCI work product. While the access was limited—a total of five e-mails, none of any consequence or involving discussions of substantive matters—it was inconsistent with the D/CIA stand-down order and with the work product limitations emphasized by [redacted] and [redacted] in their taskings.

III. (U) The OIG Findings: Questions and Issues of Fact

A. (U) Undisputed Facts

(U~~//FOUO)~~ The Agency and SSCI did not enter into a signed, final agreement to govern the management of security in this unusual circumstance, but agreed to resolve issues informally, case by case. No record exists to establish that the SSCI staff security briefings agreed to in principle were provided.

(U~~//FOUO)~~ The Agency monitored and collected all computer activity on RDINet as part of its standard information system

[95](U) IG Report, p. 43.

[96](U) Ibid.

security process. The [redacted] included all activity on the SSCI portion of the network.

(U~~//FOUO)~~ On the basis of this monitoring, and as known by SSCI staff, previous instances of improper conduct on the RDINet had been identified and responsive security measures taken. On certain occasions, SSCI staff requested CIA technology staff assistance in locating documents by accessing SSCI space on the system.

(U~~//FOUO)~~ [redacted] in discussions with [redacted] made the decision to find out if SSCI staff had access to WCR or SRT documents that were deemed privileged, and not part of the SSCI review, and were created after the information cut-off date of 22 January 2009.

(U~~//FOUO)~~ [redacted] directed RDINet IT officers to help [redacted] determine the location of the WCRs and SRTs on RDINet and the documents were discovered on the SSCI portion of the shared drive.

~~(S//NF)~~ CIC [redacted] was brought in to examine its [redacted] to determine if SSCI staff accessed and used the WCRs and SRTs.

~~(S//NF)~~ The Office of Security's Cyber Blue Team analyzed [redacted] and the Team's final report included a limited number of SSCI staff e-mails.

B. (U) Facts and Issues in Dispute

1. (U) Legal Authorities and Authorization

(U~~//FOUO)~~ The IG concluded that communications in 2009 between SSCI and the Agency created a common understanding that CIA access to the SSCI portion of RDINet would be restricted to IT staff for administrative purposes unless authorized by the SSCI. In this context, the IG found actions directed or performed by [redacted] and the IT staff to be improper and/or unauthorized.

(U~~//FOUO)~~ IG investigators highlighted to the Board that the five officers were not part of an investigative body (CIC, OS,

or OIG) and had no investigative authority. Two IG officers had extensive IT experience and further noted to the Board that actions taken by the IT officers were unusual and beyond what is expected for an IT officer.

(U~~//FOUO)~~ The five officers countered the IG's findings by highlighting how searches for documents on RDINet had become a common practice over the years with IT staff regularly called upon to help determine the location of documents across RDINet. They also emphasized that the Agency always maintained responsibility for RDINet security, and the SSCI was aware of this fact from previous incidents and express notification before access to the system. With respect to who should have initiated an investigation, [redacted] determined [redacted] had the authority and responsibility to ensure the security of RDINet and [redacted] actions were in line with [redacted] responsibilities. In [redacted] written response to the IG report, [redacted] notes that the System Security Plan [redacted] to address unauthorized access.

(U~~//FOUO)~~ The Board notes that [redacted] proactively and consistently communicated that the Agency take very limited actions so it would not intrude upon SSCI work product.

2. (U) Accountability and Reporting to Leadership

(U~~//FOUO)~~ There is some confusion as to who in Senior Leadership authorized what action and when they issued these directives. The OIG told the Board that [redacted] conveyed the D/CIA's interest in the matter before [redacted] had received feedback from the D/CIA, but other information before the Board makes it appear there was regular dialogue with leadership as events unfolded. Alerts to the D/CIA can take different paths and it appears that the Acting General Counsel, the [redacted] and the [redacted] were informed of the discoveries after the first look. Of note, it was difficult for the Board to develop a precise timeline because events happened in parallel and some of the communications were face-to-face or via phone calls.

3. (U) Recusal Question

(U~~//FOUO~~) The IG report notes that the Acting General Counsel by 7 February 2014 had previously recused himself from RDI-related matters and was therefore unaware of programmatic details. The IG asserts that the recusal meant [redacted] did not have a supervisor during the events in question.

(U~~//FOUO~~) When interviewed by the Board on 8 September 2014, the Acting General Counsel explained that he recused himself after the 11 March 2014 SSCI Chair speech on the Senate floor and was not recused when he signed out the crimes report on 7 February 2014. He explained his active participation throughout the events in question and that he had a discussion with [redacted] about the potential security incident where he outlined the key issues as:

- RDINet is an Agency system.
- SSCI staff members were briefed on the audit capability (the Board could not confirm SSCI staffers were briefed on this audit capability).
- IT staff had authorized access.
- There was a past practice of removing items from the SSCI side of RDINet.
- That it is within Agency responsibilities to determine if someone took something.

IV. (U) Board Conclusions

A. (U) Standard for Reviewing Conduct

(U~~//FOUO~~) The Board determined there was no agreement between SSCI and the Agency on what steps would be taken in the event of a suspected security incident. In the absence of an agreement, the Agency followed its standard security practices with the understanding that the separations of powers concerns were very sensitive, and of keen importance to Agency leadership, and that SSCI work product should, therefore, be protected.

(U~~//FOUO~~) In the absence of a formal agreement, the Board the "reasonable person" standard when evaluating the actions of the five individuals. The Board notes that this is the standard that

the OIG told the Board was used in evaluating the conduct in question.

(U~~//FOUO~~) The Board did not attempt to define what path, decisions, or courses of action would represent the most reasonable responses among various reasonable alternatives, but instead evaluated if the conduct of these officers could be determined to have been unreasonable.

(U~~//FOUO~~) Under the "reasonable person" standard, it is possible that different conclusions can be reached by different people from the same set of facts. This is particularly so in a fundamentally complex case such as this, involving an unprecedented shared system holding millions of highly sensitive materials which was operated by the Agency and the Senate without a clear, settled agreement on the management of security.

(U~~//FOUO~~) The fact that the potential security breach involved a co-equal branch of the United States Government added substantially to the complexity and sensitivity of the situation. Great certitude was understandably desired before raising it with the Senate and pursuing formal allegations of wrongdoing.

B. (U) Legal Authorities and Authorization

(U) Application of Criminal Law § 1030

(U~~//FOUO~~) The IG referred this matter to the Department of Justice for potential violations of the Wiretap Act and the Computer Fraud and Abuse Act.[97] The OIG Report provided no rationale for either referral. In Board interviews, the investigative staff asserted that [redacted] violated the Computer Fraud and Abuse Act because they accessed the SSCI side of RDINet in violation of an unwritten "Common Understanding" between CIA and the SSCI.

(U~~//FOUO~~) The facts and circumstances of this case do not support the use of either statute to establish "unauthorized access" by these Agency personnel. The Wiretap Act criminalizes

[97] (U) IG Report, ¶ 1.

under certain circumstances the intentional interception, disclosure, or use of the electronic communications of others. 18 U.S.C. § 2511. The Act excludes from its coverage the interception of electronic communications if a party consents to the interception. Id. § 2511(2)(c). Each time a SSCI staffer logged onto RDINet, he or she was presented with the warning that his or her actions were subject to monitoring, and asked to consent to the monitoring as a condition of accessing the system. Thus, SSCI Staffers consented to Agency access of the SSCI side of RDINet for some purposes, not to include the examination of SSCI work product. The Act also excludes from its coverage the interception of communications "under color of law to intercept the . . . communications of a computer trespasser." Id. § 2511(i). When Agency personnel accessed information from the SSCI Side of RDINet, they were investigating suspected access to highly classified information from the CIA side of RDINet, which the Agency has a legal duty to protect from unauthorized disclosure. Accordingly, the Wiretap Act does not support a finding of Agency personnel misconduct in the relation to the events of January 2014.

(U~~//FOUO)~~ There also is no basis for such a finding in the Computer Fraud and Abuse Act referral. An individual violates that Act when he "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains - . . . Information from any department or agency of the United States." 18 U.S.C. § 1030(a)(2)(B). The Board could not find evidence of a "Common Understanding" that would have prevented [redacted] from looking on the SSCI side of RDINet for the presence of CIA documents—highly classified and sensitive documents SSCI was not entitled to access. To the contrary, CIA routinely and without controversy searched the SSCI side of RDINet for CIA documents and it did so on certain occasions at SSCI staff request.

~~(S//NF)~~ As for the more detailed examination conducted by [redacted] at [redacted] direction, [redacted] reasonably believed [redacted] was acting under the authority of the D/CIA when [redacted] tasked [redacted] to discover whether SSCI staff had accessed and printed the documents.

(U~~//FOUO~~) Because there is no basis for a finding against [redacted] under these statutes, neither can they establish misconduct [redacted] who simply carried out [redacted] instructions.

C. (U~~//FOUO~~) The Reasonableness of [redacted] and [redacted] Actions

(U~~//FOUO~~) As previously noted, by early January 2014 [redacted] had reason to believe that CIA documents had been accessed without authorization by SSCI staff. The origins and extent of the probable security breach were unknown to [redacted]

(U~~//FOUO~~) This presented [redacted] with a dilemma. [redacted] needed to ensure that a CIA system containing substantial sensitive material was secure. [redacted] also needed to safeguard the prerogatives of the Senate, particularly the protection of work product.

(U~~//FOUO~~) Several courses of actions were possible, but none were without risk. In fact, no good options may have existed and any may have led to the subsequent controversy.

(U~~//FOUO~~) [redacted] chose to first verify that a security breach in fact existed before informing [redacted] superiors. This seems reasonable given the embarrassment to the Agency and harm to the Agency-SSCI relationship that would have resulted from a false allegation. [redacted] at all times attempted to limit the scope of the verification process. On the day the document was discovered on the SSCI side of the RDINet, [redacted] relayed this information to Agency leadership. There is no evidence that [redacted] authorized the review of SSCI work product.

~~(S//NF)~~ The IG contends that [redacted] should not have undertaken steps to verify [redacted] concerns and instead should have gone to the Office of Security. This would have spared [redacted] adverse OIG findings, but in all likelihood could have led to the same controversy or worse. [redacted]

[redacted]

[redacted]

(U~~//FOUO~~) [redacted] subsequent efforts to determine whether the documents had been copied or accessed also seem reasonable. First, [redacted] understood the D/CIA to have requested that [redacted] do so (even though the D/CIA did not fully appreciate the technical methods this effort would necessitate). Second, this was no normal potential security problem; it involved the United States Senate. Accordingly, it seems reasonable for [redacted] to have explored all alternatives and possible solutions before the problem was confirmed and the D/CIA would have raised it with Senate leaders.

(U~~//FOUO~~) The Board evaluated [redacted] actions in light of directives [redacted] received from [redacted] to determine the presence of documents on the SSCI side of RDINet. The Board considered [redacted] actions to use IT permissions to search for the documents as arguably unorthodox, but they seemed to be within reason given the imperative relayed to [redacted] by [redacted]

~~(S//NF)~~ In [redacted] written statement to the Board, [redacted] highlighted the Agency on 8 January 2014 responded to the 26 November 2013 SSCI request for copies of the "Panetta Review and associated materials" after the White House Counsel's office reviewed them on 7 January 2014 and confirmed they were subject to privilege. This sets the framework for [redacted] initial speculative discussions with [redacted] that SSCI staffers likely had access to the documents. [redacted] had a lingering concern with the Google search tool configuration because SSCI staffers in April 2013 obtained a copy of a privileged spreadsheet containing a list of Agency videos and the staffers agreed with the Agency to destroy the document.[98]

~~(S//NF)~~ Regarding the use of SSCI-like access, [redacted] wrote to the Board that "we sought to test whether the previously known Google misconfiguration still existed and allowed an IT professional with IT permissions of a SSCI user to access particular nonresponsive, privileged **CIA** documents, which existed on RDINet with restrictions intended to limit access only to CIA users." (emphasis in the original) Search terms were

[98] (U~~//FOUO~~) [redacted] AAB submission, pages 9-10.

chosen to return only CIA work product and [redacted] first assumption was SSCI staff could have accessed the documents in a CIA-only location. [redacted] was surprised to see the documents "saved into a space intended for SSCI work product."[99]

(U~~//FOUO)~~ [redacted] briefed [redacted] actions to Agency leaders at the previously mentioned 14 January 2014 morning meeting and none of the officers present objected to the way [redacted] identified the documents. Upon the D/CIA's later stand down directive, [redacted] wrote to the IT staff to see if access to the documents could be restricted but directed that no further steps be taken.[100]

(U~~//FOUO)~~ Summary: It is entirely possible that reasonable people would make different decisions under this complex, unique set of circumstances. We conclude, however, that [redacted] and [redacted] did not act unreasonably and in fact tried to carefully balance both need for RDINet security with the desire to protect SSCI work product while ascertaining the facts necessary for their superiors' review.

D. (U) Candor (IT staff)

(U~~//FOUO)~~ The IG findings of lack of candor against the IT employees did not assert untruthfulness. Instead the IG contends that their responses were initially incomplete and that reasonable persons would have highlighted their actions taken at the direction of the OGC officers.

(U~~//FOUO)~~ This contention is unsupported for numerous reasons. First, no transcript, recording, or other comprehensive record of the interviews exists, so it is impossible to reconstruct the questions asked of the IT employees and their purportedly evasive answers.[101] Second, the purported problematic responses

---

[99](U) Ibid, page 10.

[100](U) Ibid, page 13.

[101]~~(C//NF)~~ The Board notes that in the IG's Memorandum of Investigative Activity (MOIA) that summarizes their only interview with [redacted] on 4 February 2014, paragraph 8 quotes [redacted] on [redacted] participation in a meeting with [redacted] approximately three weeks prior to the interview. The Board assumed this meeting was related to the events in question and [redacted] might have intended to have referred to them.

came at the end of very brief interviews which focused mostly on unrelated technical matters, so there is a reasonable basis for the IT employees' belief that they were being responsive. Third, the IG staff characterized the questions they asked as intentionally general and designed to elicit as broad a response as possible, not specific and detailed responses. Fourth, when the Board interviewed the IT employees, each credibly denied any attempt to evade questioning. Fifth, [redacted] and [redacted] were open about the searches they had ordered, so it would have been purposeless for the IT employees to conceal their actions.

(U~~//FOUO~~) The Board evaluated the OIG's questions used during their first interviews of the three IT officers and the Board as unable to discern questions that would have led [redacted] and [redacted] to explain their recent work under the direction of [redacted]

(U~~//FOUO~~) IG investigators stressed to the Board that [redacted] and [redacted] provided relevant details when they were "confronted with the evidence." However, there is no evidence mentioned in the corresponding MOIAs, and the OIG did not document the exact content of the questions asked during the second interview. When pressed, one investigator could not recall what was shown during the interview.

(U~~//FOUO~~) Under these circumstances, where the alleged transgression is a lack of completeness not lying, more is needed to conclude that the individuals involved were unreasonable in their initial responses. The Board concluded that the allegations of lack of candor were unsupported by the evidence.

E. (U) Crimes Report Questions: Clarification In the Course of the IG Interviews

(U~~//FOUO~~) The IG asserted that [redacted] provided inaccurate information that was subsequently included in the 7 February 2014 letter to DOJ. The OIG in interviews with the Board stated the OIG did not intend to suggest that [redacted] acted improperly in providing this information. The Board determined that this assertion is at any rate erroneous. The

Cyber Blue Team provided the factual basis for the referral, wholly apart from any contribution by [redacted]

F. (U) In Extraordinary Circumstances, Difficulties with All Choices Available

(U~~//FOUO~~) The Board noted the difficulty of identifying the most appropriate, reasonable proper course of action for this security incident because nearly every such course is open to objection or question:

- (U~~//FOUO~~) The Agency agreed to hold work product as off-limits, yet was required to maintain the security of its network by installing [redacted] monitoring systems that saved nearly all computer events on the SSCI portion of RDINet.
- (U~~//FOUO~~) The common agreement called for a walled-off and stand-alone network but this was not implemented so documents could be easily shared with SSCI staff. Instead, access protocols were used to approve or deny access to each document in a common database and Agency IT staff had full view of the entire network.
- ~~(TS/~~ [redacted] ~~/NF)~~ [redacted] detected unauthorized activities on the SSCI portion of RDINet and these events documented that SSCI understood the extent of monitoring applied to the network. However, the OIG never located SSCI staff signed non-disclosure agreements that would verify their knowledge and acceptance of the security agreement.
- (U~~//FOUO~~) The Board was not presented with an instruction or guidance that described what would constitute the transfer of ownership for an Agency document. The Agency retrieved documents given to SSCI in error and SSCI staff complained this violated the (unsigned) agreement. However, the Agency declined to return the documents en masse and reviewed them for privilege, while at the same time the White House agreed in communications with Senator Feinstein that these were matters that required careful, sensitive treatment.

V. (U) Recommendations

A. (U) Recommendations Addressing Specific Issues and Allegations in this Matter

~~(C//NF)~~ After examining the facts, the Board recommends no disciplinary actions are warranted for [redacted] The Board found the actions and decisions of these officers to be reasonable in light of their responsibilities to manage an unprecedented computer system. The ambiguity surrounding the agreement between the SSCI and the Agency could have created alternative Agency responses and solutions to this potential security incident, but each could also have raised questions such as those giving rise to the OIG investigation and this Board review. The violation of SSCI work product that occurred resulted from communication failures, was not ordered by the individuals under review, and happened in spite of their protective efforts.

(U~~//FOUO~~) The Board has one recommendation that could improve how the Agency handles future potential security issues with Congress, and a separate recommendation for the Inspector General's consideration.

(U~~//FOUO~~) Recommendation 1: In any future questions of this kind involving Congress, advice from the Office of Congressional Affairs should be sought. Another assessment might not alter the course chosen but could lead to a more comprehensive evaluation of the matter and greater assurance that protective measures are in fact implemented in a manner less likely to generate conflict between the branches.

(U~~//FOUO~~) Recommendation 2: While the Board disagrees with the conclusions in the matter under review, we do not question that the OIG performs a valuable public service or that it did not strive to address appropriately the issues in this matter. It would better serve its investigative purposes, and aided this board in its review, if OIG kept more complete records of interviews.

B. (U) Systemic Recommendations

(U~~//FOUO~~) The Board found four systemic problems that surfaced in this matter and from which specific recommendations are offered.

(U~~//FOUO~~) Systemic Factor 1: No Signed Agreement and a Lack of Transparency between the SSCI and CIA Regarding RDINet

((U~~//FOUO~~)) As noted, the Board disagrees with the OIG that one could conclude there was a "common understanding" between the SSCI and CIA that would have governed the actions taken to determine the existence of a security incident. The core agreement was centered on the establishment of SSCI shared drives that would be walled-off but also accessible to CIA IT staff for the purpose of IT network administration.

- There was no documentation that established agreed-upon joint (SSCI and CIA) responsibilities and procedures to be used in the event of a suspected security incident.

- Several officers and the OIG highlighted that SSCI members clicked on the standard Agency warning banner when they logged onto RDINet and this warning included the text, "use of this system may be monitored and you have no expectation of privacy." However, SSCI staff members may not have been aware that standard monitoring capabilities included [redacted]

- SSCI work product was often cited as protected but these products were not clearly defined or agreed to by both parties.

(U//~~FOUO~~) Recommendation 3: For network connectivity involving two branches of government and/or multiple lines of authority, that the D/CIA direct the program's start-up and subsequent performance reviews include specific discussion and signed documentation by each stakeholder to include terms of references, network ownership, network monitoring roles and responsibilities, incident reporting, and accountability. The agreement shall be briefed to any officer involved with the effort and separate copies shall be kept in OIG, OS, and CIC.

(U//~~FOUO~~) Systemic Factor 2: Failure to Document and Update the RDINet Agreement in Light of Experience

(U//~~FOUO~~) The IG's investigation highlighted three incidents that could have served as watershed events to refine security restrictions for access to RDINet and further show how the Agency will rely on its monitoring capabilities to investigate breaches of security. The Board could not locate an updated agreement with the exception of a summary that directed Agency officers to consult with SSCI staff members before removing documents from the Reading Room. As previously mentioned:

- ~~(TS~~ [redacted] ~~NF)~~ In December 2009 the [redacted] monitoring [redacted] detected a SSCI Staff Member [redacted] Further analysis of monitoring data revealed the same Staff Member [redacted] on the network in November and December 2009 (though the OIG reported lists 2010) and the Member was removed from the team.

- (U//~~FOUO~~) In May 2010 the RDI team removed documents from the virtual reading room after they were unintentionally comingled with documents intended for the SSCI.

- ~~(TS~~ [redacted] ~~NF)~~ CIC [redacted] in May 2010 detected a Staff Member attempting to bypass a print restriction by [redacted] The RDI team reminded the SSCI staff of the need for security of sensitive documents.

(U~~//FOUO~~) Recommendation 4: For network connectivity involving two branches of government and/or multiple lines of authority, that the D/CIA direct a quarterly review for issues that may warrant clarification, policymaker awareness, notification, or further policy guidance.

(U) Systemic Factor 3: Authorities and Operations under One Hat

(U~~//FOUO~~) [redacted] created a situation where [redacted] fundamentally authorized [redacted] to investigate the potential security incident. Splitting these responsibilities would create shared responsibility and opportunities for discussion of alternatives and checks on matters of judgment.

(U~~//FOUO~~) Recommendation 5: If at all possible, the Agency should avoid assigning operational control and [redacted] oversight to one officer.

(U~~//FOUO~~) Systemic Factor 4: The Installation of a Computer Search Tool with Access Control Deficiencies

~~(S//NF)~~ The Agency installed a Google search capability at the request of SSCI staff members but the capability had vulnerabilities that provided SSCI staff with access to CIA protected documents. The search tool was installed as early as 2010 but was not fixed until April 2013.

(U~~//FOUO~~) Recommendation 6: For network connectivity involving two branches of government and/or multiple agencies, that the Office of Security address network security issues in a timely fashion and hold quarterly reviews for issues that may warrant clarification, notification, or further policy guidance.