Highlights

House Intelligence Committee Review of Edward Snowden Disclosures

Most of the documents Snowden stole have no connection to programs that could impact privacy or civil liberties—they instead pertain to military, defense, and intelligence programs of great interest to America's adversaries.

- "The vast majority of documents Snowden removed were unrelated to electronic surveillance or any issues associated with privacy and civil liberties." (p. 22)
- "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." (p. 12)
- "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." (p. 11)
- "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. . . .
  But only a few weeks after [he became engaged in a] 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." (p. 10)

Snowden was not a whistleblower.

- "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." (p. 16)
- "Snowden did, however, contact NSA personnel who worked in an internal oversight office about his personal difficulty understanding the safeguards against unlawful intelligence activities." (p. 17)
- "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." (p. 18)

Snowden was, and remains, a serial exaggerator and fabricator

- "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.' 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.'" (p. 5)

House Intelligence Committee Review of Edward Snowden Disclosures

- "Several years later, Snowden claimed that, while in [redacted], he had ethical qualms about working for CIA. 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." (p. 6).
- "In September 2012, [Snowden] 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 NSA networks, he passed the test." (p. 14)

Snowden was a disgruntled employee who became engaged in numerous spats with his supervisors.

- "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 unfairly targeted' by his supervisor."(p. 3-4)
- "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 judgement." (p. 5)
- "His supervisor in [redacted] cataloged six counseling sessions between October 2007 and April 2008, nearly one per month, regarding his behavior at work." (p. 5)
- "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.'" (p. 9)

Snowden's disclosures did tremendous damage to U.S. national security, and 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.

- "As of June 2016, the most recent DoD review identified 13 high-risk issues . . . . 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." (p. 22)

Highlights

House Intelligence Committee Review of Edward Snowden Disclosures

- "Since Snowden's arrival in Moscow, he has had, and continues to have, contact with Russian intelligence services." (p. 20)
- "In the aftermath of Snowden's disclosures, NSA compiled a list of [redacted] security improvements for its networks. . . . In August 2016, more than three years after Snowden's first disclosures, four of the [redacted] initiatives remained outstanding." (p. 29)
- "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." (p. 29)
- "[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." (p. 30)