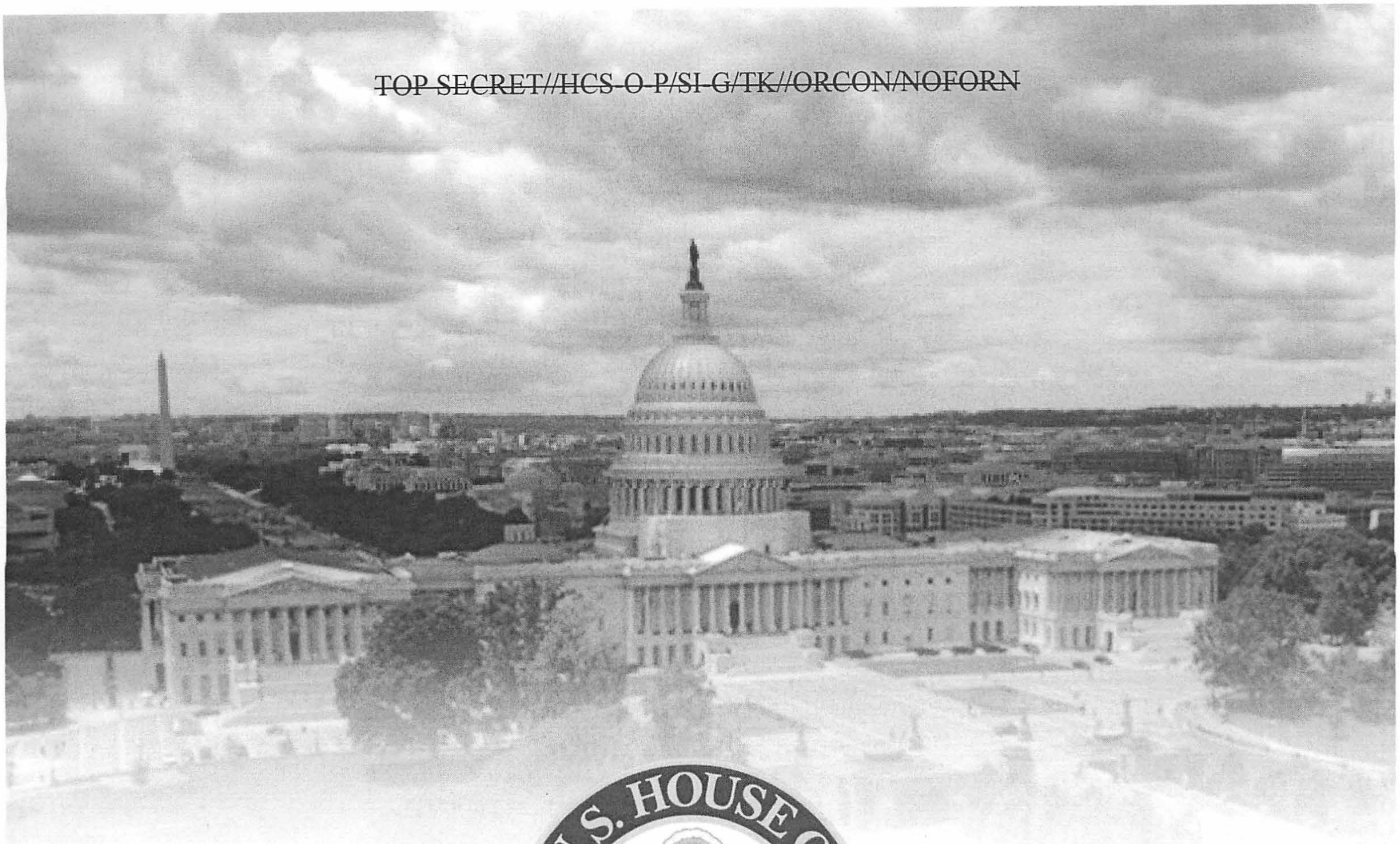

(U) Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden

September 15, 2016

(U) Executive Summary

(U) In June 2013, former National Security Agency (NSA) contractor Edward Snowden perpetrated the largest and most damaging public release of classified information in U.S. intelligence history. In August 2014, the Chairman and Ranking Member of the House Permanent Select Committee on Intelligence (HPSCI) directed Committee staff to carry out a comprehensive review of the unauthorized disclosures. The aim of the review was to allow the Committee to explain to other Members of Congress—and, where possible, the American people—how this breach occurred, what the U.S. Government knows about the man who committed it, and whether the security shortfalls it highlighted had been remedied.

(U) Over the next two years, Committee staff requested hundreds of documents from the Intelligence Community (IC), participated in dozens of briefings and meetings with IC personnel, conducted several interviews with key individuals with knowledge of Snowden's background and actions, and traveled to NSA Hawaii to visit Snowden's last two work locations. The review focused on Snowden's background, how he was able to remove more than 1.5 million classified documents from secure NSA networks, what the 1.5 million documents contained, and the damage their removal caused to national security.

(U) The Committee's review was careful not to disturb any criminal investigation or future prosecution of Snowden, who has remained in Russia since he fled there on June 23, 2013. Accordingly, the Committee did not interview individuals whom the Department of Justice identified as possible witnesses at Snowden's trial, including Snowden himself, nor did the Committee request any matters that may have occurred before a grand jury. Instead, the IC provided the Committee with access to other individuals who possessed substantively similar knowledge as the possible witnesses. Similarly, rather than interview Snowden's NSA co-workers and supervisors directly, Committee staff interviewed IC personnel who had reviewed reports of interviews with Snowden's co-workers and supervisors. The Committee remains hopeful that Snowden will return to the United States to face justice.

(U) The bulk of the Committee's 37-page review, which includes 237 footnotes, must remain classified to avoid causing further harm to national security; however, the Committee has made a number of unclassified findings. These findings demonstrate that the public narrative popularized by Snowden and his allies is rife with falsehoods, exaggerations, and crucial omissions, a pattern that began before he stole 1.5 million sensitive documents.

(U) First, Snowden caused tremendous damage to national security, and the vast majority of the documents he stole have nothing to do with programs impacting individual privacy interests—they instead pertain to military, defense, and intelligence programs of great interest to America's adversaries. A review of the materials Snowden compromised makes clear that he handed over secrets that protect American troops overseas and secrets that provide vital defenses against terrorists and nation-states. Some of Snowden's disclosures exacerbated and accelerated existing trends that diminished the IC's capabilities to collect against legitimate foreign intelligence targets, while others resulted in the loss of intelligence streams that had saved American lives. Snowden insists he has not shared the full cache of 1.5 million classified documents with anyone; however, in June 2016, the deputy chairman of the

Russian parliament's defense and security committee publicly conceded that "Snowden did share intelligence" with his government. Additionally, although Snowden's professed objective may have been to inform the general public, the information he released is also available to Russian, Chinese, Iranian, and North Korean government intelligence services; any terrorist with Internet access; and many others who wish to do harm to the United States.

(U) The full scope of the damage inflicted by Snowden remains unknown. Over the past three years, the IC and the Department of Defense (DOD) have carried out separate reviews—with differing methodologies—of the damage Snowden caused. Out of an abundance of caution, DOD reviewed all 1.5 million documents Snowden removed. The IC, by contrast, has carried out a damage assessment for only a small subset of the documents. The Committee is concerned that the IC does not plan to assess the damage of the vast majority of documents Snowden removed. Nevertheless, even by a conservative estimate, the U.S. Government has spent hundreds of millions of dollars, and will eventually spend billions, to attempt to mitigate the damage Snowden caused. These dollars would have been better spent on combating America's adversaries in an increasingly dangerous world.

(U) Second, Snowden was not a whistleblower. Under the law, publicly revealing classified information does not qualify someone as a whistleblower. However, disclosing classified information that shows fraud, waste, abuse, or other illegal activity to the appropriate law enforcement or oversight personnel—including to Congress—does make someone a whistleblower and affords them with critical protections. Contrary to his public claims that he notified numerous NSA officials about what he believed to be illegal intelligence collection, the Committee found no evidence that Snowden took any official effort to express concerns about U.S. intelligence activities—legal, moral, or otherwise—to any oversight officials within the U.S. Government, despite numerous avenues for him to do so. Snowden was aware of these avenues. His only attempt to contact an NSA attorney revolved around a question about the legal precedence of executive orders, and his only contact to the Central Intelligence Agency (CIA) Inspector General (IG) revolved around his disagreements with his managers about training and retention of information technology specialists.

(U) Despite Snowden's later public claim that he would have faced retribution for voicing concerns about intelligence activities, the Committee found that laws and regulations in effect at the time of Snowden's actions afforded him protection. The Committee routinely receives disclosures from IC contractors pursuant to the Intelligence Community Whistleblower Protection Act of 1998 (IC WPA). If Snowden had been worried about possible retaliation for voicing concerns about NSA activities, he could have made a disclosure to the Committee. He did not. Nor did Snowden remain in the United States to face the legal consequences of his actions, contrary to the tradition of civil disobedience he professes to embrace. Instead, he fled to China and Russia, two countries whose governments place scant value on their citizens' privacy or civil liberties—and whose intelligence services aggressively collect information on both the United States and their own citizens.

(U) To gather the files he took with him when he left the country for Hong Kong, Snowden infringed on the privacy of thousands of government employees and contractors. He obtained his colleagues' security credentials through misleading means, abused his access as a systems administrator to search his co-workers' personal drives, and removed the personally identifiable information of thousands of IC employees and contractors. From Hong Kong he went to Russia, where he remains a guest of the Kremlin to this day.

(U) It is also not clear Snowden understood the numerous privacy protections that govern the activities of the IC. He failed basic annual training for NSA employees on Section 702 of the Foreign Intelligence Surveillance Act (FISA) and complained the training was rigged to be overly difficult. This training included explanations of the privacy protections related to the PRISM program that Snowden would later disclose.

(U) Third, two weeks before Snowden began mass downloads of classified documents, he was reprimanded after engaging in a workplace spat with NSA managers. Snowden was repeatedly counseled by his managers regarding his behavior at work. For example, in June 2012, Snowden became involved in a fiery e-mail argument with a supervisor about how computer updates should be managed. Snowden added an NSA senior executive several levels above the supervisor to the e-mail thread, an action that earned him a swift reprimand from his contracting officer for failing to follow the proper protocol for raising grievances through the chain of command. Two weeks later, Snowden began his mass downloads of classified information from NSA networks. Despite Snowden's later claim that the March 2013 congressional testimony of Director of National Intelligence James Clapper was a "breaking point" for him, these mass downloads ***predated*** Director Clapper's testimony by eight months.

(U) Fourth, Snowden was, and remains, a serial exaggerator and fabricator. A close review of Snowden's official employment records and submissions reveals a pattern of intentional lying. He claimed to have left Army basic training because of broken legs when in fact he washed out because of shin splints. He claimed to have obtained a high school degree equivalent when in fact he never did. He claimed to have worked for the CIA as a "senior advisor," which was a gross exaggeration of his entry-level duties as a computer technician. He also doctored his performance evaluations and obtained new positions at NSA by exaggerating his résumé and stealing the answers to an employment test. In May 2013, Snowden informed his supervisor that he would be out of the office to receive treatment for worsening epilepsy. In reality, he was on his way to Hong Kong with stolen secrets.

(U) Finally, the Committee remains concerned that more than three years after the start of the unauthorized disclosures, NSA, and the IC as a whole, have not done enough to minimize the risk of another massive unauthorized disclosure. Although it is impossible to reduce the chance of another Snowden to zero, more work can and should be done to improve the security of the people and computer networks that keep America's most closely held secrets. For instance, a recent DOD Inspector General report directed by the Committee found that NSA has yet to effectively implement its post-Snowden security improvements. The Committee has taken actions to improve IC information security in the Intelligence Authorization Acts for Fiscal Years 2014, 2015, 2016, and 2017, and looks forward to working with the IC to continue to improve security.

Table of Contents

(U) Scope and Methodology

(U) Since June 2013, the unauthorized disclosures of former NSA contractor Edward Snowden and the impact of these disclosures on the U.S. Intelligence Community (IC) have been a subject of continual Committee oversight. The Committee held an open hearing on the disclosures on June 18, 2013, and, over the next year, held eight additional hearings and briefings, followed by numerous staff-level briefings on Snowden's disclosures.

(U) In August 2014, then-Chairman Rogers and Ranking Member Ruppersberger directed Committee staff to begin a review of the actions and motivations of Edward Snowden related to his removal of more than 1.5 million classified documents from secure NSA networks. The intent was not to duplicate the damage assessments already under way in the executive branch; rather, the report would help explain to other Members of Congress—and, where possible, the American people—how the "most massive and damaging theft of intelligence information in our history" occurred,[1] what the U.S. Government knows about the man who perpetrated it, and what damage his actions caused.

(U) Over the next two years, Committee staff requested hundreds of documents from the IC, participated in dozens of briefings and meetings with IC personnel, and conducted several interviews with key individuals with knowledge of Snowden's background and actions, and traveled to NSA Hawaii to visit Snowden's last two work locations.

(U) The Committee's product is a review, not an investigation, largely in deference to any criminal investigation or future prosecution. Since he arrived in Russia on June 23, 2013, Snowden has not returned to the United States to face the criminal charges against him. Accordingly, the Committee did not interview or seek documents from individuals whom the Department of Justice identified as possible witnesses at Snowden's trial, including Snowden himself, nor did the Committee request any matters that may have occurred before a grand jury. Instead, the IC provided the Committee with access to other individuals who possessed substantively similar knowledge. Similarly, rather than interview Snowden's NSA co-workers and supervisors directly, Committee staff interviewed IC personnel who had reviewed reports of interviews with Snowden's co-workers and supervisors.

(U) The Committee's review has informed numerous congressionally directed actions and resource allocation decisions in the enacted Intelligence Authorization Acts for Fiscal Years 2014, 2015, and 2016, and in the House-passed Intelligence Authorization Act for Fiscal Year 2017.

(U) Early Life

(U) Edward Joseph Snowden was born on June 21, 1983, in Elizabeth City, North Carolina. His parents, Lon Snowden, a Coast Guard chief petty officer, and Elizabeth Snowden,

[1] Testimony of Director of National Intelligence James R. Clapper, HPSCI Worldwide Threats Hearing (Open Session, Feb. 4, 2014).

a federal court clerk, moved the family to Annapolis, Maryland, when Edward was a child.[2] In 2001, his parents divorced.[3]

(U) By his own account, Snowden was a poor student.[4] He dropped out of high school in his sophomore year and began taking classes at the local community college.[5] Snowden hoped that the classes would allow him to earn a General Education Diploma (GED), but nothing the Committee found indicates that he did so. To the contrary, on an applicant resume submitted to NSA in 2012, Snowden indicated that he graduated from "Maryland High School" in 2001;[6] earlier, in 2006, Snowden had posted on a public web forum that he did not "have a degree of ANY type. I don't even have a high school diploma."[7]

(U) After leaving community college, Snowden eventually enlisted in the Army Reserve as a special forces recruit. He left after five months, receiving a discharge in September 2004 without finishing training courses.[8] Snowden would later claim he had to leave basic training because "he broke both his legs in a training accident."[9] An NSA security official the Committee interviewed took a different view, telling Committee staff that Snowden was discharged after suffering from "shin splints," a common overuse injury.[10]

(U) Unable to pursue his preferred military career, Snowden turned to security guard work. In February 2005, the University of Maryland's Center for the Advanced Study of

---

[2] "NSA Leaker Edward Snowden Has Ties to North Carolina," *Raleigh News & Observer* (Aug. 1, 2013).
[3] John M. Broder & Scott Shane, "For Snowden, A Life of Ambition, Despite the Drifting," *New York Times* (June 15, 2013).
[4] Glenn Greenwald, Ewen MacAskill, and Laura Poitras, "Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations," *The Guardian* (June 11, 2013), *available at* https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (accessed June 28, 2016).
[5] Matthew Mosk, et al., "TIMELINE: Edward Snowden's Life As We Know It," ABC News, (June 13, 2013).
[6] *See, e.g.*, Edward Snowden Resume. Regarding "High School Education," the resume Snowden submitted to NSA's Tailored Access Operations unit says as follows: For "Grad/Exit dt," Snowden wrote "2001-06-21;" For his "School," Snowden wrote "Maryland High School"; and for "Level Achieved", Snowden wrote "High School Graduate."
[7] *See supra*, note 3. One of Snowden's associates claims to have reviewed official educational records that demonstrate Snowden's passage of a high school equivalency test and receipt of high school equivalency diploma in June 2004. Any receipt of such a diploma in 2004 stands in tension with Snowden's 2006 claim to not have a "degree of any type [or]… even a high school diploma"; and with his 2012 resume, which stated that he either left or graduated from "Maryland High School" in 2001.
[8] "What We Know About NSA Leaker Edward Snowden," *NBC News* (June 10, 2013), *available at* http://usnews.nbcnews.com/_news/2013/06/10/18882615-what-we-know-about-nsa-leaker-snowden?lite (accessed June 28, 2016); *see also* "Edward Snowden Did Enlist For Special Forces, US Army Confirms," *The Guardian* (June 10, 2013), *available at* http://www.theguardian.com/world/2013/jun/10/edward-snowden-army-special forces (accessed September 15, 2016).
[9] "Edward Snowden Did Enlist For Special Forces, US Army Confirms," *The Guardian* (June 10, 2013), *available at* http://www.theguardian.com/world/2013/jun/10/edward-snowden-army-special forces (accessed September 15, 2016).
[10] *See supra*, note 6. If untreated, shin splints can progress into stress fractures, but the Committee found no evidence that Snowden was involved in a training accident.

Language (CASL) sponsored Snowden for a Top Secret security clearance.[11] The investigation for that clearance turned up only one piece of derogatory information: [redacted] of Snowden's said she did not recommend him for access to classified information.[12] Snowden sought counseling [redacted], and the counselor recommended him for a position of trust with no reservations.[13] The favorable investigation, combined with a successful polygraph test, enabled Snowden to work at CASL's lobby reception desk as a "security specialist." He worked there for four months, until he was hired by BAE Systems to work on a CIA Global Communications Services Contract.

~~(S//NF)~~ Snowden's stint as a BAE Systems contractor was similarly short-lived. For less than a year, he worked as a systems administrator who "managed installations and application rollouts" in the Washington, DC, area.[14] In August 2006, he converted from a contractor to a CIA employee. As part of that conversion, Snowden went through an "entrance on duty" psychological evaluation. [redacted].[15]

(U) CIA Employment

(U) Snowden was not, as he would later claim, a "senior advisor" at CIA.[16] Rather, his only position as a CIA employee was as a Telecommunications Information Systems Officer, or TISO. The job description for a TISO makes clear that the position is an entry-level IT support function, not a senior executive. TISOs "operate, maintain, install, and manage telecommunications systems," and "provide project management and systems integration for voice and data communications systems," including "support to customers after installation."[17] Even so, the position may have appealed to Snowden because TISOs "typically spend 60-70% of their career abroad."[18]

(U) In November 2006—less than three months after starting with CIA—Snowden contacted the Agency's Inspector General (IG) seeking "guidance" because he felt he was "being

---

[11] NSA, Edward Snowden Timeline (Sept. 30, 2014). Overall document classified C//NF; cited portion classified U//FOUO.
[12] NSA, FBI, and NCSC, "'Negative Information' Found in Edward Snowden's Personnel Security File," (Sept. 30, 2014). Overall document classified U//FOUO.
[13] *Id.*
[14] CIA Office of Security, "Response to HPSCI Staffer Meeting," (Nov. 18, 2014). Overall document classified S//NF; cited portion classified S//NF.
[15] *Id.*
[16] Laura Poitras and Glenn Greenwald, "NSA Whistleblower Edward Snowden: 'I Don't Want To Live in a Society that Does These Sorts of Things," *The Guardian* (Jun. 9, 2013), *available at* http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video (accessed May 2, 2016).
[17] CIA, Careers and Internships, "Telecommunications Information Systems Officer – Entry/Developmental," www.cia.gov (Oct. 2, 2015).
[18] *Id.*

unfairly targeted" by his supervisor.[19] After entering on duty, Snowden believed there were "morale and retention issues" among his fellow TISOs.[20] He raised those concerns with his training supervisor, the chief of the communications training unit, but "felt they were left unaddressed."[21] He next tried the chief and deputy chief of his operational group, but was similarly dissatisfied with their response.[22]

(U) Undeterred, Snowden spent the next week surveying the other TISOs who entered on duty at the same time as him.[23] He wrote up his findings and sent them to the CIA's Strategic Human Capital Office. Then, instead of attempting to raise his concerns again with his supervisor or work collaboratively with other TISOs to resolve the concerns, Snowden sent his concerns to the Deputy Director of CIA for Support—the head of the entire Directorate of Support and one of the ten most senior executives of CIA.[24]

(U) In his e-mail, Snowden complained about the process of assigning new TISOs to overseas locations, the pay of TISOs compared to contractors who performed similar work, and the difficulty for TISOs to transfer laterally to other jobs.[25]

~~(C)~~ Despite his lack of experience, the 23-year-old Snowden told the Deputy Director he felt "pretty disenfranchised" because his immediate supervisors did not take his unsolicited recommendations to heart.[26]

(U) Snowden told the IG that, after he contacted the Deputy Director for Support, his supervisors pulled him in to their offices for unscheduled counseling. In his view, they were "extremely hostile" and "seem[ed] to believe I have trouble bonding with my classmates."[27] Those counseling sessions prompted Snowden to contact the IG to help protect him from "reprisal for speaking truth to power."

(U) One day after receiving his complaint, an IG employee responded to Snowden and recommended he contact the CIA's Ombudsman, an official who could help Snowden sort through the options available to him and mediate disputes between managers and employees.[28] The IG employee also directed Snowden to the relevant Agency regulation regarding the factors managers could consider when deciding to retain an employee beyond the initial three-year trial period.[29] Whether that response satisfied Snowden is unclear; shortly after receiving it, Snowden sent another message to the IG employee instructing him to disregard the initial request because

[19] E-mail from Snowden to CIA Office of Inspector General (Nov. 2, 2006). Overall document classified S; cited portion marked U//AIUO.
[20] *Id.* Overall document classified S; cited portion not portion-marked.
[21] *Id.* Overall document classified S; cited portion not portion-marked.
[22] *Id.* Overall document classified S; cited portion not portion-marked.
[23] *Id.* Overall document classified S; cited portion not portion-marked.
[24] *Id.* Overall document classified S; cited portion not portion-marked.
[25] *Id.* Overall document classified S; cited portion not portion-marked.
[26] *Id.* Overall document classified S; cited portion classified C.
[27] *Id.* Overall document classified S; cited portion not portion-marked
[28] E-mail from CIA Office of Inspector General to Edward Snowden (Nov. 3, 2006). Overall document classified S; cited portion classified U//AIUO.
[29] *Id.* Overall document classified S; cited portion classified U//AIUO.

the issue had been "addressed."[30] During the rest of his time at CIA, Snowden did not contact the IG.

~~(S)~~ After the completion of his training, Snowden was assigned to [redacted] in March 2007 for his first TISO assignment.[31] Snowden was, in the words of his supervisor, "an energetic officer" with a "plethora" of experience on Microsoft operating systems, but he "often does not positively respond to advice from more senior officers, . . . does not recognize the chain of command, often demonstrates a lack of maturity, and does not appear to be embracing the CIA culture."[32]

~~(S)~~ A few months after starting in [redacted], Snowden asked to apply for a more senior position in [redacted] as a regional communications officer. His supervisor did not endorse his application. When he was not selected for the position, Snowden responded by starting "a controversial e-mail exchange with very senior officers" in which he questioned the selection board's professional judgment.[33] Years later, when characterizing his experience as a CIA TISO, Snowden would write that he was "specially selected by [CIA's] Executive Leadership Team for [a] high-visibility assignment" that "required exceptionally wide responsibility."[34] The description is in tension with his supervisor's account of a junior officer who "needed more experience before transitioning to such a demanding position."[35]

~~(S)~~ Snowden also modified CIA's performance review software in connection with his annual performance review, by manipulating the font.[36] This behavior led to Snowden's recall for "professional consultations" with the head of all CIA technical officers in Europe.[37] This was the first but not the only time more senior CIA officers attempted to correct Snowden's behavior. His supervisor in [redacted] cataloged six counseling sessions between October 2007 and April 2008, nearly one per month, regarding his behavior at work.[38] In September 2008, Snowden requested to leave [redacted] "short of tour," that is, before his scheduled rotation date to a new assignment.[39] The request was denied. Disobeying orders, Snowden traveled back to the Washington, D.C., area for his and his fiancée's medical appointments. Because of his disobedience, Snowden's supervisors recommended he not return to [redacted].[40]

---

[30] E-mail from Snowden to CIA Office of Inspector General (Nov. 3, 2006). Overall document classified S; cited portion classified U//AIUO.

[31] NSA, Edward Snowden Timeline (Sept. 30, 2014); overall document classified C//NF; cited portion classified C//NF.

[32] Memorandum for the Record by Senior Telecommunications Officer – Europe, "TISO [redacted]—Edward Snowden" (Sept. 4, 2008).

[33] CIA Office of Security, "Response to HPSCI Staffer Meeting," (Nov. 18, 2014).

[34] Edward Snowden Resume.

[35] Memorandum for the Record by Senior Telecommunications Officer – Europe, "TISO [redacted]—Edward Snowden" (Sept. 4, 2008). Overall document classified S//NF; cited portion classified S.

[36] *Id.* Overall document classified S//NF; cited portion classified S.

[37] *Id.* Overall document classified S//NF; cited portion classified S.

[38] Memorandum for the Record by Office in Charge, [redacted], "TISO [redacted]—Edward Snowden" (Dec. 18, 2008). Overall document classified S//NF; cited portion classified S.

[39] *Id.* Overall document classified S//NF; cited portion classified S.

[40] *Id.* Overall document classified S//NF; cited portion classified S.

~~(S//NF)~~ In January 2009, CIA submitted a "fitness for duty" report for Snowden, an administrative tool to determine whether Snowden had any work-related medical issues.[41] The Agency also assigned him to a position in the Washington, D.C., area so he could be available for any medical appointments.[42]

~~(S//NF)~~ Several years later, Snowden claimed that, while in [redacted], he had ethical qualms about working for CIA.[43] None of the memoranda for the record detailing his numerous counseling sessions mention Snowden expressing any concerns about [redacted]. Neither the CIA IG nor any other CIA intelligence oversight official or manager has a record of Snowden expressing any concerns about the legality or morality of CIA activities.

(U) Transition to NSA Contractor

~~(C//NF)~~ Around the same time that Snowden returned to the D.C. area, he applied for a position with an NSA contractor, Perot Systems, as a systems administrator. He was still a CIA employee at the time and his clearance remained in good standing with no derogatory information.[44] On March 25, 2009, Perot Systems sponsored Snowden for employment; six days later, on March 31, NSA Security checked the Intelligence Community-wide security database, "Scattered Castles," to verify Snowden's clearance.[45]

(U) Seeing no derogatory information in Scattered Castles, NSA Security approved Snowden for access eight days later, on April 7.[46]

~~(S//NF)~~ On April 16, Snowden formally resigned as a CIA employee.[47] CIA's Security Office updated his Scattered Castles record on April 20, [redacted].[48] Because NSA had checked the database three weeks earlier, NSA Security did not learn of the [redacted] in his record at that time.[49] It is unclear if NSA Security would have treated Snowden's onboarding any differently had NSA been aware of [redacted].

[41] CIA Office of Security, "Response to HPSCI Staffer Meeting," (Nov. 18, 2014). Overall document classified S//NF; cited portion classified S//NF.
[42] *Id.* Overall document classified S//NF; cited portion classified S//NF.
[43] [redacted]
[44] NSA, Edward Snowden Timeline (Sept. 30, 2014). Overall document classified C//NF; cited portion classified C//NF.
[45] *Id.* Overall document classified C//NF; cited portion classified U//FOUO.
[46] *Id.* Overall document classified C//NF; cited portion classified U//FOUO.
[47] *Id.* Overall document classified C//NF; cited portion classified C//NF.
[48] CIA Office of Security, "Response to HPSCI Staffer Meeting," (Nov. 18, 2014). Overall document classified S//NF.
[49] NSA, Edward Snowden Timeline (Sept. 30, 2014). Overall document classified C//NF; cited portion classified C//NF. The alerting function for [redacted] in Scattered Castles has since been fixed.

(U) From May 2009 to February 2012, Snowden worked in a variety of roles supporting IC contracts for Dell, which had purchased Perot Systems in 2009. He worked as an IT systems administrator at NSA sites in [redacted] for a little more than a year, where he supported NSA's Agency Extended Information Systems Services (AXISS) contracts.[50]

(U) One co-worker recalled that while he was working in [redacted], Snowden traveled to Thailand to learn how to be a ship's captain, but never finished the training course. According to another co-worker, at some point before he was stationed in [redacted], Snowden took a trip to China and spoke about his admiration for the Chinese people and Chinese martial arts.[51] The same co-worker remembered Snowden expressing his view that the U.S. government had overreached on surveillance and that it was illegitimate for the government to obtain data on individuals' personal computers.[52] There are no indications of how Snowden attempted to square this belief with his continued employment in support of the foreign signals intelligence mission of NSA.

(U) Other co-workers from Snowden's time in [redacted] recalled him as someone frustrated with his lack of access to information. One remembered Snowden complaining how he lacked access at CIA;[53] another recalled him attempting to gain access to information about the war in Iraq that was outside of his job responsibilities.[54] Although Snowden did not obtain the information he was looking for, he later claimed it was "typical" of the U.S. government to cover up embarrassing information.[55]

~~(C//NF)~~ In September 2010, Snowden returned to the United States and Dell attempted to move him to a position where he would support IT systems at CIA. Because of the [redacted] in Scattered Castles, however, CIA refused to grant Snowden access to its information.[56] Dell put Snowden on leave for three months while waiting for a position that did not require a security clearance to open up. Eventually, one did: In December 2010, Snowden started work in an uncleared "systems engineer/pre-sales technical role" for Dell supporting a CIA contract.[57]

(U) Snowden was also due for a periodic background reinvestigation in the fall of 2010. OPM contractor U.S. Information Services completed that review in May 2011, finding no derogatory information. According to an after-the-fact review by the National Counterintelligence Executive, the reinvestigation was "incomplete" and "did not present a complete picture of Mr. Snowden."[58] Among its other flaws, the investigation never attempted to verify Snowden's CIA employment or speak to his CIA supervisors, nor did it attempt to independently verify Snowden's self-report of a past security violation—areas where further

[50] *Id.* Overall document classified C//NF; cited portion classified U//FOUO.
[51] Interview with NSA Attorney (Feb. 8, 2016) (report of interview with [redacted]).
[52] *Id.* The same co-worker, [redacted], also mentioned that Snowden considered himself a privacy advocate.
[53] Interview with NSA Attorney (Feb. 8, 2016) (report of interview with [redacted]).
[54] *Id.* (report of interview with [redacted]).
[55] *Id.* (report of interview with [redacted]).
[56] NSA, Edward Snowden Timeline (Sept. 30, 2014). Overall document classified C//NF; cited portion classified C//NF.
[57] *Id.* Overall document classified C//NF; cited portion classified C//NF.
[58] National Counterintelligence Executive, Technical and quality review of the April 2011 Single Scope Background Investigation – Periodic Reinvestigation on Mr. Snowden," (Aug. 23, 2013); overall document classified U//FOUO.

information could have alerted NSA to CIA's concerns.[59] Contrary to best practices, the investigation also failed to develop any character references beyond the two people Snowden himself listed, his mother and his girlfriend. [60]

~~(S)~~ From August 31, 2011, to January 11, 2012, Snowden took a leave of absence from Dell. His Dell co-workers offered conflicting accounts of how he spent his leave,[61] [redacted]

(U) NSA Hawaii – Contract Systems Administrator

(U) Snowden returned from leave in early 2012 and took a position as a general systems administrator supporting Dell's AXISS work at NSA's Hawaii Cryptologic Center.[62] As part of the change in station, he took a counterintelligence polygraph examination. The first exam was "inconclusive," but did not lead to NSA Security developing any further information; the second was successful.[63] At the end of March 2012, Snowden moved to Hawaii.

(U) The job Snowden performed in Hawaii was similar to his duties during the previous three years with Dell. He was a field systems administrator, working in technical support office of NSA Hawaii. Some of his work involved moving large numbers of files between different internal Microsoft SharePoint servers for use by other NSA Hawaii employees. Although most NSA Hawaii staff had moved to a new building at the start of 2012, Snowden and other technical support workers remained in the Kunia "tunnel," an underground facility originally built for aircraft assembly during World War Two.

(U) Snowden had few friends among his co-workers at NSA Hawaii.[64] Those co-workers described him as "smart" and "nerdy," but also someone who was "arrogant," "introverted," and "squirrelly"; an "introvert" who frequently "jumped to conclusions."[65] His supervisors found his work product to be "adequate," but he was chronically late for work, frequently not showing up until the afternoon.[66] Snowden claimed he had trouble waking up on time because he stayed up late playing video games.[67]

(U) Few of Snowden's Hawaii co-workers recall him expressing political opinions. One remembered a conversation in which Snowden claimed the Stop Online Piracy Act and the

---

[59] *Id.*
[60] *Id.*
[61] Interview with NSA Attorney (Feb. 8, 2016).
[62] NSA, Edward Snowden Timeline (Sept. 30, 2014). Dell Federal was a subcontractor to CACI International for NSA's AXISS Field IT support contracts. E-mail from NSA Legislative Affairs to HPSCI Staff, "Responses to Your Questions on Read and Return Documents for HPSCI Media Leaks Review," (Dec. 2, 2014, at 3:47 PM). Overall document cited U//FOUO; cited portion classified U//FOUO.
[63] *Id.*
[64] Interview with NSA Security Official (Jan. 28, 2016).
[65] Interview with NSA Attorney (Jan. 28, 2016).
[66] *Id.*
[67] *Id.*

Protect Intellectual Property Act would lead to online censorship.[68] In the same conversation, Snowden told his colleague that he had not read either bill.[69] The same co-worker recalled Snowden once claiming that, based on his meetings with Chinese hackers at a conference, the United States caused problems for China but China never caused problems for the United States.[70] Although no other co-worker in Hawaii recalled Snowden expressing any sympathy for foreign governments, a different co-worker from the Kunia tunnel remembered that Snowden defended the actions of Private Bradley Manning.[71]

(U) One incident early in Snowden's time at NSA Hawaii merits further description. In June 2012, Snowden installed a patch to a group of servers on classified networks that supported NSA field sites, including NSA Hawaii. Although the patch was intended to fix a vulnerability to the classified servers, the patch caused the servers to crash, resulting in a loss of network access for several NSA sites.[72] One of NSA's senior technical support managers, a government employee, fired off an e-mail to a number of systems administrators, asking who had installed the troublesome patch and sarcastically chiding that individual for failing to test the patch before loading it.[73]

(U) Snowden replied to all the recipients and added the deputy head of NSA's technical services directorate to the e-mail thread. This individual was several levels above the immediate government supervisors whom Snowden could have contacted first. Calling the initial e-mail "not appropriate and . . . not helpful," Snowden accused the middle manager of focusing on "evasion and finger-pointing rather than problem resolution."[74]

(U) Snowden received a quick rebuke. The NSA civilian employee in Washington responsible for managing field AXISS contracts sent Snowden an e-mail telling him his response was "totally UNACCEPTABLE" because "[u]nder no circumstances will any contractor call out or point fingers at any government manager whether you agree with their handling of an issue or not."[75] She further instructed Snowden that if he "felt the need to discuss with any management it should have been done with the site management you are working with and no one else."[76]

~~(S)~~ That weekend, Snowden came in to work [redacted][77]

[68] Interview with NSA Attorney (Jan. 28, 2016) (citing co-worker [redacted]).
[69] *Id.* (citing co-worker [redacted])
[70] *Id.* (citing co-worker [redacted])
[71] *Id.*; Interview with NSA Attorney (Feb. 8, 2016) (citing co-worker [redacted]).
[72] Interview with [redacted] (Oct. 28, 2015).
[73] E-mail from [redacted], "RE: (U) ICA-tcp issues with KB2653956," (Jun. 21, 2012, at 1:20AM). Overall document classified U//FOUO.
[74] E-mail from Edward Snowden, "RE: (U) ICA-tcp issues with KB2653956," (Jun. 21, 2012, at 1:00PM). Overall document classified U//FOUO.
[75] E-mail from [redacted], "(U) E-mail you sent in response to ICA-tcp issues with a patch," (Jun. 22, 2012, at 3:26AM). Overall document classified U//FOUO.
[76] *Id.*
[77] Interview with NSA Security Official (Jan. 28, 2016).

(U) The following Monday, he sent an e-mail to the NSA middle manager saying he "understood how bad this e-mail looked for what was intended to be a relatively benign message" and acknowledging that the e-mail "never should have happened in the first place."[78] The manager accepted the apology, explaining that his problem with the message "had nothing to do with the content but with distribution" because he did not understand "the elevation of the issue to such a high management level"; that is, to the deputy head of NSA's technical services directorate.[79]

(U) Snowden would later publicly claim that his "breaking point"—the final impetus for his unauthorized downloads and disclosures of troves of classified material—was March 2013 congressional testimony by Director of National Intelligence James Clapper.[80]

~~(S//REL TO USA, FVEY)~~ But only a few weeks after his conflict with NSA managers, on July 12, 2012—eight months before Director Clapper's testimony—Snowden began the unauthorized, mass downloading of information from NSA networks.[81] [redacted][82] [redacted][83]

(U) Snowden's Downloading and Removal Process

(U) Snowden used several methods to gather information on NSA networks, none of which required advanced computer skills.

(U) At first, Snowden used blunt tools to download files en masse from NSA networks. Two non-interactive downloading tools, commonly known as "scraping" tools, called "wget" and DownThemAll! were available on NSA classified networks for legitimate system administrator purposes.[84] Both tools were designed to allow users to download large numbers of files over slow or unstable network connections.[85] Snowden used the two tools with a list of website addresses, sometimes writing simple programming scripts to generate the lists. For

---

[78] E-mail from Edward Snowden, "RE: (U) ICA-tcp issues with KB2653956" (Jun. 25, 2012, at 2:31AM). Overall document classified U//FOUO.

[79] E-mail from [redacted], "RE: (U) ICA-tcp issues with KB2653956" (Jun. 25, 2012, at 1:51AM). Overall document classified U//FOUO.

[80] "Transcript: ARD Interview with Edward Snowden," (Jan. 26, 2014), *available at* https://edwardsnowden.com/2014/01/27/video-and-interview-with-edward-snowden.

[81] NSA, Edward Snowden Timeline (Sept. 30, 2014). Overall document classified C//NF; cited portion classified C//REL TO USA, FVEY.

[82] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL.

[83] [redacted]

[84] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified U//FOUO

[85] *Id.* Overall document classified S//REL TO USA, FVEY; cited portion classified U//FOUO

instance, if NSA webpages were set up in numerical order (i.e., page 1, page 2, page 3, and so on), Snowden programmed a script to automatically collect the pages.[86] Neither scraping tool targeted areas of potential privacy or civil liberties concerns; rather, Snowden downloaded *all* information from internal NSA networks and classified webpages of other IC elements.[87]

~~(S//NF)~~ [redacted][88].

~~(S//REL)~~ [redacted][89]. [redacted][90].

(U) Exceeding the access required to do his job, Snowden next began using his systems administrator privileges to search across other NSA employees' personal network drives and copy what he found on their drives.[91] Snowden also enlisted his unwitting colleagues to help him, asking several of his co-workers for their security credentials so he could obtain information that they could access, but he could not.[92] One of these co-workers subsequently lost his security clearance and resigned from NSA employment.[93]

~~(S//REL)~~ Snowden infringed the privacy of at least [redacted] NSA personnel by searching their network drives without their permission, removing a copy of any documents he found to be of interest.[94] [redacted][95] [redacted][96]

---

[86] *Id.* Overall document classified S//REL TO USA, FVEY; cited portion classified U//FOUO

[87] *Id.* Overall document classified S//REL TO USA, FVEY; cited portion classified U//FOUO

[88] NSA, "HPSCI Recollection Summary Paper," (Jan. 26, 2015). Overall document classified S//NF; cited portion classified S//NF. *See infra* for a more detailed description of the files Snowden removed.

[89] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY.

[90] Interview with NSA Security Official (Jan. 28, 2016). [redacted]

[91] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified U//FOUO.

[92] HPSCI Memorandum for the Record, NSA Briefing to HPSCI Staff (July 22, 2013).

[93] NSA Legislative Affairs Memorandum to Staff Director and Minority Staff Director (Feb. 10, 2014). Overall document classified U; document not portion-marked.

[94] Interview with NSA Security Official (Jan. 28, 2016); NSA, "Number of Personal Network Drives Searched," (Mar. 14, 2016). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY.

[95] Interview with NSA Security Official (Jan. 28, 2016).

[96] *Id.*

(U) Snowden's searches quickly expanded beyond surveillance programs. Some of the personal network drives Snowden searched belonged to individuals involved in the hiring decision for a job for which Snowden had applied. On these individuals' network drives, Snowden searched for human resources files and files related to the promotion and hiring decisions.[97]

~~(S//REL)~~ Snowden first saved the information he gathered on his personal network drive.[98] At some point in 2012, a fellow systems administrator noticed that Snowden's personal drive used a significantly larger amount of memory than most other employees and asked him what he was doing.[99] Snowden responded that he was downloading system patches for NSA networks, a task that was consistent with his job responsibilities.[100] [redacted][101]

(U) In late August 2012, Snowden requested a "thin-on-thick" machine for his desk.[102] At the time, NSA Hawaii was in the middle of a transition from "thick clients,"—physical desktop computers at each worker's desk, to "thin clients,"—virtual desktops hosted on servers. On a "thin client," there is no traditional desktop computer at workers' desks, rather, each user has a client that provides a display and input, with computing processors, memory, and storage on network servers. Snowden's "thin-on-thick" setup meant that he had a physical desktop computer at his desk, but he only used its computing power and hard drive to operate a virtual computer. This "thin-on-thick" setup allowed NSA Hawaii to reap some of the benefits of thin clients, such as uniform security policies and improved information sharing, without the cost of buying new thin client devices. NSA Hawaii could also make use of a large quantity of "thick client" desktop computers it had recently purchased.[103] Yet the thin-on-thick setup opened up a loophole for Snowden to exploit.

~~(S//NF)~~ Snowden knew NSA's networks recorded and logged every action by users on thick client workstations while connected to the network.[104] He also knew that auditing controls

---

[97] NSA, "Number of Personal Network Drives Searched," (Mar. 14, 2016). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY.
[98] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY.
[99] Interview with NSA Attorney (Jan. 28, 2016).
[100] *Id.*
[101] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY.
[102] NSA Response to HPSCI Question on Thin-on-Thick Computer at Snowden's Workstation (Mar. 2, 2016). Overall document classified S//NF; cited portion classified S//NF. Because thin-on-thick workstations were prevalent at NSA Hawaii at the time, Snowden did not have to go through any special approval process to obtain a thin-on-thick workstation.
[103] Interview with NSA Security Official (Jan. 28, 2016).
[104] NSA, "Response to HPSCI Document Request – Question # 10" (May 1, 2015). Overall document classified S//NF; cited portion classified S//NF. [redacted]

would send an alert to network security personnel if he tried to remove data from the network. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted][106]

~~(S//REL)~~ [redacted][108]

~~(S//REL)~~ There is no evidence that NSA was aware of this specific vulnerability to its networks. Because Snowden's legitimate work responsibilities involved transferring large amounts of data between different SharePoint servers, the large quantities of data he copied as Step 1 of the exfiltration process did not trigger any NSA alerts for abnormal network traffic.[109]

---

[105] NSA, "Purpose of Functioning CD-ROM and USB Drive," (Mar. 14, 2016). Overall document classified S//REL USA, FVEY; cited portion classified S//REL USA, FVEY.

[106] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY. *See also id.* for additional details on the NSA forensics process that allowed for the reconstruction of Snowden's methods.

[107] [redacted]

[108] Interview with NSA Security Official (Jan. 28, 2016).

[109] NSA, "Response to HPSCI Document Request – Question # 10" (May 1, 2015). Overall document classified S//REL USA, FVEY; cited portion classified S//REL USA, FVEY. Although Snowden, as a systems administrator, was authorized to transfer large quantities of data on the NSA network, he was *not* authorized to remove data from the network for his intended purpose of later transferring it to removable media so he could disclose it.

[redacted][110]

(U) NSA Hawaii – Gaining More Access and Departing for China and Russia

(U) After he began removing documents in the summer of 2012, Snowden spent several months applying for employment as a NSA civilian. In September 2012, he took a test to obtain a position in the Tailored Access Operations office, or TAO, the group within NSA responsible for computer network exploitation operations. After finding the test and its answers among the documents he had taken off of NSA networks, he passed the test.[111] Based on the test result and his exaggerated resume,[112] TAO offered him a position. The pay grade TAO offered, however—a GS-12 position that would have paid around $70,000 per year—was not sufficient for Snowden. He instead believed he should have been offered a GS-15 position that would have paid nearly $120,000 per year.[113]

~~(C)~~ [redacted][114]

(U) In early December 2012, Snowden attempted to contact journalist Glenn Greenwald. To hide his identity, Snowden used the pseudonym "Cincinnatus" and asked Greenwald for his public encryption key so Snowden could send him documents securely.[115] In January 2013, he contacted filmmaker Laura Poitras.[116]

(U) In late March 2013, Snowden finally obtained a new position, not with NSA as a civilian but with Booz Allen Hamilton as a contractor.[117] He would be a SIGINT Development Analyst, meaning he analyzed foreign networks and cyber operators to help NSA's National Threat Operation Center (NTOC) in its cyber defense efforts. NTOC's operations helped defend U.S. military networks from attacks by foreign cyber actors, including Russia and China.

---

[110] NSA, "Purpose of Functioning CD-ROM and USB Drive," (Mar. 14, 2016).
[111] Bryan Burrough, Sarah Ellison, and Suzanna Andrews, "The Snowden Saga: A Shadowland of Secrets and Light," *Vanity Fair* (May 2014), *available at* www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview (quoting NSA Deputy Director Rick Ledgett).
[112] Edward Snowden Resume (June 28, 2012). Snowden described himself as a "Senior Advisor" at "Dell/NSA/CIA/DIA" rather than as a systems administrator. Resume inflation was a habit for Snowden—in the files he sent to Glenn Greenwald, he described himself as an NSA Special Advisor "under corporate cover" and as a former CIA "field officer." *See* Glenn Greenwald, No Place to Hide at 32.
[113] Interview with NSA Security Official (Jan. 28, 2016).
[114] NSA, Edward Snowden Timeline (Sept. 30, 2014).
[115] Glenn Greenwald, No Place to Hide at 7 (2014).
[116] NSA, Edward Snowden Timeline (Sept. 30, 2014).
[117] NSA, Edward Snowden Timeline (Sept. 30, 2014).

~~(C//NF)~~ In his new position, Snowden had access to more documents on NSA networks, many of which he later removed.[118] Because there was not a thin-on-thick workstation at Snowden's new desk, he had to return after hours to his old desk—located at a different NSA facility a twenty-minute drive away—to exfiltrate documents [redacted].[119] His NTOC job did not require him to visit his old building, so he had no reason other than document removal to return.[120]

(U) On May 15, 2013, Snowden told his Booz Allen Hamilton supervisor that he needed to take two weeks of leave without pay to return to the continental United States for medical reasons.[121] According to his supervisor, Snowden had previously claimed he suffered from epilepsy, [122] although he never presented evidence of a diagnosis from any doctor.[123] Four days later, Snowden flew to Hong Kong without telling either his girlfriend or his mother (who was in Hawaii at the time visiting him) where he was going.[124] The Committee found no conclusive evidence indicating why Snowden chose Hong Kong as his destination, but, according to later accounts, Snowden believed he would be safe in the city based on its tradition of free speech.[125]

(U) On Friday May 31, Snowden's leave without pay ended. The following Monday, June 3, Booz Allen Hamilton started looking for him.[126] Two days later, on June 5, Booz Allen reported Snowden to NSA's Office of Security and Greenwald published the first of Snowden's disclosures.[127]

(U) Four days after the first Greenwald articles were published, Snowden revealed himself as the source of the disclosures.[128] According to press reports, between June 10 and June 23, Snowden hid in the apartments of refugees in Hong Kong while his lawyer worked to arrange transit for him out of the city.[129] On June 23, 2013, he flew from Hong Kong to Moscow's Sheremetyvevo airport, accompanied by Wikileaks activist Sarah Harrison.[130] The next day, he failed to appear on a flight to Havana and disappeared from public view until August 1, 2013, when Russia granted him asylum and he left the airport.[131] As of September 15, 2016, Snowden remains in Russia.

---

[118] Interview with NSA Security Official (Jan. 28, 2016).
[119] NSA, "Response to HPSCI Document Request – Question #2" (June 24, 2015). Overall document classified S//NF; cited portion classified C//REL.
[120] *Id.* Cited portion classified C//REL.
[121] NSA, Edward Snowden Timeline (Sept. 30, 2014).
[122] Interview with NSA Attorney (Jan. 28, 2016) (citing BAH supervisor).
[123] Interview with NSA Security Official (Jan. 28, 2016).
[124] NSA, Edward Snowden Timeline (Sept. 30, 2014); Interview with NSA Security Official (Jan. 28, 2016).
[125] *See* Luke Harding, The Snowden Files (2014) at 108.
[126] NSA, Edward Snowden Timeline (Sept. 30, 2014).
[127] Glenn Greenwald, "Verizon Order: NSA Collecting Phone Records of Millions of Americans Daily," *The Guardian* (June 5, 2013).
[128] *See* Luke Harding, The Snowden Files (2014) at 146-52.
[129] Theresa Tedesco, "How Snowden Escaped," *National Post* (Sept. 6, 2016), *available at* http://news.nationalpost.com/features/how-edward-snowden-escaped-hong-kong/
[130] Luke Harding, The Snowden Files (2014) at 224.
[131] *Id.* at 229-30, 250.

~~(S//NF)~~ [redacted].[132] Additionally, although Snowden's objective may have been to inform the public, the information he released is also available to Russian, Chinese, Iranian, and North Korean intelligence services; any terrorist with Internet access; and many others who wish to do harm to the United States.

~~(S//NF)~~ When he fled Hong Kong, Snowden left a number of encrypted computer hard drives behind. [redacted][133]

(U) Communications with Intelligence Oversight Personnel

(U) In March 2014 public testimony to the European Parliament, Snowden claimed that he reported his concerns about "clearly problematic programs to more than ten distinct officials" at NSA.[134] Snowden also publicly stated that he "specifically expressed concern about [NSA's] suspect interpretation of the law," inviting "members of Congress to request a written answer to this question [from the NSA]."[135] The Committee requested such an answer from NSA,[136] and found no evidence to support these claims. The Committee further found no evidence that Snowden attempted to communicate concerns about the legality or morality of intelligence activities to any officials, senior or otherwise, during his time at either CIA or NSA.

(U) As already described, one of Snowden's Hawaii co-workers recalls him defending Bradley Manning's actions,[137] another remembered him criticizing bills under consideration in Congress that he regarded as harmful to online privacy[138] and criticizing U.S. foreign policy toward China.[139] None of his co-workers or his supervisors, however, recall Snowden raising concerns about the legality or morality of U.S. intelligence activities.[140]

---

132 DIA, Information Review Task Force-2, "Initial Assessment" (Dec. 26, 2013), at 3. Overall document classified TS//SI//RSEN/OC/NF; cited portion classified S//NF.

133 HPSCI Memorandum for the Record, Insider Threat/Counterintelligence Monthly Briefing (Feb. 4, 2014).

134 Edward Snowden, Testimony to the European Parliament (Mar. 7, 2014) at 6.

135 Bryan Burrough, Sarah Ellison, and Suzanna Andrews, "The Snowden Saga: A Shadowland of Secrets and Light," *Vanity Fair* (May 2014), *available at* www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview.

136 Letter from HPSCI Chairman Mike Rogers to Director James Clapper (Aug. 5, 2014) (requesting, among other things, "[a]ll communications between Edward Snowden and any IC or Department of Defense compliance, legal, or Inspector General personnel").

137 *See supra*, note 71.

138 *See supra*, note 68.

139 *See supra*, note 70.

140 Interview with NSA Attorney (Jan. 28, 2016) (citing supervisors, co-workers). The co-worker who recalled Snowden defending Manning expressly mentioned that Snowden did not believe Americans' privacy rights were being violated and that Snowden had no qualms about the legality of the NSA mission. *See* Interview with NSA Attorney (Feb. 8, 2016) (citing co-worker [redacted]).

(U) Neither did Snowden raise any concerns with IC oversight personnel. As previously discussed, Snowden contacted the CIA IG within a few months of his start at the Agency to complain about training issues and management style, but he later dropped the complaint.[141] He did not contact the NSA IG, the Department of Defense (DOD) IG, or the Intelligence Community (IC) IG, all of whom could have responded to a complaint regarding unlawful intelligence activities. Nor did Snowden attempt to contact the Committee or the Senate Select Committee on Intelligence through the procedures available to him under the Intelligence Community Whistleblower Protection Act (IC WPA). He could have done this anonymously if he feared retribution.

(U) Snowden did, however, contact NSA personnel who worked in an internal oversight office about his personal difficulty understanding the safeguards against unlawful intelligence activities. While on a trip to NSA headquarters at Ft. Meade in June 2012, Snowden visited a training officer in the internal oversight and compliance office of the Signals Intelligence Directorate. The training officer remembered that Snowden was upset because he had failed NSA's internal training course on how to handle information collected under FISA Section 702, the legal authority by which the government can target the communications of non-U.S. persons outside the United States.[142]

(U) The internal training is a rigorous computer-based course that walks NSA employees and contractors through the laws and regulations that govern the proper handling of information collected under the authority of FISA Section 702, including information collected under the programs Snowden would later disclose, PRISM and "upstream" collection. At the end of the course, NSA personnel take a scenario-based test to gauge their comprehension of the material; if they do not receive a minimum score on the test, they must retake the computer-based training course. All of the answers to the test questions can be found within the training material. After three failures of the computer-based course, the individual must attend an in-person training course to ensure they are able to understand the rules governing Section 702, including privacy protections.

(U) According to the training officer, Snowden had failed the computer-based training course and was afraid of the consequences.[143] He was also upset because he believed the course was rigged.[144] After the training officer explained to Snowden that he could take the course again—and that careful reading would allow him to find all of the answers to the test—Snowden became calm and left the oversight and compliance office.[145] At no point during his visit to the compliance office did Snowden raise any concerns about how NSA used Section 702, PRISM, or "upstream" collection.[146]

[141] *See supra*, notes 19 through 30.
[142] NSA, "OVSC1203 Issue Regarding Course Content and Trick Questions," overall document classified TS//NF; cited portion classified U//FOUO.
[143] Interview with [redacted] (Oct. 28, 2015).
[144] *Id*
[145] *Id.*
[146] *Id.*

(U) In April 2013—after he had removed documents multiple times from NSA systems—Snowden contacted the NSA Office of General Counsel with a question about a different training course.[147] He was curious about the mandatory training on United States Signals Intelligence Directive 18, which is the foundational authority for NSA's collection activities overseas targeting foreigners.[148] Specifically, he believed the training erroneously accorded the same precedence to statutes and executive orders. A few days later, an NSA attorney clarified that while executive orders have the force of law, they cannot trump a statute.[149] Snowden did not respond to that e-mail; he also did not raise any concerns about the legality or morality of U.S. intelligence activities.[150]

(U) Was Snowden a Whistleblower?

(U) As a legal matter, during his time with NSA, Edward Snowden did not use whistleblower procedures under either law or regulation to raise his objections to U.S. intelligence activities, and thus, is not considered a whistleblower under current law. He did not file a complaint with the DOD or IC IG's office, for example, or contact the intelligence committees with concerns about fraud, waste, abuse, mismanagement, or violations of law. Instead, Snowden disclosed classified information to the press.

(U) Snowden, however, has argued that even a lawful disclosure would have resulted in retaliation against him.

(U) Among other things, Snowden has argued that he was unable to raise concerns about NSA programs because he was not entitled to protection as an IC whistleblower given his status as a contractor. (He was with Booz Allen at the time of his leaks to the press.) But the 1998 IC WPA applies to IC employees as well as contractors. Although the statute does not explicitly prohibit reprisals, the IC WPA channel nevertheless enables confidential, classified disclosures and oversight, as well as a measure of informal source protection by Congress. The statute specifically authorizes *IC contractors* to inform the intelligence committees of adverse actions taken as a consequence of IC WPA-covered disclosures.

(U) Moreover, explicit protection against such actions was conferred on Snowden by DoD regulation 5240 1-R. Snowden's unauthorized disclosures involved Executive Order (EO) 12333 activities as well as activities conducted under FISA. At least with respect to intelligence activities authorized under E.O. 12333—and, according to the DoD Senior Intelligence Oversight Official, activities conducted under other authorities—5240 1-R *requires* employees and contractors of a DoD intelligence element to report "questionable activities," or "conduct that constitutes, or is related to, [an] intelligence activity *that may violate the law, any Executive*

[147] E-mail from Edward Snowden to NSA Office of General Counsel (Apr. 5, 2013, at 4:11PM), overall document classified U//FOUO; cited portion classified U//FOUO.
[148] *Id.*, cited portion classified U//FOUO.
[149] E-mail from NSA Office of General Counsel Attorney to Edward Snowden (Apr. 8, 2013, at 1:37PM), overall document classified U//FOUO; cited portion classified U//FOUO.
[150] IC on the Record, "Edward J. Snowden email inquiry to the NSA Office of General Counsel," (May 29, 2014) ("There was not additional follow-up noted.").

Order or Presidential directive ... or applicable DoD policy[.]"[151] 5240 1-R also says that DoD senior leaders shall "ensure that *no adverse action is taken against any employee* [or contractor] because the employee reports [questionable activities]" pursuant to the regulation.[152] The IC IG's Executive Director for Intelligence Community Whistleblowing & Source Protection (ICW&SP), a former employee of the DoD IG's staff, has advised HPSCI staff that these procedures applied to Snowden during his employment as an NSA contractor and would have helped to shield him from retaliation for voicing his objections internally.

(U) Finally, Snowden also likely was covered by 10 U.S.C. § 2409 (Section 2409). As written at the time of Snowden's leaks,[153] Section 2409 was primarily focused on protecting DoD contractors from reprisals if they properly disclosed a "violation of law related" to a DoD contract. However, Snowden has not advanced any contract-related claims about NSA surveillance. Rather, he generally disagreed with NSA surveillance programs on policy and constitutional grounds.

(U) If Snowden did have concerns with programs related to a DoD contract, then the prior version of Section 2409 authorized him to raise those concerns without fear of retaliation with a "Member of Congress, a representative of a Committee of Congress, an Inspector General, the Government Accountability Office, a Department of Defense employee responsible for contract oversight or management, or an authorized official of an agency or the Department of Justice[.]"

(U) Foreign Influence

[redacted][154], [redacted][155].

[redacted][156]

[151] Department of Defense Regulation 5240 1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect U.S. Persons,* C.15.2.1, 3.1.1 (Dec. 7, 1982) (emphasis added).
[152] *Id.* at C.14.2.3.2.
[153] Important amendments to Section 2409, which took effect in July 2013, substantially altered the statute. Among other things, the updates extended reprisal protections to DoD subcontractors as well as contractors, and widened the list of persons to whom contractors and subcontractors could make disclosures. At the same time, the amendments also narrowed Section 2409's coverage by explicitly excluding employees and contractors of IC elements. However, that limitation, like other alterations to Section 2409, did not take effect until July 2013—*after* Snowden had unlawfully disclosed NSA material to journalists.
[154] *See, e.g.*, Testimony of Gen. Keith Alexander at 30, HPSCI Hearing (Jun. 13, 2013) ("It is not clear to us if there is a foreign nexus. There [are] some things; it does look odd that someone would go to Hong Kong to do this.")
[155] [redacted]
[156] [redacted]

[redacted].[157] [redacted].[158] [redacted][159]

~~(TS//HCS/OC/NF)~~ Since Snowden's arrival in Moscow, he has had, and continues to have, contact with Russian intelligence services. [redacted],[160] and in June 2016, the deputy chairman of the Russian parliament's defense and security committee asserted that "Snowden did share intelligence" with his government.[161] [redacted][162]

(U) What Did Snowden Take?

~~(S//NF)~~ [redacted].[163] In light of the volume at stake, it is likely that even Snowden does not know the full contents of all 1.5 million documents he removed.

(U) One thing that is clear, however, is that the IC documents disclosed in public are merely the tip of the iceberg.

~~(S//NF)~~ As of August 19, 2016, press outlets had published or referenced [redacted] taken by Snowden.[164] This represents less than one-tenth of one percent of the nearly 1.5 million documents the IC assesses Snowden removed.[165]

---

157 [redacted]

158 [redacted]

159 [redacted]

160 *Id.* Cited material classified S//OC//NF.

161 Mary Louise Kelly, "During Tenure in Russia, Edward Snowden Has Kept A Low Profile," *National Public Radio* (June 29, 2016), *available at* http://www.npr.org/2016/06/29/483890378/during-tenure-in-russia-edward-snowden-has-kept-a-low-profile.

162 [redacted].

163 *See* NSA, "HPSCI Recollection Summary Paper," (Jan. 26, 2015) [redacted] Overall document classified S//NF; cited portion classified S//NF.

164 E-mail from NSA Legislative Affairs (Aug. 22, 2016, at 4:48PM). Overall document classified S//REL TO USA, FVY; cited portion classified S//REL TO USA, FVEY.

(U) The 1.5 million documents came from two classified networks, an internal NSA network called NSANet and an IC-wide Top Secret/Sensitive Compartmented Information network called the Joint Warfighter Information Computer System (JWICS). If printed out and stacked, these documents would create a pile more than three miles high.[166]

~~(S//NF)~~ [redacted][167]. [redacted][168]. [redacted][169]. [redacted].[170]

~~(S//NF)~~ [redacted][171] [redacted][172]. [redacted][173] [redacted].[174]

---

[165] NSA, "HPSCI Recollection Summary Paper," (Jan. 26, 2015) Overall document classified S//NF; cited portion classified S//NF.

[166] Testimony of Mr. Scott Liard, Deputy Director for Counterintelligence, Defense Intelligence Agency, HPSCI Hearing (Jan. 27, 2014), at 7-8. The 1.5 million document count does not include 374,000 blank documents Snowden downloaded from the Department of the Army Intelligence Information Service (DAIIS) Message Processing System. *See* DIA, Information Review Task Force-2, "Fourth Quarter Report, 2014" (Dec. 31, 2014), at xvii.

[167] NSA, "HPSCI Recollection Summary Paper," (Jan. 26, 2015). Overall document classified S//NF; cited portion classified S//NF.

[168] NSA, "Timing of Recollection and Security Flags," (Mar. 14, 2016). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL.

[169] *Id.*

[170] *Id.*

[171] NSA, "HPSCI Recollection Summary Paper," (Jan. 26, 2015).

[172] *Id.*; *see also* DIA, Information Review Task Force-2, "Fourth Quarter Report, 2014" (Dec. 31, 2014), at xvii.

[173] *Id.*; *see also* DIA, Information Review Task Force-2, "Fourth Quarter Report, 2014" (Dec. 31, 2014), at xvii.

[174] *Id.*; *see also* DIA, Information Review Task Force-2, "Fourth Quarter Report, 2014" (Dec. 31, 2014), at xvii.

~~(S)~~ The vast majority of the documents Snowden removed were unrelated to electronic surveillance or any issues associated with privacy and civil liberties. [redacted][175] [redacted]

(U) What Damage Did Snowden Cause?

~~(S//NF)~~ Over the past three years, the Intelligence Community and the Department of Defense (DoD) have carried out separate reviews—with differing methodologies—of the contents of all 1.5 million documents Snowden removed. It is not clear which of the documents Snowden removed are in the hands of a foreign government. All of the documents that have been publicly disclosed—[redacted][176]—can be accessed by foreign militaries and intelligence services as well as the public. [redacted][177] [redacted][178] [redacted].

(U) Out of an abundance of caution, DoD therefore reviewed all 1.5 million documents to determine the maximum extent of the possible damage.

~~(TS//NF)~~ As of June 2016, the most recent DoD review identified 13 high-risk issues, which are identified in the following table.[179] Eight of the 13 relate to [redacted] capabilities of DoD; if the Russian or Chinese governments have access to this information, American troops will be at greater risk in any future conflict.[180]

---

175 [redacted]

176 E-mail from NSA Legislative Affairs (Aug. 22, 2016, at 4:48PM). Overall document classified S//REL TO USA, FVY; cited portion classified S//REL TO USA, FVEY.

177 DIA, Information Review Task Force-2, "Initial Assessment" (Dec. 26, 2013), at 3. Overall document classified TS//SI//RSEN/OC/NF; cited portion classified S//NF.

178 Mary Louise Kelly, "During Tenure in Russia, Edward Snowden Has Kept A Low Profile," *National Public Radio* (June 29, 2016), *available at* http://www.npr.org/2016/06/29/483890378/during-tenure-in-russia-edward-snowden-has-kept-a-low-profile.

179 DoD, Mitigation Oversight Task Force, "Quarterly Report" (Oct. 2015), at 8. Overall document classified TS//SI/TK//ORCON/NF; cited portion classified TS//NF

180 *Id.*

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]

(U) The Intelligence Community, by contrast, has carried out a damage assessment for only a small subset of the documents Snowden removed. And unlike IC damage assessments for previous unauthorized disclosures,[181] the IC assessment on Snowden does not contain an assessment of Snowden's background and motive, an assessment of whether he was the agent of a foreign intelligence service, or recommendations for how to improve security in the IC. In its review, the National Counterintelligence and Security Center (NCSC), a component of the Office of the Director of National Intelligence, divided the documents Snowden removed into three "tiers."[182]

[181] *See, e.g.*, Office of the National Counterintelligence Executive, "Ana Belen Montes: A Damage Assessment," (July 1, 2004). Overall document classified S//NF.

[182] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 January 2015 through 31 August 2015," (Apr. 8, 2016), at 5. Overall document classified TS//HCS-P/SI-G/TK//OC/NF; cited portion classified U//FOUO.

~~(S//REL)~~ **Tier One:** Documents that have been disclosed in the media, either in whole or in part. As of August 19, 2016, press outlets had published or referenced [redacted] files taken by Snowden.[183]

~~(TS//SI//OC/NF)~~ **Tier Two:** Documents that, based on forensic analysis, Snowden would have collected in the course of collecting Tier One, but have not yet been disclosed to the public. The IC assesses these documents are likely in the hands of the media. [redacted][184]

~~(TS//SI//OC/NF)~~ **Tier Three:** The remaining [redacted] documents that Snowden accessed [redacted][185]

~~(S//NF)~~ The IC damage assessment of Tier One documents is still ongoing, but, as of late May 2016, the IC had no plans to carry out a damage assessment of the documents in Tier Two or Tier Three.[186] [redacted].[187] As a result, the IC's damage assessment cannot be considered a complete accounting of the damage Snowden caused to U.S. intelligence.

(U) However, even the IC's limited damage assessment of documents in Tier One indicates that Snowden's disclosures caused massive damage to national security. A few examples, listed below, illustrate the scale of the damage.

- ~~(TS//SI//NF)~~ [redacted][188]

---

[183] E-mail from NSA Legislative Affairs (Aug. 22, 2016, at 4:48PM). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY.
[184] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 January 2015 through 31 August 2015," (Apr. 8, 2016), at 5. Overall document classified TS//HCS-P/SI-G/TK//OC/NF, cited portion classified TS//SI/OC/NF.
[185] *Id.*, cited portion classified TS//SI/OC/NF.
[186] HPSCI Staff Briefing with NCSC (May 25, 2016).
[187] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 January 2015 through 31 August 2015," (Apr. 8, 2016), at 1. Overall document classified TS//HCS-P/SI-G/TK//OC/NF; cited portion classified S//NF.
[188] HPSCI Staff Memorandum for the Record, "NSA Notification of [redacted] Resulting from Recent Media Disclosures," (July 8, 2014). Overall document classified TS//SI//NF.

- ~~(TS//SI//NF)~~ [redacted].[189]
- ~~(TS//SI//NF)~~ [redacted]

- ~~(S//SI//NF)~~ [redacted].[191]
- ~~(TS//SI//NF)~~ [redacted],[192] [redacted][193]
  - ~~(TS//SI//NF)~~ [redacted].[194]

---

[189] *Id.*

[190] *Id.*

[191] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 August 2014 through 31 December 2014," (Dec. 22, 2015), at 25. Overall document classified TS//HCS-P/SI-G/TK//OC/NF; cited portion classified S//SI//NF.

[192] Presidential Policy Directive 28, "Signals Intelligence Activities" (Jan. 17, 2014).

[193] Letter from Director of National Intelligence James R. Clapper to Chairman Devin Nunes and Ranking Member Adam Schiff (Jun. 23, 2015). Overall document classified TS//SI//NF, cited portion classified TS//SI//NF.

[194] NSA, "Response to Congressionally Directed Action: [redacted]," (Nov. 17, 2014), at 2-4. Overall document classified TS//SI//NF; cited portion classified TS//SI//NF.

    - ~~(TS//SI//NF)~~ [redacted]

  - ~~(TS//SI//NF)~~ [redacted].

  - ~~(TS//SI//NF)~~ [redacted].[195]

  - ~~(S//HCS-O//OC/NF)~~ Because of disclosures attributed to Snowden [redacted],[196] and in August 2015, [redacted].[197]

- ~~(S//NF)~~ [redacted]

  - ~~(TS//SI//NF)~~ [redacted].[198]

    - ~~(TS//SI//NF)~~ [redacted].[199]

---

[195] HPSCI Staff Briefing with ODNI (Sept. 6, 2016).
[196] HPSCI Staff Briefing with NCSC, NSA, CIA, and FBI (Jun. 17, 2016).
[197] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 August 2014 through 31 December 2014 – HCS-O Annex" (Dec. 22, 2015), . Overall document classified TS//HCS-O/SI//OC//NF; cited portion classified S//HCS-O//OC/NF.
[198] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 January 2015 through 31 August 2015," (Apr. 8, 2016), at 11. Overall document classified TS//HCS-P/SI-G/TK//OC/NF; cited portion classified TS//SI//NF.
[199] HPSCI Staff Briefing with NCSC, NSA, CIA, and FBI (Jun. 17, 2016).

- ~~(S//HCS-P/SI//OC/NF)~~ [redacted].[200]
- ~~(S//HCS-P/SI//OC/NF)~~ [redacted].[201]
- ~~(TS//SI//NF)~~ [redacted].[202]
  - ~~(TS//SI//REL TO USA, FVEY)~~ [redacted].[203]

- ~~(TS//SI//OC/NF)~~ [redacted].[204] [redacted].[205] [redacted].[206]

[200] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 January 2015 through 31 August 2015," (Apr. 8, 2016), at 11. Overall document classified TS//HCS-P/SI-G/TK//OC/NF; cited portion classified S//HCS-P/SI//OC/NF.
[201] *Id.*, cited portion classified S//HCS-P/SI//OC/NF.
[202] NSA, "Response to Request for Information Re: [redacted]," (Dec. 16, 2014). Overall document classified TS//SI//NF; cited portion classified TS//SI//NF.
[203] CIA, Memorandum for Congress, "In Response to Questions on Decreased Collection Possibly Caused by Unauthorized Disclosures since June 2013," (July 20, 2016), at 2. Overall document classified TS//HCS-O-P CRD/SI//OC/NF; cited portion classified TS//SI/REL TO USA, FVEY).
[204] ODNI, Recouping Intelligence Capabilities Brief (Jun. 7, 2016), at 8. Overall document classified TS//SI//NF; cited portion classified TS//SI//NF; ODNI Briefing to HPSCI Staff on Recouping Intelligence Capabilities Brief (July 13, 2016).
[205] *Id.*
[206] ODNI, "Remediation of Unauthorized Disclosures" (June 2015), at 3. Overall document classified TS//SI//OC/NF; cited portion classified TS//SI/OC/NF.

- ~~(TS//SI//NF)~~ [redacted][207] [redacted].
  - [redacted][208].
- ~~(TS//SI//NF)~~ [redacted][209] [redacted][210].

(U) How Has the IC Recovered from Snowden?

~~(TS//SI//NF)~~ There is no IC-wide estimate for the total cost to the government of remediating Snowden's disclosures. However, a mid-2015 study by ODNI's Systems and Resources Analysis Group estimated that NSA and CIA will spend [redacted] over Fiscal Years 2016 and 2017 to recover from the damage Snowden's disclosures caused to SIGINT capabilities.[211]

~~(TS//SI//NF)~~ As a whole, the IC will undoubtedly spend even more. The [redacted] estimate represents a conservative assessment of the amount CIA and NSA will spend to rebuild SIGINT capabilities that were damaged by Snowden's disclosures. The estimate captures only two years of spending and does not reflect investments made before Fiscal Year 2016 or planned investments for Fiscal Year 2018 and beyond. Moreover, it does not capture the costs associated

---

207 [redacted]

208 [redacted].

209 [redacted]

210 HPSCI Staff Memorandum for the Record, "Upcoming Unauthorized Disclosures of [redacted] Overall document classified TS//SI//NF.

211 ODNI SRA, "FY17 Major Issue Studies – Recouping Intelligence Capabilities," (June 7, 2016), at 9. Overall document classified TS//SI//NF; cited portion classified TS//SI//NF.

with the IC's damaged relationships with foreign and corporate partners, the opportunity cost of the time and resources the IC and DOD have spent mitigating the damage of the disclosures, or the costs of improved security measures across the federal government.

(U) Snowden's actions also exposed significant vulnerabilities in the IC's information security. Although it is impossible to reduce the risk of an insider threat like Snowden to zero, relatively simple changes such as automatically detecting the malicious use of scraping tools like "wget," physically disabling removable media from the workstations of NSA personnel who lack a work reason to use removable media, and implementing two-person controls to transfer data by removable media would have dramatically reduced the quantity of files Snowden could have removed or stopped him altogether.

(U) The Committee remains concerned that NSA, and the IC as a whole, have not done enough to reduce the chances of future insider threats like Snowden.

~~(C//REL TO USA, FVEY)~~ In the aftermath of Snowden's disclosures, NSA compiled a list of [redacted] security improvements for its networks. These improvements, called the "Secure the Net" initiatives, contained many steps that would have stopped Snowden, such as two-person control for transfer of data by removable media, and many broader security improvements, such as reducing the number of privileged users and authorized data transfer agents, and moving toward a continuous evaluation model for background investigations.[212] In July 2014, more than a year after Snowden's first disclosures, many of these "Secure the Net" initiatives—including some relatively simple initiatives, such as two-stage controls for systems administrators—had not been completed.[213] In August 2016, more than three years after Snowden's first disclosures, four of the [redacted] initiatives remained outstanding.[214]

(U) In the House-passed Intelligence Authorization Act for Fiscal Year 2016, the Committee directed the Department of Defense Inspector General (DOD IG) to carry out an assessment of information security at NSA, including whether NSA had successfully remediated the vulnerabilities exposed by Snowden.

(U) In August 2016, DOD IG issued its report, finding that NSA needed to take additional steps to effectively implement the privileged access-related "Secure the Net" initiatives.[215]

(U) In particular, DOD IG found that NSA had not: fully implemented technology to oversee privileged user activities; effectively reduced the number of privileged access users; or effectively reduced the number of authorized data transfer agents. In addition, contrary to the

[212] NSA, "Secure the Net Initiatives," (Aug. 22, 2016). Overall document classified C//REL TO USA, FVEY.
[213] NSA, "Secure the Net Initiatives," (July 2014). Overall document classified C//REL TO USA, FVEY.
[214] NSA, "Secure the Net Initiatives," (Aug. 22, 2016). Overall document classified C//REL TO USA, FVEY.
[215] Department of Defense Inspector General, Report 2016-129, "The National Security Agency Should Take Additional Steps in Its Privileged Access-Related Secure the Net Initiatives" (Aug. 29, 2016). Overall document classified S//NF, cited portion classified U//FOUO.

"Secure the Net" initiatives, NSA did not consistently secure server racks and other sensitive equipment in data centers, and did not extend two-stage authentication controls to all high-risk users.[216] Recent security breaches at NSA underscore the necessity for the agency to improve its security posture.

(U) And even though NSA has been the victim of recent breaches, it is not the only IC agency where information security needs to be improved. For instance, a recent CIA Inspector General report found that CIA has not yet implemented multi-factor authentication controls such as a physical token for general or privileged users of the Agency's enterprise or mission systems.[217]

(U) As a recent Committee report concluded, the introduction of the Intelligence Community Information Technology Enterprise (IC ITE) should produce an improved security environment in the IC.[218] And as that report noted, although IC data will be more secure and better protected under IC ITE than it is today, from both internal and external threats, IC ITE will also increase risks in different areas.[219] These risks will require dedicated attention to ensure IC ITE reaches its full potential for an improved security environment.

(U) Conclusion – Efforts to Improve Security

(U) Although it is impossible to reduce the chance of another Snowden to zero, more work can and should be done to improve the security of the people and computer networks that keep America's most closely held secrets.

(U) Since the beginning of Snowden's disclosures, the Committee has directed the IC to carry out a number of studies and security improvements to reduce the risk of another insider threat. Among its other oversight efforts, the Committee has:

- **(U)** Authorized an additional [redacted] for insider threat detection efforts in Fiscal Year 2014. Consistent with a spend plan and updated insider threat strategy provided to Congress, 60 percent of these funds were to be used for insider threat detection and the remaining 40 percent toward continuous evaluation;[220]

- **(U)** Directed the DNI to ensure that the President's National Insider Threat Policy and Minimum Standards were fully implemented on TS/SCI networks and all NIP-funded

---

[216] *Id.*, cited portion classified C//REL TO USA, FVEY.
[217] CIA Office of Inspector General, "Review of National Security Systems Required by the Cybersecurity Act of 2015," Report No. 2016-0022-AS (Aug. 2016). Overall report classified S//NF, cited portion classified S//NF.
[218] HPSCI Report, "Assessing IC ITE's Security Posture," (Feb. 4, 2016). Overall report classified S//NF, cited portion classified U.
[219] *Id.* at 25, cited portion classified U//FOUO.
[220] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, pp. 15-16.

networks at CIA, DIA, NSA, NGA, NRO, FBI, and DOE by October 1, 2014;[221]

- **(U)** Directed the DNI, as the Security Executive Agent, to establish a structure for a comprehensive continuous evaluation system for holders of TS/SCI within 270 days of the enactment;[222]

- **(U)** Directed the DNI, in coordination with the USD(I) to review whether the continuous evaluation process, insider threat auditing tools, and background investigation processes should consider different kinds of information to detect potential leakers than the current process collects to detect traditional security threats;[223]

- **(U)** Directed the DNI to review the management controls on privileged access, to include Systems Administrators;[224]

- **(U)** Directed the NSA to implement a "two person rule" for Tier 3 Systems Administrators and select Tier 2 Systems Administrators and directed the DNI to report to the Intelligence Committees on actions he is undertaking to lead the other IC elements in enacting a similar two person rule, or similar safeguards;[225]

- **(U)** Directed the DNI to attempt to reduce the number of Tier 3 System Administrators and ensure consistency in tier ratings across the IC;[226]

- **(U)** Directed the DNI to expand Scattered Castles to contain all TS/SCI clearance holders and list any pertinent exceptions or "flags" as close to real-time as possible;[227]

- **(U)** Directed the DNI to ensure that insider threat security measures were fully applied to contractors and contractor facilities;[228]

---

[221] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, p. 16; Classified Annex to Accompany the Report to the House-passed Intelligence Authorization Act for Fiscal Year 2014 pp. 32.
[222] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, p. 16; Classified Annex to Accompany the Report to the House-passed Intelligence Authorization Act for Fiscal Year 2014 pp. 32-33.
[223] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, p. 16; Classified Annex to Accompany the Report to the House-passed Intelligence Authorization Act for Fiscal Year 2014 p. 33.
[224] *Id.*
[225] *Id.*
[226] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, p. 16; Classified Annex to Accompany the Report to the House-passed Intelligence Authorization Act for Fiscal Year 2014 p. 34.
[227] *Id.*
[228] *Id.*

- **(U)** Required the IC to continuously evaluate the eligibility of personnel to access classified information, to develop procedures for automatically sharing derogatory information between agencies, and other improvements to the reinvestigation process;[229]

- **(U)** Encouraged the DNI to make a determination of how periodic reinvestigations will be handled in concert with a continuous evaluation program;[230]

- **(U)** Directed an IC analysis of private sector policies to reduce insider threats;[231]

- **(U)** Directed a DNI-led review once every three years of all U.S. government positions with access to classified information;[232]

- **(U)** Directed the DNI, in consultation with the Attorney General, the Secretary of Defense, and the Director of the Office of Personnel Management, to develop and implement procedures that govern whether and how publicly available information may be used in the security clearance process;[233]

- **(U)** Required each IC element to implement a program to enhance security reviews of individuals applying for access to classified information;[234]

- **(U)** Required the Inspector General of each federal agency that operates national security systems to report on, among other things, information security practices to detect data exfiltration and other threats;[235]

- **(U)** Directed NSA to produce a plan for completing security improvements to its networks by the end of Calendar Year 2018, including enclaves and systems used outside of NSA-controlled facilities; and[236]

---

[229] Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, Title V.
[230] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, p. 16
[231] Intelligence Authorization Act for Fiscal Year 2015, P.L. 113-293, § 308.
[232] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2015, P.L. 113-293, p. 11.
[233] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2015, P.L. 113-293, pp. 11-12.
[234] Intelligence Authorization Act for Fiscal Year 2016, Division M, Consolidated Appropriations Act for Fiscal Year 2016, P.L. 114-113, § 306.
[235] Cybersecurity Act of 2015, Division N, Consolidated Appropriations Act for Fiscal Year 2016, P.L. 114-113, § 406
[236] Classified Annex to Accompany the Joint Explanatory Statement to the Intelligence Authorization Act for Fiscal Year 2016, Division M, Consolidated Appropriations Act for Fiscal Year 2016, P.L. 114-113, p. 19.

- **(U)** Directed the Intelligence Community Inspector General (IC IG) to carry out an assessment of post-Snowden information security improvements at CIA, DIA, FBI, NGA, NRO, and ODNI.[237]

(U) As the Fiscal Year 2017 Intelligence Authorization Act moves toward enactment and Congress begins its consideration of the President's Fiscal Year 2018 budget request, the Committee looks forward to working with the IC to ensure our nation's secrets receive the security they deserve.

---

[237] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2017, H.R. 5077, p. 93.