CHAPTER ONE
Introduction and Recent Developments

There is a strong presumption against the grant or maintenance of a security clearance. ISCR Case No. 15-06440 at 2 (App. Bd. Dec. 26, 2017), *citing Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990), *cert. denied*, 499 U.S. 905 (1991).

That presumption underlies all consideration of the work of the Defense Office of Hearings and Appeals (DOHA). It has been said that DOHA is in the business of predicting the future. It must disqualify otherwise highly qualified and dedicated workers from carrying out their duties because something in their past or off-duty behavior portends the possibility that those employees might, by accident or design, allow our government's secrets to fall into the hands of some present or future enemy. How DOHA makes these decisions as to who may be granted a security clearance, and who may obtain access to classified information, is the primary subject of this book.

With each passing decade, changes in society are reflected in the changing Guidelines. In the 1960s, the issues of loyalty and membership in Communist organizations were paramount. In the 1970s and 1980s, "moral turpitude" fell as a basis for disqualification, and the focus was instead on whether the behavior involved a criminal offense or reflected the existence of an emotional disorder affecting the person's judgment. In the 1990s, the *per se* disqualification on the basis of sexual orientation was replaced with concern as to whether the conduct could subject the individual to blackmail or other forms of coercion. Today the focus is on the continuing federal illegality of marijuana despite legalization in the majority of states and the desire to encourage mental health treatment while monitoring for dangerous psychiatric problems.

Beginning in 1985, highly publicized espionage cases like the Walkers, Jonathan Pollard, Aldrich Ames, Earl Pitt, and Harold Nicholson elevated the profile of the security clearance process, causing questions to be posed as to the effectiveness of the government's ability to identify potential spies. More recently, serious breaches by individuals granted security clearances have caught the public eye, including Edward Snowden, Aaron Alexis, Jerry Chun Shing Lee, Chelsea Manning, and Harold T. Martin, III.

Security clearances are issued by many government agencies, including the Department of Defense (DoD), the Department of State (DOS), the Department of Homeland Security (DHS), the Department of Energy (DoE), the Department of Justice (DOJ), the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Central Intelligence Agency (CIA). There are three types of clearances:

- Confidential clearance—provides access to information or material that may cause damage to national security if disclosed without authorization.
- Secret clearance—provides access to information or material that may cause serious damage to national security if disclosed without authorization.
- Top secret clearance—provides access to information or material that may cause exceptionally grave damage to national security if disclosed without authorization.

Though not a clearance, many public employees and contractors also must be cleared to access Sensitive Compartmented Information (SCI), which provides access to intelligence information and material that requires restricted handling within compartmented channels. A Public Trust is a type of background investigation; it is not a security clearance, though many people refer to them inaccurately as Public Trust Clearances. Certain sensitive positions are designed Public Trust positions and require a higher level of scrutiny, though not as high as those requiring a clearance.

The DoE issues two levels of clearance:

1. Q Clearance—Allows access to classified information up to and including top secret data with the special designation: Restricted Data (TS//RD) and special Q-Cleared security areas, such as the White House, the Pentagon, the Hall of Congress, and the Supreme Court.

2. L Clearance—Allows access to classified information up to and including secret data with the special designation: formerly restricted data (S//FRD) and special L-cleared "limited" areas.

I. CHANGES AFTER 9/11

The events of September 11, 2001, called greater attention to the work of DOHA. People frequently ask how that day changed DOHA, and the answer is that it has changed the way cases are considered and analyzed. A greater universe of candidates is now coming before DOHA, because security clearances are required of more occupations and agencies. Prior to September 11, 2001, DoD processed approximately 200,000 security clearances annually. That number has grown exponentially. DoD processed more than 850,000 clearances in FY 2013. In FY 2013, the number of clearance-eligible personnel exceeded 5.1 million, including civilian and military employees and contractors. Of that number, over 1.4 million were cleared for access at the "top secret" level. *See* OMB Suitability and Security Clearance Performance Accountability Council, *Suitability and Security Processes Review—Report to the President* (Feb. 2014), *available at* .

In more recent times, the numbers are decreasing. As of October 1, 2016, there were 4,080,728 individuals eligible to hold a clearance, which included those investigated and adjudicated favorably and who may or may not have had access. ODNI Fiscal Year 2016 Annual Report on Security Clearance Determinations, *available at* https://www.dni.gov/files/documents/Newsroom/FY16-Report-Security-Clearance-Determinations-PubRelease-20171017.pdf. Only 594,894 clearances were approved in FY 2016, which reflected a 6.9% reduction from FY 2015. *Id.*

Since September 11, 2001, new agencies, like the Transportation Security Administration, and old occupations previously free from the burden of security clearance processing (like U.S. Department of Agriculture plant inspectors or airport tarmac workers), now come under the umbrella of the Department of Homeland Security (DHS) and are subject to security clearance requirements. Portions of the Federal Emergency Management Agency that previously dealt only with the possibility of natural disasters within our borders are now applying that expertise to the prospect of human-made disasters. The National Disaster Medical System, previously a part of the Department of Health and Human Services, now also comes under the ambit of the DHS.

In addition, even where positions do not involve access to classified information, the vast proliferation of computer systems led to "trustworthiness determinations" being imposed for positions which involve access to government information systems. The concern is that individuals might make unauthorized modifications, corrupt or destroy data, or engage in inappropriate uses of such systems. Concern also arose regarding potential misuse of information technology systems, such as gaining unauthorized access for an improper purpose.

II. BACKLOGS

These increasing numbers of positions requiring clearances led to debilitating backlogs in clearance processing, which in turn led to a major focus on speeding up the process. The Intelligence Reform and Terrorist Prevention Act of 2004 (IRTPA) was enacted in the wake of September 11, 2001, and was designed, in part, to combat the tremendous national backlog of pending security clearance determinations. IRTPA set aggressive mandates for improved timeliness and required 90% of initial security clearance determinations to be completed within an average of 60 days by the end of 2009. In 2005, the Government Accountability Office (GAO) placed the Personnel Security Clearance Process on its High-Risk List due to the massive backlog of applications and insufficient quality standards. *See* U.S. GAO, GAO-05-207, High-Risk Series: An Update (2005), *available at* https://www.gao.gov/new.items/d05207.pdf. According to a June 20, 2013 GAO study, "[e]xecutive branch agency efforts to improve the personnel security process have emphasized timeliness but not quality." *See* U.S. GAO, GAO-13-728T, Personnel Security Clearances: Further Actions Needed to Improve the Process and Realize Efficiencies (2013), *available at* https://www.gao.gov/assets/660/655360.pdf. Once again, on January 25, 2018, GAO added the government-wide personnel security clearance process to its High Risk List. Press Release: U.S. GAO, GAO Adds Government-Wide Personnel Security Clearance Process to "High Risk List" (Jan. 25, 2018), *available at* https://www.gao.gov/press/high_risk_security_clearance_process.htm. The Comptroller explained this was a call to policymakers to address the problem because "[a] high-quality and timely personnel security clearance process is essential to minimize the risks of unauthorized disclosures of classified information and to help ensure that information about individuals with criminal histories or other questionable behavior is identified and assessed." Yet, as of September 2017, there were more than 700,000 background investigations pending throughout the executive branch agencies.

(As of) Date	Total Backlog/ Outstanding Requests[1]	Total Nat'l Security Determinations Initial Re-Investigations		Simple Record Checks/ Sustainability & Credentialing Determinations	Time to Complete/ Perform an Investigation
03/31/2004 [2]	DoD's: 188,000	101,000	61,000	25,000	Initial Investigations: 35 days Top Secret Investigations: 75 days 375 days
End of 3rd Quarter FY2016 [3]	OPM's: 569,000	343,557	156,172	70,271	Fastest 90% of Initial Investigations: 105 days Fastest 90% of Initial Top Secret Clearance: 214 days
08/2017 [4]	NBIB's: 695,000	335,000	210,000	155,000	Initial Investigations: 158 days 450 days (as of 3/31/17 [5])
09/27/2017 [6]	NBIB's: 707,000	~330,000	~210,000	~134,000	—
Presently [7]	OMB issued Memoranda M-17-26 permitting the Office of Personnel Management to stop reporting on the backlog/number of people waiting for BI approvals.				

Time to Perform/Complete a Background Investigation [8]

Investigation Type	FY 2005	FY 2014	FY 2015	FY 2016
All Initial Investigations	145 days	35 days	67 days	123 days
Top Secret	308 days	75 days	147 days	220 days
Secret/Confidential	115 days	30 days	58 days	108 days
Re-Investigations	419 days	117 days	197 days	219 days

[1] Total Backlog/Outstanding Requests includes Simple Record Checks; Suitability & Credentialing Investigations; and National Security Investigations.

[2] GAO Highlights: GAO-04-632, DoD Personnel Clearances: Additional steps can be taken to reduce backlogs and delays in determining security clearance eligibility for industry personnel. (May 2004).

[3] Memorandum from Norbert E. Vint, Deputy Inspector General to Beth F. Colbert, Acting Director re: Fiscal Year 2016 Top Management Challenges (Oct. 12, 2016) in U.S. Office of Personnel Management (2016). Fiscal Year 2016 Agency Financial Report, pp. 105–107, 118–120.

[4] Briefing by Charles Phalen, Director, National Background Investigations Bureau, to H. Comm. on Oversight & Gov't Reform Staff, 115th Cong. (June 5, 2017).

[5] The National Background Investigations Bureau Impact Assessment of the FY2017 National Defense Authorization Act, Section 951 Implementation Plan (2016).

[6] Statement of Charles Phalen, Director, National Background Investigations Bureau, to H. Comm. on Oversight & Gov't Reform Staff, 115th Cong. (Oct. 11, 2017).

[7] OMB Memorandum M-17-26, Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda. (June 15, 2017).

[8] U.S. Office of Personnel Management, Fiscal Year 2016 Agency Financial Report, Nov. 2016, available at https://www.opm.gov/about-us/budget-performance/performance/2016-agency-financial-report.pdf.

Another change is in the increasing number of cases involving the Foreign Preference and Foreign Influence Guidelines. According to the U.S. Census, the total foreign-born population in the U.S. almost quadrupled, from 9.7 million in 1970 to more than 40 million during the 40-year period from 1970 to 2010. These changes in the U.S. work force as a whole are also reflected in the demographics of the cleared population. Concerns have multiplied that naturalized U.S. citizens with relatives remaining abroad might have less than 100% loyalty to their adopted land. Or, in another scenario, malefactors in a foreigner's home country might use the threat of violence to the naturalized American's relatives to coerce him to disclose classified information. [Refer to "Part Two—Adjudicative Guideline B."] DOHA now considers that these foreign relatives create a "heightened risk" of exploitation or coercion of the American-based security clearance holder.

III. ESPIONAGE

In 2017, the top three countries engaged in economic espionage against the U.S. were Russia, China, and Iran. The first target is information technology, the second is manufacturing, and the third is defense. Insiders are responsible for 71% of the espionage. Two studies by the Defense Personnel Security Research Center (PERSEREC) indicate that divided loyalty, usually on the part of naturalized Americans with roots in a foreign land, is now the dominant motive for espionage. *See* Reports at GAO-13-728T https://www.gao.gov/assets/660/655360.pdf and DoD PERSEREC, *Espionage and Other Compromises of National Security 1975–2008* (July 2009), *available at* http://www.dhra.mil/perserec/espionagecases/. Among the espionage cases involving naturalized Americans are:

— Hanjuan Jin, a former Motorola software engineer and naturalized U.S. citizen born in China, whose mother still resides in China. Jin was stopped at Chicago's O'Hare Airport in February 2007, traveling on a one-way ticket to Beijing. She came to the officials' attention only because she had declared that she had $10,000 in U.S. currency in her carry-on luggage. She was indicted for theft of trade secrets and intent to pass them to unauthorized persons.

— Xiaodong Sheldon Meng, a software engineer for a defense contractor, who was born in China and became a Canadian citizen. He was indicted on charges of economic espionage by misappropriating a trade secret, known as "Mantis 1.5.5," with the intent to benefit a foreign government, specifically China's Navy Research Center in Beijing. In August 2007, Meng pled guilty to one count of violating the Economic Espionage Act and one count of violating the Arms Export Control Act and the International Traffic in Arms Regulations.

— Donfan (Greg) Chung, a Boeing employee and naturalized U.S. citizen born in China. He was arrested in February 2008 and charged with economic espionage. He is accused of having collected and sent numerous engineering manuals relating to the B-1 Bomber to his handlers in the PRC.

— Nghia Pho, an employee of NSA's elite cyberwarfare unit—the Tailored Access Operations (TAO) unit and a naturalized American citizen born in Vietnam. In November 2017, Pho, who worked for TAO from 2006 to 2016, pled guilty to removing classified documents and taking them home. He removed these documents, from 2010 to 2015, to assist in writing his resume, but hackers were able to gain access to those documents on his home computer using antivirus software made by the Kaspersky Lab, a prominent Russian cybersecurity company. Pho pled guilty to one count of willful retention of national defense information and is scheduled to be sentenced on April 6, 2018.

— Jerry Chun Shing Lee, an ex-CIA employee and naturalized citizen born in 1965. An employee for the CIA from 1994 to 2007, he was arrested in January 2018 for keeping and traveling with notebooks containing classified information, including the real names of covert CIA employees. A mole-hunting investigation commenced after U.S. intelligence concluded that China had ascertained the identities of and detained many prized assets. It is believed that his actions contributed to the deaths or arrests of numerous informants for the United States. U.S. officials spent years gathering evidence against him because he proved to be a very savvy and difficult target given his extensive training in counter-spy defensive maneuvers. During the investigation, they discovered he had received hundreds of thousands of dollars in unexplained bank deposits. Lee is currently awaiting trial.

Others involve American-born individuals:

— Ben-Ami Kadish, an 84-year old retired engineer and U.S.-born citizen, was arrested in April 2008 and charged with four counts of conspiracy, allegedly for serving as a foreign agent for Israel and for lying to the FBI. He worked as a mechanical engineer at the U.S. Army's Picatinny Arsenal from 1963 to 1990. He apparently told the agents that he "borrowed" classified documents at the urging of his Israeli handler.

— Gregg Bergersen, a Weapons Systems Policy Analyst in the Navy International Programs Office of the Defense Security Cooperation, was a native-born U.S. citizen with Sensitive Compartmented Information (SCI) access who pled guilty in March 2008 to conspiracy to disclose national defense secrets to China. He sold classified defense information to a naturalized U.S. citizen from Taiwan, thinking that the information was for the benefit of Taiwan. Unbeknownst to Bergersen, the recipient actually forwarded the information to the government of the PRC. On July 11, 2008, he was sentenced to 57 months imprisonment.

IV. LEAKING OF CLASSIFIED INFORMATION

Recent incidents involving leaks of classified information have not typically involved individuals born abroad.

A. CHELSEA MANNING

Chelsea Manning (formerly Bradley Manning) was a U.S. Army soldier who was convicted in 2013 of leaking a massive amount of classified government data to the anti-government secrecy group WikiLeaks. In the months leading up to the unauthorized disclosure, Manning displayed behaviors indicating instability through multiple emotional and physical outbursts, expressed discontent with the Army and the federal government, and exhibited disregard for basic security measures common to all classified working environments. Manning gained access to classified databases in 2009 while assigned to an Army unit in Iraq as an intelligence analyst. Manning was caught after having confided what she had done to Adrian Lamo, himself a convicted hacker, whom Manning met online. She described herself as "isolated," "desperate," "broken," and "self-medicating like crazy." Even though Lamo was a hacker, he was concerned about the nature of the information Manning said she had leaked and turned her in to Army Counterintelligence. She was court-martialed in August 2013, found guilty of six counts of violating the Espionage Act, and sentenced to 35 years in prison. This was the longest sentence ever imposed for a leak conviction. On January 17, 2017, after being in custody for more than seven years, President Obama commuted all but four months of her sentence. She was released on May 17, 2017.

When the Manning leak to WikiLeaks first became public, the Office of Management and Budget (OMB) sent a memo to federal agencies forbidding unauthorized federal employees and contractors from accessing classified documents publicly available on WikiLeaks and other websites. Other news stories reported that university students were advised not to view classified information at WikiLeaks, because it could result in the denial of a security clearance in the future.

In 2012, as a direct result of the WikiLeaks disclosures, the President issued Presidential Memorandum: National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. *Presidential Memorandum: National Insider Threat Policy & Minimum Standards for Executive Branch Insider Threat Programs* (2012), *available at* https://www.dni.gov/index.php/ic-legal-reference-book/presidential-memorandum-nitp-minimum-standards-for-insider-threat-program. The cover memorandum signed by the President states,"elements [of an insider threat program] include the capability to gather, integrate, and centrally analyze and respond to key threat-related information; monitor employee use of classified networks; provide the workforce with insider threat awareness training; and protect the civil liberties and privacy of all personnel." *Id.*

B. EDWARD SNOWDEN

Also, of course, is the case of Edward Snowden. He was hired by the CIA in 2006 as a systems administrator and telecommunications systems officer and granted a top secret clearance. In 2007, the CIA stationed Snowden with diplomatic cover in Switzerland where he was responsible for maintaining computer network security. Snowden's supervisor wrote a negative report, voicing suspicions that Snowden was trying to break into classified computer files, which he was not authorized to access. The supervisor sent him home. Although there was an internal investigation and his clearance was suspended, he was allowed to resign and the CIA ended the investigation. The CIA never included any derogatory information in his security file. He was then hired by Dell, a private contractor, and assigned to work at an NSA facility on a U.S. military base in Japan. In 2011, U.S. Investigation Services, Inc. (USIS) completed Snowden's five-year periodic reinvestigation and gave him a new clearance because none of the derogatory information was in his file.

In 2013, Snowden was hired by Booz Allen Hamilton and sent to Hawaii to work on an NSA contract. Recruitment officials at Booz Allen discovered that he had padded his resume, but hired him anyway. While in Hawaii, he allegedly persuaded coworkers to enter their logins and passwords on his computer by telling them they were needed for him to do his job as a computer systems administrator. Snowden was able to capture the passwords, gaining extraordinary access to numerous systems. Snowden worked in Hawaii for only about four weeks before traveling to Hong Kong in May 2013 and leaking a vast trove of NSA documents describing classified surveillance programs to a British newspaper.

On June 14, 2013, Snowden was charged with theft of government property and two counts of disclosing information under the Espionage Act—charges which together carry a penalty of up to 30 years in prison. Snowden currently lives in Moscow, where his temporary residence permit has been extended until 2020.

C. STEPHEN KIM

In August 2010, Kim, an analyst working under contract with the State Department, was indicted for giving classified information to Fox News concerning the military capabilities and preparedness of North Korea and making false statements. He was born in South Korea and moved with his family to the U.S. at the age of ten. He graduated from Georgetown's School of Foreign Service, obtained a master's degree in national security from Harvard and a PhD in diplomatic and military history from Yale. He pled guilty to one charge of disclosing classified national defense information to an unauthorized person, and on April 2, 2014, was sentenced to 13-months incarceration. Some published reports said Stephen Kim may have been motivated to leak the report out of concern that the U.S. government was not doing enough to address the threat posed by North Korea.

D. THOMAS DRAKE

In April 2010, NSA employee Thomas Drake was charged with violating the Espionage Act for retaining classified documents for "unauthorized disclosure." As a senior executive with NSA, Drake opposed NSA's use of a system called Trailblazer, a data collection tool, believing that it violated the Fourth Amendment. To expose the problems he saw at the agency, Drake complained internally to his bosses, the NSA IG, the DoD IG, and both the House and Senate Congressional Intelligence Committees. Perceiving that no one was paying attention, he emailed a reporter, but did not disclose classified information. The reporter wrote several articles about waste, fraud, and abuse at the NSA, including articles on Trailblazer. As a result, Drake was suspected of leaking information to the reporter, and the FBI raided his home and confiscated his computers, documents, and books. He was never charged with disclosing sensitive information to anyone; the charge brought against him was for possessing classified documents at his home, in violation of 18 USC § 793(e). Drake is one of only four people in the history of the U.S. to be charged with "willful retention" of "national defense" information under 18 USC § 793(e).

In June 2011, Drake pled guilty to a minor charge, not under the Espionage Act, and served no prison time. The government contended that they could not prosecute him without revealing details about the documents he supposedly leaked. Critics considered this rationale suspect and noted that the case was a shameful example of government overreach.

E. SHAMAI LEIBOWITZ

In May 2010, FBI translator Shamai Leibowitz pled guilty to leaking classified information (FBI wiretaps of conversations between Israeli diplomats about Iran) to a blogger. He was sentenced to 20 months in prison. He stated, "I came across wrongdoings that led me to conclude this is an abuse of power and a violation of the law. I reported these violations to my superiors at the FBI who did nothing about them."

F. JEFFREY STERLING

In December 2010, CIA Officer Jeffrey Sterling was charged with leaking information about the CIA's efforts against Iran's nuclear program to reporter and journalist, James Risen. In 2013, the case against Sterling was stayed while the issue of whether Risen could be compelled to testify against Sterling was appealed first to the Fourth Circuit and then to the Supreme Court. The Fourth Circuit held that Risen was required to testify and had no reporter's privilege because neither the First Amendment nor common law protects journalists who promise anonymity to their sources from having to testify about those sources in criminal proceedings (Risen was granted immunity so he could not invoke the Fifth

Amendment). The Supreme Court denied *certiorari*. Risen vowed that he would go to jail before he revealed any sources, and ultimately, the department did not call him to testify.

In 2015, Sterling was convicted by a jury of ten felony counts, including multiple violations of the Espionage Act for giving classified information to a journalist, and sentenced to 42 months. He served most of his sentence and was released to a halfway house in January 2018.

G. JOHN KIRIAKOU

In January 2012, former CIA Officer John Kiriakou was charged with leaking information about the interrogation of an Al Qaeda leader and disclosing the name of a CIA analyst involved. Kiriakou gave an interview on ABC News in 2007 detailing the Bush administration's use of waterboarding in interrogating terrorist suspects. He pled guilty to one count of violating the Intelligence Identities Protection Act by passing classified information to the media and was sentenced to 2 1/2 years in prison.

H. REALITY WINNER

Another NSA contractor, Reality Winner, was charged with violating the Espionage Act for leaking to the news site, The Intercept, a single classified report about the NSA's belief that the Russians hacked the 2016 American elections through a voting software vendor. The Intercept has not identified and denies knowing the source of the report. Winner is an Air Force veteran, who held the rank of Senior Airman, serving as a Cryptologic Language Analyst who speaks Farsi, Pashto, Dari, and Urdu (learned at the Defense Language Institute while enlisted), prior to her honorable discharge. Winner has been held in pre-trial detention for the past nine months, with bail denied on the grounds that she is "dangerous" to society; a "flight risk"; and "sympathetic to terrorists" due to her ability to speak multiple languages and social media statements that she "admires Edward Snowden and Julian Assange." Currently being litigated is whether any statements taken from her while questioned in her home should be suppressed, because all parties agree Winner was never read her Miranda rights. A new trial date has not yet been established, but Winner is facing 10 years in prison.

I. HAROLD T. MARTIN, III

Harold Martin, III worked for seven private companies at various intelligence agencies, including the CIA, the U.S. Cyber Command, and the ODNI. From 2012 to 2015, he worked at the NSA as a contractor through Booz Allen Hamilton. Martin was for a period in the NSA's elite hacker unit, Tailored Access Operations. Over more than 25 years (beginning in the late 1990s), Martin took over 50 terabytes of data, including paper documents, flash drives, and hard drives of highly classified documents and files, and stored this information in his home, shed, and car. Included in the purloined information were many of the NSA's hacking tools and actual codes used to spy on other countries. In August 2016, these tools and codes eventually became available for purchase on the Internet by a group named the Shadow Brokers. The sale alerted officials to the breach, which eventually led them to Martin, although no connection between Martin and the Shadow Brokers has been established. The stolen tools, which contain the software to bypass computer firewalls, breach Windows, and break into the Linux system (most commonly used on Android phones), have been used by North Korea and Russia to carry out cyberattacks around the world. Martin was arrested on August 27, 2016. He has been charged with 20 felony counts of violating the Espionage Act. Each count can carry up to 10-years imprisonment. Martin pled guilty to one count of willful retention on January 22, 2018; however, because he did not strike a plea deal, he could still face additional prison time based upon the other 19 charges.

J. GOVERNMENT RESPONSE

In response to the cases of leaking information to the media, in March 2014, the Director of National Intelligence issued a new directive forbidding most intelligence community employees from discussing "intelligence-related information" with a reporter unless they have specific authorization to do so. Media Contacts, DNI, ICD 119 (Mar. 20, 2014), *available at* http://www.fas.org/irp/dni/icd/icd-119.pdf. The prohibition applies even if the information is not classified, as long as it is "related" to intelligence. This policy means discussions an intelligence community employee may have with a friend or neighbor (or any other member of the public) is not permitted with someone who fits the definition of a member of the media.

V. SPEED SACRIFICED QUALITY?

A. AARON ALEXIS—THE NAVY YARD SHOOTER

The September 2013 Navy Yard Shooter incident resulted in much soul-searching in an effort to figure out how an obviously troubled individual was able to maintain his security clearance and remain under the radar, notwithstanding numerous incidents that were clear indications of a person whose judgment was impaired.

The Navy Yard shooter, Aaron Alexis, was granted a secret clearance in connection with his enlistment in the Navy in 2007. He completed the Security Clearance Application (SCA), the SF-86, in which he falsely denied having been arrested. USIS conducted his investigation. He received the minimum level of investigation required for military service, the National Agency Check with Local Agency Checks and Credit Check.

The investigation revealed that he had been arrested in Seattle in 2004, but at that time, Seattle Police Department practice was to release only conviction information to U.S. Office of Personnel Management (OPM) investigators—not incident reports on arrests that did not result in a conviction. During his subject interview, Alexis was asked about the arrest and characterized it as nothing more than an altercation with another individual in which Alexis retaliated by "deflating the tires" of the other individual's car. Alexis did not disclose that he had actually shot out the tires with his Glock .45 caliber handgun. Had the police department provided the arrest report to investigators, USIS would have learned of these details, as well as that Alexis told police he had an anger-fueled "blackout" and his rampage was prompted by his fellow workers who "mocked" and "disrespected" him.

Notwithstanding Alexis's falsification of his SF-86 by failing to disclose the arrest, the Navy granted his secret clearance in 2008. Because a secret clearance did not require a new investigation for ten years, this investigation was the only inquiry done into Alexis's trustworthiness.

During his Navy enlistment, Alexis had three incidents: an arrest for disorderly conduct outside a nightclub, for which he was jailed for two days; a charge for being drunk and disorderly; and an arrest for discharging a firearm in his residence. Police records indicated that he had gone into a rage and fired a shotgun through the ceiling of his apartment because the resident upstairs was disturbing him. No charges were filed. These incidents resulted in two instances of non-judicial punishment, but they were not reported to JPAS, the central repository for clearance-related data.

After the third incident, Alexis's Commanding Officer initiated proceedings to administratively separate him from the Navy. The county district attorney's office determined there was not enough evidence to pursue the criminal case. As a result, the Navy halted the process to separate him. He received no discipline or mental evaluation. In 2011, he was honorably discharged from the Navy. What is more, he garnered a Navy Reserve Identification and Privilege card which permitted access onto Navy bases, consistent with Alexis's post-discharge status as a member of the Navy's Individual Ready Reserve.

With no adverse information recorded in JPAS and no break in service in excess of 2 years, Alexis remained eligible for a secret security clearance after his release from active duty. In 2012, he was hired by The Experts, Inc., a subcontractor to Hewlett Packard. When The Experts first hired Alexis, there was no information available in JPAS that would have alerted the company to any misconduct while on active duty in the Navy. The Experts did perform a background check, which revealed no issues of concern. It is not known whether The Experts, as part of its hiring process, contacted any references such as Alexis's former Navy supervisor to ascertain his fitness for employment.

In July 2013, The Experts assigned Alexis to a project in Newport, RI. On August 7, 2013, Newport Police were dispatched to his hotel room to respond to a complaint that a hotel guest was making noise and disturbing patrons. They interviewed Alexis, who told them he had a verbal altercation with someone who "sent three people to follow him and keep him awake by talking to him and sending vibrations into his body." He explained that he had switched hotels three times, but the individuals kept following him, talking to him through the wall, and "zapping" him with a "microwave machine" that sent vibrations which penetrated his body so he could not fall asleep. The Newport Police contacted the Newport Naval Station and faxed them a copy of their report. The Navy told the Newport Police they would follow up on it. Navy security agents decided Alexis was not a threat to the institution or himself. They did not interview Alexis, suspend his security clearance, or report the incident in JPAS. Nor did the Navy contact The Experts or suspend his base access.

Alexis contacted The Experts' human resources office multiple times to complain about hearing voices in his hotel room. Hotel records contain a log entry from the hotel clerk as follows: "Brenda from The Experts Inc., called…she explained

that he is unstable and the company is bringing him home." This did not happen. Instead, The Experts took Alexis off his Newport, RI, assignment "for a few days rest." They did not report the incident in JPAS or seek guidance from the Defense Security Service (DSS) about whether it should be reported. Apparently, The Experts believed it was not reportable because the incident did not involve criminal activity, nor had Alexis been referred to a medical facility for psychiatric evaluation.

Later in August, Alexis twice visited the VA emergency room, complaining of hearing voices, prior violent episodes, and sleep deprivation. The first time he was given a "small amount" of a generic anti-depressant and instructed to see his primary care provider. The second time, he obtained a refill of the medicine.

On September 9, 2013, Alexis reported to NAVSEA at the Navy Yard and was given an entry pass called a Common Access Card (CAC). Five days later he bought a shotgun in Lorton, Virginia. He carved into the gun the words "my ELF weapon" and "end to the torment!" ELF refers to "extremely low-frequency" in Navy submarine communications. He used a hacksaw to shorten the barrel of the gun and stock.

On September 16, 2013, Alexis arrived at the Washington Navy Yard, used his pass to gain entry, and over the course of approximately one hour, shot and killed 12 victims and wounded four surviving victims before being shot and killed by law enforcement officers. A document retrieved after the shooting from Alexis's computer or cell phone stated, "[u]ltra low frequency attack is what I've been subject to for the last 3 months, and to be perfectly honest that is what has driven me to this."

B. CONGRESSIONAL RESPONSE

After the Navy Yard Shooting, the issue of reforming security clearances received increased attention from Congress. The new watchword was (and is) "Continuous Evaluation" (CE). A bipartisan group of senators introduced legislation in October 2013 requiring frequent records checks of an increased number of government, public, and commercial databases—including those of the major consumer reporting agencies. An independent DoD panel recommended that personnel undergo a status-change review at key junctures in their career, rather than waiting for the next scheduled periodic reinvestigation.

In April 2014, two Democratic and two Republican Senators introduced bipartisan legislation to implement periodic automated reviews of public records and databases by OPM for any information that might affect the security clearance status of individuals who have such a clearance. These audits would identify information that individuals are already obligated by law to disclose, including information relating to any criminal or civil legal proceeding; financial information; data maintained on any terrorist or criminal watch list; and any publicly-available information that suggests ill intent, vulnerability to blackmail, compulsive behavior, allegiance to another country, or change in ideology of the covered individual.

Another review panel recommended that, in adjudicating security clearance cases involving allegations that the individual falsified the SF-86 by failing to disclose relevant information, DoD be required to "adjudicate more restrictively."

One report recommended that investigators be required to explore social media sites and to facilitate that process applicants be required to disclose their passwords. They observed, "anyone who seeks to be trusted with a clearance should not object to allowing an evaluation of social-media information and images that he…may have voluntarily shared with hundreds or thousands of people worldwide." Security From Within: Independent Review of the Washington Navy Yard Shooting 21 (Nov. 2013), *available at* https://www.defense.gov/Portals/1/Documents/pubs/Independent-Review-of-the-WNY-Shooting-14-Nov-2013.pdf.

An Army pilot program reviewed approximately 3,370 cleared Army personnel and found that at least 20% of the individuals had information relevant to adjudication. Although that information was not disqualifying on its own, it was thought to have "potential value."

Another proposal recommended encouraging a "culture in which it is acceptable to report concerns about colleagues who are showing signs of disturbance or violent tendencies." *Id*. This would mark a shift from a system largely reliant on self-reporting to one that encourages coworkers, supervisors, and even family members, to communicate their concerns:

> DoD must provide mechanisms for parties to report concerns without exposing their identities. Employees who

> report on their workmates must feel safe from both violence and any negative consequences of reporting, such as reprisal…. Friends and family, outside care providers, and other threat management teams (such as those established at educational institutions in some states), may provide key pieces of the puzzle in assessing threats.
>
> DoD must create policy and procedures to enable employees, family members, or the general public to report on troubling behavior. Availability of multiple reporting channels may encourage active employee participation. These could include anonymous tip lines and increased awareness campaigns to spread the word that early reporting of suspect behavior could prevent a potential terrible and violent act. DoD must establish training programs to educate the work force that peer reporting is critical and no stigma should attach to the act of reporting a serious concern.

Id. at 20.

Continuous Evaluation continues to be the watchword today. The National Counterintelligence and Security Center (NCSC) began a one-year CE pilot in September 2016, and is scheduled to roll out a fully functional CE system by Fall 2018. The system will cover executive branch employees and check about ten databases for warning signs. Any executive branch agency will be able to use it. The initial focus will be on holders of TS clearances with those holding secret clearances included next. NCSC developed a community-wide best practices directive, which OMB is currently reviewing. In addition, an SEAD is being developed to ensure consistency among agencies using CE programs, but it is not yet available. A November 2017 report from GAO outlined in detail the myriad problems facing the roll-out of the CE program. U.S. GAO, GAO-18-117, Personnel Security Clearances: Plans to Oversee Continuous Evaluation of Clearance Holders (2017), *available at* https://www.gao.gov/assets/690/688530.pdf.

Daniel Payne, Director of DSS, explained that DoD's CE process, which began in October 2014, now regularly checks approximately 22 different databases. DoD planned to enroll 1 million employees by the end of calendar year 2017 and all clearance holders by the end of FY2021. DoD's CE IT system is called Mirador. When a records check results in an alert, it is forwarded to DSS's CE validation cell to ensure:

(1) the alert applies to the correct individual;

(2) the issue was not previously known; and

(3) the issue is adjudicatively relevant.

If all three concerns are met, a report is forwarded to the individual's designated security manager (SMO). The SMO gathers any additional information necessary and prepares a final report that is forwarded to the CAF. Adjudicators at the CAF may request additional information or make a determination whether to continue access to classified information or take adverse action. All due process safeguards are applicable to CE actions.

The Department of State also implemented a CE pilot program in January 2015, but because there is no overarching guidance yet from ODNI, DoD's and State's CE programs have taken different approaches. State is now monitoring all of its Tier 5 employees. Because State has its own investigative functions, follow-up is easy. According to officials, minor issues, such as traffic violations, are added to personnel files for consideration during the individual's next periodic reinvestigation.

Because there are still significant gaps in certain databases, for example, many local criminal records databases are incomplete or inaccessible, periodic reinvestigations will continue alongside CE for the time being, though the ultimate goal is to dispense with them entirely.

C. US ARMY MAJOR NIDAL HASAN—2009 FORT HOOD SHOOTER

On the one hand, encouraging coworkers to file reports on their colleagues has great potential for abuse. Someone with a quirky personality could find herself marched out of the facility, suspended without pay, and having to obtain a private psychiatric evaluation and report before being certified as fit for duty.

On the other hand, someone like U.S. Army Major Nidal Hasan, the 2009 Fort Hood shooter, might have been stopped had his colleagues and superiors been more aggressive about reporting his behavior. Before his assignment to Fort Hood, Hasan worked as an intern and resident at Walter Reed Army Medical Center. His colleagues and superiors there

expressed concern about his behavior and comments. Hasan was described as socially isolated, increasingly and vocally opposed to the wars in Afghanistan and Iraq, and troubled by his work with traumatized soldiers returning from combat. In the year leading up to the attack, Hasan was known to have been in communication with Anwar Al-Awlaki, expressing interest in jihad and suicide attacks. Army commanders were notified of his emails to Awlaki, but at the time their communications were deemed nonthreatening.

D. U.S. INVESTIGATIONS SERVICES, INC. (USIS)

Questions about the adequacy of security clearance investigations focused more attention on the company that did the majority of background checks, USIS. The company previously served as the investigative branch of the OPM until it was privatized in 1996 as part of then-Vice President Al Gore's effort to "reinvent" government by reducing the size of the civil service. The company conducts background security checks through contracts with OPM. In Fiscal Year 2012, USIS received $253 million for its contract work with OPM, comprising 67% of OPM's contract spending for that fiscal year. As of June 2013, it had 100 federal contracts, conducted background checks for over 95 federal agencies, and was the largest background security check provider for the U.S. government.

In 2011, a former USIS employee, Blake Percival, sued USIS under the False Claims Act, alleging he was fired in retaliation for refusing to certify cases as complete before they had gone through the full review process. Percival was the Director of Fieldwork Services, a position that oversaw the work of 350 reviewers reviewing all the ROIs of each case for completeness and thoroughness before submitting them to OPM. The complaint alleged that in order to boost revenue and profit, USIS would certify investigations as complete and release them to the government for payment, although they had not received the quality reviews required by the contract. This was called "dumping" or "flushing."

Among other colorful details in the court complaint are employee emails stating: "Shelves are as clean as they could get. Flushed everything like a dead goldfish" and "They will dump cases when word comes from above." In another email, the director of national quality assurance wrote: "Come EOM [end of month], if they're going to tell us to just dump all those cases anyways without a proper review, which will only make that ugly baby even uglier." The same person also wrote, "We dumped all we could to try and hit the 1,100 mark but fell short," according to the complaint.

The U.S. government joined the case in October 2013, accusing the company of failing to provide adequate background checks in at least 665,000 instances. The case was initially filed as *United States of America ex rel Blake Percival v. U.S. Investigations Services, LLC*, No. 2:11-cv-00527, U.S. District Court, Middle District of Alabama (Montgomery); when the federal government joined the case it became *United States of America, ex rel., Blake Percival v. U.S. Investigations Services*, LLC, No. 14-cv-00726-RMC (D.D.C.). The government alleged that beginning in at least March 2008 and continuing through at least September 2012, USIS deliberately circumvented contractually required quality reviews by "dumping" or "flushing," which involved releasing cases to OPM and representing them as complete when, in fact, not all the reports of investigations comprising those cases had received a contractually-required quality review.

In July 2014, after being hit by a massive cyberattack, OPM suspended its contract with the firm.

In February 2015, USIS filed for bankruptcy. The case against it was settled in August 2015 with USIS agreeing to forgo their right to collect payments of amounts claimed owed to them by OPM, totaling more than $30 million. As a whistleblower, Percival was ultimately awarded 20% or approximately $6,000,000.

E. NATIONAL BACKGROUND INVESTIGATIONS BUREAU (NBIB)

On September 29, 2016, President Obama issued Executive Order 13741, which amended Executive Order 13467, and established the National Background Investigative Bureau (NBIB), housed within OPM, and tasked with conducting OPM's background investigations. The purpose of the NBIB was to:

> serve as the primary executive branch service provider for background investigations for eligibility for access to classified information; eligibility to hold a sensitive position; suitability or, for employees in positions not subject to suitability, fitness for Government employment; fitness to perform work for or on behalf of the Government as a contractor employee; and authorization to be issued a Federal credential for logical and physical access to federally controlled facilities and information systems.

EO 13741 § 2.4(1)(a). While NBIB is headquartered in Washington, DC, it has offices throughout the U.S. and in select