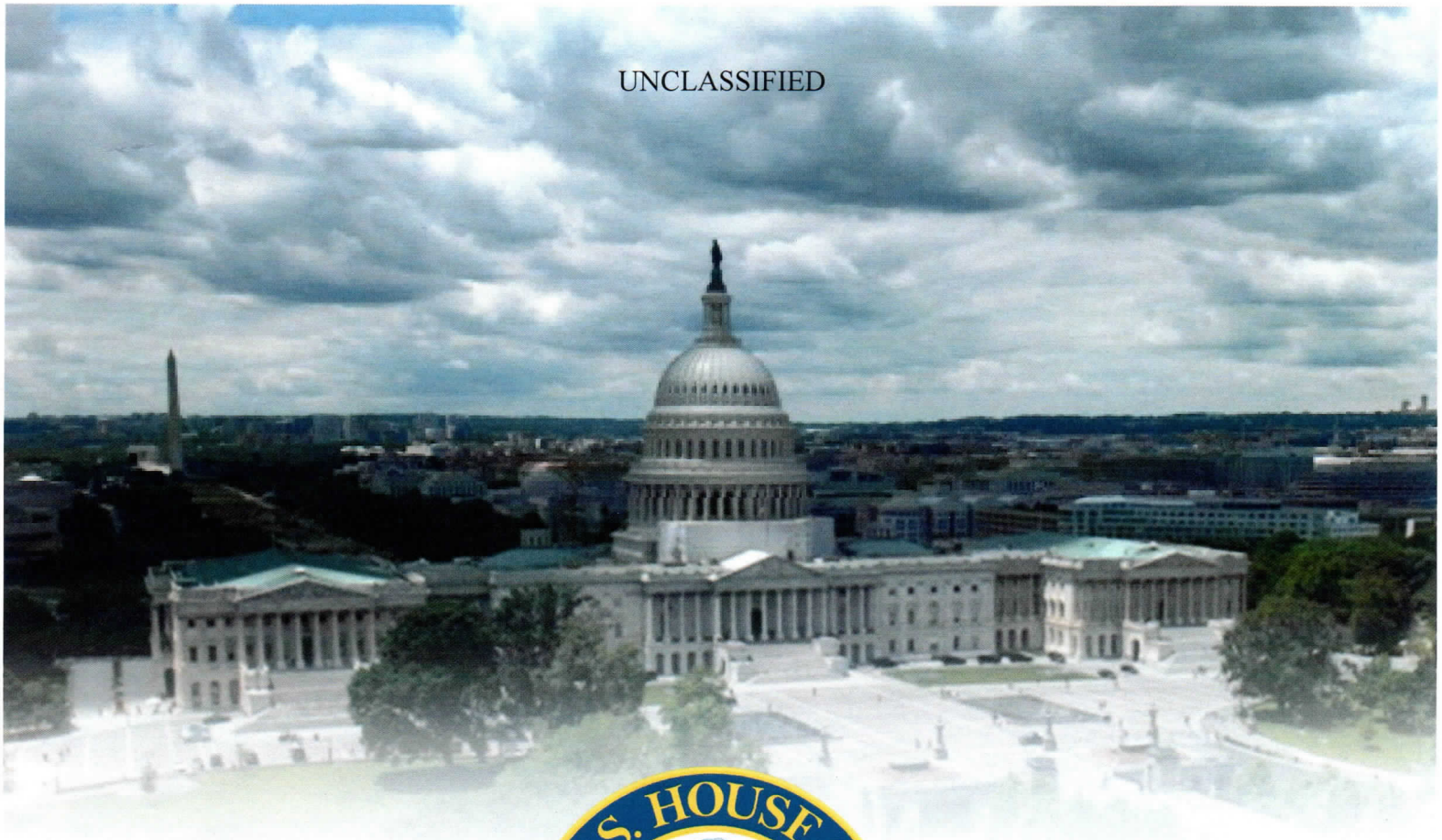

Executive Summary of Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden

September 15, 2016

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.

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.

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.

The bulk of the Committee's 36-page review, which includes 230 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.

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.

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.

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.

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.

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.

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.

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.

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.

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.