HOW TO USE THE SECURITY CLEARANCE LAW AND PROCEDURE GUIDE

Statutes, Executive Orders, DOD directives and regulations, and Defense Office of Hearings and Appeals (DOHA) and court decisions, among other reference materials, are all discussed in this book as they relate to security clearances. In an effort to assist our readers in navigating their way through this book and the governing law, we have developed the following "how to" section.

DOHA is the administrative body within the DoD that renders decisions on federal employees' and contractors' eligibility to access classified U.S. government information. DOHA decisions are available through a search engine at http://ogc.osd.mil/doha/industrial/.

ISCR Case No. XX-XXXX (App. Bd. month, day, year), is the current format used to cite DOHA Appeal Board decisions. The first two digits of the case number reflect the year the case was first received by DOHA. Administrative Hearing Judge decisions are indicated using ID (initial decision) or RD (remand decision) in place of App. Bd. ADP is used in place of ISCR for Public Trust cases. DISCR is simply the predecessor to ISCR. Page references are provided where they are indicated in the decisions on the DOHA website. On the DOHA website, but not on Westlaw, the cases will have a letter and number following each ISCR Case No. that reflect the procedural posture of the case, e.g., ISCR Case No. 17-00541.a1. All initial hearing decisions end in .h1; all Appeal Board decisions end in .a1; hearing decisions following remand from the Appeal Board end in .h2; and Appeal Board decisions following a remanded decision (or second appeal) end in .a2.

DOHA refers to its written Personal Appearance recommended decisions as "Recommended Decision of Administrative Judge [name]." The case number reflects the referring organization, such as WHS-C (Washington Headquarters Service) and the date. In its citations, the government puts the letters first so that the case name appears as WHS-C No. XX-XXXX.

Security Executive Agent Directive (SEAD) 4—National Security Adjudicative Guidelines; DoD Directive (DoDD) 5220.6 Defense Industrial Personnel Security Clearance Review Program (which incorporates SEAD 4 as Enclosure 2); and DoD Manual (DoDM) 5200.02 Procedures for the DoD Personnel Security Program (PSP) guide all of DOHA's decisions and are cited with regularity therein. On June 8, 2017, the National Security Adjudicative Guidelines, contained within SEAD 4, were revised. https://fas.org/sgp/othergov/intel/sead-4.pdf. These revised Guidelines create common criteria for all civilian and military personnel, consultants, contractors, licensees, certificate holders or grantees and their employees, and other individuals who require access to classified information or eligibility to hold a sensitive position and are to be used by all Executive Branch Agencies. Because of the changes to the Guidelines over the decades, the reader will find them referenced in various iterations throughout the DOHA decisions, including: AG (Adjudicative Guidelines), SEAD 4, and Directive 5220.6 Enclosure 2.

Appendix 2 of this book contains a list of important documents and publications and where they can be found on the web.

ACRONYMS AND ABBREVIATIONS USED IN THIS GUIDE

AA	Alcoholics Anonymous
ACDC	Alcohol Consumption Disqualifying Condition
ADR	Adjudicative Desk Reference
AGA	Another Government Agency, usually referring to the CIA or NSA
AJ	Administrative judge
ANACI	Access NACI
APG	Additional Procedural Guidance
App. Bd.	DOHA Appeal Board
ASDC3I	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
Board	DOHA Appeal Board
CAF	Central Adjudication Facility(ies)
CATS	Case Adjudication Tracking System. This is the DoD's case management system for investigation and adjudication information.
CD	Compact disc
CI	Counterintelligence
CIA	Central Intelligence Agency
DC	Disqualifying condition
DCID	Director of Central Intelligence Directive
CVS	Central Verification System is the OPM-managed database used to record adjudicative outcomes for all investigations performed by OPM and includes government-wide debarments.

DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIMC	Drug Involvement mitigating condition
Directive	Department of Defense Directive 5220.6 Defense Industrial Personnel Security Clearance Review Program, issued January 2, 1994, as amended by Change 1 (Nov. 22, 1993), Change 2 (May 20, 1994), Change 3 (Feb. 16, 1996), Change 4 (April 20, 1999), and incorporating the revised National Security Adjudicative Guidelines issued by the Director of National Intelligence, which are effective for any adjudication on or after June 8, 2017.
DISCO	Defense Industrial Security Clearance Office
DISCR	Defense Industrial Security Clearance Review
DNI	Director of National Intelligence
DoD	Department of Defense
DoD CAF	DoD Consolidated Adjudication Facility
DoDD	Department of Defense Directive
DoDI	DoD Issuances
DoDM	Department of Defense Manual
DOHA	Defense Office of Hearings and Appeals
DSM	*Diagnostic and Statistical Manual of Mental Disorders*
DSS	Defense Security Service
DSS OCC	Defense Security Service Operations Center, Columbus
DUI	Driving under the influence of alcohol
DWI	Driving while intoxicated
EEOC	Equal Employment Opportunity Commission
EO	Executive Order
FBI	Federal Bureau of Investigation
FIMC	Foreign influence mitigating condition
FOIA	Freedom of Information Act
FOIA/PA	Freedom of Information Act/Privacy Act
FORM	File of Relevant Material
FSO	Facility Security Officer
ID	Initial Decision
IG	Inspector General
IRS	Internal Revenue Service
ISCR	Industrial Security Clearance Review
ISP	Industrial Security Program
JPAS	Joint Personnel Adjudication System
JVS	Joint Verification System
LOD	Letter of Denial
LOI	Letter of Intent
MC	Mitigating condition
MSPB	Merit Systems Protection Board
NAC	National Agency Check
NACLC	NAC with Local Agency Check and Credit
NAF	Nonappropriated Fund positions
NACI	National Agency Check and Inquiries
NISPOM	National Industrial Security Program Operations Manual
NOIA	Notice of Intent to Appeal
NOPA	Notice of Proposed Action
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
OI	Operating Instruction
OSD	Office of the Secretary of Defense
PA	Personal Appearance
PAG	DOHA Personal Appearance Guide
PCDC	Personal conduct disqualifying condition
PCMC	Personal conduct mitigating condition
PERSEREC	Defense Personnel Security Research Center
PHG	DOHA Prehearing Guidance
PIPS	Personnel Investigations Processing System
POC	Point of contact
PRC	People's Republic of China (China)
PSAB	Personnel Security Appeal Board
PSI	Personnel Security Investigation
RD	Remand Decision

Regulation	DOD Regulation 5200.2-R, Personnel Security Program, January 1987, as amended by Change 1 (Feb. 12, 1990), Change 2 (July 7, 1993), Change 3 (Nov. 8, 1995), and incorporating the revised Adjudicative Guidelines as indicated by the memorandum from the Under Secretary of Defense on August 30, 2006. Incorporated and cancelled on April 3, 2017, by DoD Manual 5200.02, Procedures for the DoD Personnel Security Program (PSP).
ROI	Report of Investigation
SAP	Special Access Program
SCA	Security Clearance Application
SCI	Sensitive Compartmented Information
SEAD	Security Executive Agent Directive
SF	Standard Form
SOR	Statement of Reasons
SSBI	Single Scope Background Investigation
TS	Top Secret
USIS	United States Investigative Services, Inc.
WHS	Washington Headquarters Service

CHAPTER ONE
SECURITY CLEARANCES: ONE STANDARD—MANY PROCESSES

It has been twenty years since Robert Hanssen was arrested for spying for Russia while working for the FBI. As he pled in 2001 before receiving a life sentence (without parole), he had used his position at the FBI to access highly classified national security and counterintelligence information and provide it to the KGB and its successor SVR in exchange for sizeable payments of cash. A 25-year veteran of the FBI, Hanssen was an expert in counterintelligence, and some speculated that his interest in spying was less the money than the challenge of beating the systems in place to protect U.S. national security information. It was, for the United States, a disastrous intelligence failure and Hanssen's case caused a review of those systems and changes to the vetting process for individuals working with national security information. His case is a good illustration of the central importance of personnel security—in particular, security clearances—in protecting U.S. national security interests. However strong physical security may be, however strong the walls or gates, however vigilant the guards, the threat from the human beings working inside the building cannot be addressed with walls or guards alone. While the government's system for securing its secrets includes requirements for facilities that must be physically secure, and networks which must be made resistant to cyber-attacks, most of all, the people who work with and for the federal government, occupying confidential positions or having access to national security information, must be vetted to ensure they can be trusted with the nation's secrets. That vetting process is the subject of this book.

Predicting whether a person is trustworthy is highly complex. The government does it by collecting a lot of information about a person's life history, evaluating it against set standards, and carefully scrutinizing any concerning information that appears to indicate poor judgment, unreliability, or lack of trustworthiness. Each determination is specific to a person's own facts and life history. This makes reliance on precedent complicated and predictions difficult. It is also the reason that the process is slow, requiring individualized investigation and adjudication. In the end, a person's past conduct is used as the basis for predicting future reliability.

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). Standards for these are set by the Director of National Intelligence (DNI). 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.

The DOE issues two levels of clearance, also called access authorization:

1. 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.
2. 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.

There also are higher levels of access: to Sensitive Compartmented Information (SCI), Special Access Program (SAP), and Restricted Data (RD) that require additional vetting. SCI provides access to intelligence information and material

that requires restricted handling within compartmented channels. A SAP is "established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level." DoDD 5205.07 at Glossary p. 19 (July 1, 2010). An unacknowledged SAP is a SAP having protective controls ensuring the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information (in other words, the very fact of its existence is classified). A waived SAP is an unacknowledged SAP with more restrictive reporting and access controls. Standards for these are also set by the DNI.

The ultimate determination of a person's access is the responsibility of the specific department or agency. 32 CFR 147.2(b). A person's clearance is determined by the work they will perform, usually described in the federal employee's position description or in the federal contractor's contract and is tied to the position, not to the person.

A clearance decision is described in the Adjudicative Guidelines (AG) as "an overall common sense determination." 32 CFR 147(c). A "sufficient period of a person's life" is examined and "[a]vailable, reliable information about the person, past and present, favorable and unfavorable," is considered in reaching the determination. *Id.* In an instruction that is basic to the clearance determination, the AG mandates, "Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security." *Id.* at § 147.2(b).

The investigation for and adjudication of personnel security clearances is part of a continuum of federal investigations and adjudications conducted as needed for new federal employees and employees of federal contractors. A Public Trust position is one that has no national security sensitivity but is judged to pose a level of potential damage to the public's trust if abused. Though it is sometimes inaccurately referred to as a Public Trust clearance, it is not a clearance at all but a type of background investigation based on a position designation. It involves a process very much like that required for a security clearance, though there are significant differences also: the particular application form (the SF-85 for positions designated Low-Risk; the SF-85P for Moderate or High-Risk positions) asks for significantly less information than the SF-86 required for clearance holders, and the investigation required is not as extensive. The adjudication is made according to similar but not identical standards; the same Adjudicative Guidelines are used to adjudicate appeals for Public Trust positions.

Most federal employees are subject to a background investigation when they are first hired to determine their "suitability" for federal employment. Employees of federal contractors are often subject to a similar vetting to determine their "fitness." [Refer to Chapter 3, "Fitness for Contractors or Others No Covered by Suitability.] To obtain a Personal Identity Verification (PIV) card, allowing access to facilities or computer systems, a new federal employee or employee of a federal contractor is subject to the vetting required under Homeland Security Presidential Directive 12, which established a common identification standard for federal employees and contractors. [Refer to Chapter 3, "PIV Card."]

The success of the vetting process in protecting the nation's security is constantly under debate—especially when there is some new breach that reminds us of the government's vulnerability to the people who work for the government and have access to government secrets. Robert Hanssen's years of espionage highlighted flaws in the system; as did Edward Snowden's more recent disclosures. But the strongest catalyst for change probably were the attacks of 9/11 and the conclusions of the 9-11 Commission. *See* The National Commission on Terrorist Attacks Upon the United States, Public Report, *available at* https://www.9-11commission.gov/.

The success of the vetting process is judged, too, on speed: how long does it take for the government to hire a qualified individual and put them to work in a job requiring a clearance? That depends in many cases on how quickly a person's clearance investigation can be completed and adjudicated. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) imposed strict requirements for the completion of security clearances: by 2009, 80% had to be completed within an average of 90 days. The Government Accountability Office added the DOD's security clearance process to its High-Risk List in 2005, citing both the more than 350,000 clearances delayed beyond mandated completion dates and the lack of a management strategy to address backlogs. https://www.gao.gov/assets/gao-05-207.pdf. In February 2005, DOD investigations were transferred to the Office of Personnel Management (OPM) for completion, although DOD retained responsibility for adjudicating its own clearances. Yet, the delays did not improve. The National Background Investigations Bureau (NBIB), a semi-autonomous entity within OPM, was created in 2016 in an effort to streamline and enhance investigations. Despite this, in early 2018, the backlog of security clearances had crested at 725,000, with clearances taking far longer than the allowed 90 days for completion. Although NBIB had some success in reducing the backlog (by June 2019 it was down to 424,000 cases), on September 29, 2019, all NBIB functions were transferred back to the DOD and NBIB was subsumed within the new Defense Counterintelligence and Security Agency (DCSA) pursuant

to Section 951 of the FY18 National Defense Authorization Act and Executive Order 138690. By May 2021, the backlog had fallen to approximately 200,000 cases.

To speed the process, the government has scrutinized which jobs should require a clearance, what level of clearance is needed, and what type of investigation should be done for each level of clearance. The government has sought to reduce unnecessary replication of efforts by insisting in many cases on reciprocity of security clearance investigations and adjudications between agencies. Most of all, it has standardized the processes that underlie a security clearance determination and even worked to align the security clearance process with other processes, like suitability and fitness determinations that also require background investigations and adjudication.

I. RECOGNITION OF THE NEED FOR A SINGLE NATIONAL STANDARD AND PROCESS

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), PL 108-485 which became law on December 17, 2004, sought to establish a more uniform system for ensuring personnel security investigations and adjudications within the intelligence community. Title III of the Act requires that the President designate a single entity to over*see* the security clearance process throughout the intelligence community and to develop uniform standards for access to classified information. This led to the creation of the DNI, who serves as principal advisor to the President, the National Security Council, and the Homeland Security Council on intelligence matters related to national security, and directs and oversees the National Intelligence Program. The IRTPA also mandated centralized oversight of the security clearance process in a single agency, chosen by the President. It mandated, too, developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of security clearances and determinations for access to highly sensitive programs, including the standardization of security questionnaires, financial disclosure requirements, and polygraph policies and procedures. IRPTA, now codified at 50 USC 3161(a)(2). Finally, it required the DNI to "ensure reciprocal recognition of eligibility for access to classified information or eligibility to hold a sensitive position among the agencies." *Id.* at § 2.5(e)(viii).

Significant changes in personnel security followed the terrorist attacks of 9/11. Similar to the IRTPA, the 9-11 Commission recommended that a single federal agency be responsible for providing and maintaining security clearances, ensuring the use of uniform standards, including uniform security questionnaires and financial report requirements, and maintaining a single database. *See* Final Report of the National Commission on Terrorist Attacks Upon the United States at 422 (Government Printing Office, 2004), *available at* http://www.9-11commission.gov. It also recommended that the designated agency be responsible for administering polygraph tests on behalf of agencies that require them. In 2005, OPM was designated as the agency responsible for establishing standards for security clearances for the federal government and for being the basic provider of background investigations. (Prior to 2005, OPM, as the successor of the old Civil Service Commission, had been performing most personnel security investigations for the federal government outside of DOD. DOD had conducted its own background investigations for both military and civilian personnel.) In 2016, the NBIB was responsible for 95% of personnel investigations in the federal government. That changed in October 2019 when NBIB was folded into the newly created DCSA. Executive Order 13869 Transferring Responsibility for Background Investigations to the Department of Defense (Apr. 24, 2019). DCSA is now charged with responsibility for personnel security investigations for security clearances as well as for suitability and fitness.

A recognition that various vetting processes across the federal government would benefit from coordination is apparent in the next effort to align processes across the government. Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information (June 30, 2008). EO 13467 established the Security Clearance, Suitability, and Credentialing Performance Accountability Council (PAC) to oversee the Security and Suitability Reform Effort and ensure agency-wide alignment on these issues. It also designated the DNI as the Security Executive Agent (SecEA), responsible for developing, implementing, and monitoring policies and procedures for security clearance investigations and adjudications for security clearances. The Director of OPM, who is also a member of the PAC, became the parallel Suitability Executive Agent (SuitEA) responsible for processes governing suitability investigations and determinations as well as credentialing. The third member of the PAC is the Under Secretary of Defense for Intelligence and Security. The PAC is chaired by the Deputy Director of OMB. The creation and continuing role of the interagency PAC represents one of the clearest efforts toward standardizing personnel vetting in the federal government and establishing a mechanism for aligning security clearance processing with suitability processing.

A critical addition to EO 13467 was the introduction of Continuous Evaluation (CE), which was defined as "reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information." EO 13467 § 1.3(d). Although originating in 2008, in 2015, the DOD was still working on implementing CE. *See* Report on DOD Plans to Adopt Continuous Evaluation (CE) and Insider Threat Capabilities within the Department of Defense (DOD) (Apr. 10, 2015) (describing "CE" as an "interim capability"), *available at* https://fas.org/sgp/othergov/dod/ce-2015.pdf. The DNI established CE within the National Counterintelligence and Security Center (NCSC) with the goal of continuously reviewing the background of individuals who have been determined to be eligible for access to classified information or eligible to hold a sensitive position. https://www.dni.gov/files/NCSC/documents/products/CE_FAQ_Sep_2020.pdf.

In March 2019, the joint efforts of the PAC resulted in an initiative, Trusted Workforce 2.0, which purports to radically rethink the personnel security process. In part, it does this by using technology to reduce unnecessary time-consuming processes, such as replacing the in-person interview with a secure teleconference. Technology should also help with a more ambitious effort, to first augment and eventually replace periodic reinvestigations and CE with "Continuous Vetting" (CV) of clearance holders. Trusted Workforce 2.0 also seeks efficiencies from the alignment of the separate personnel vetting processes for credentialing, suitability, and security clearances. [Refer to Chapter 3]

Increasing numbers of cleared employees across the government are being enrolled in the CE program and subjected to continuous monitoring, which currently supplements but does not replace periodic investigations. Additionally, parts of the planned National Background Investigation Services platform have begun to appear in the Defense Information System for Security (DISS) at DCSA. DISS replaced the earlier storage system for clearance information, the Joint Personnel Adjudication System (JPAS), but provides more than just storage: DCSA describes it as, "[a]n innovative, web-based application" that "provides secure communications between adjudicators, security officers, and components, allowing users to request, record, document, and identify personnel security actions." https://www.dcsa.mil/is/diss/.

Whistleblower protection for clearance holders became a part of the DNI's portfolio with PPD-19, Protecting Whistleblowers with Access to Classified Information, signed on October 10, 2012, giving the DNI overall responsibility for intelligence community whistleblowing and source protection. [Refer to Chapter 4, "Whistleblowing for Clearance Holders."] With this last piece in place, the DNI became solely responsible for directing the oversight of investigations and adjudications for personnel security clearances; developing and implementing uniform and consistent policies and procedures for completion of security clearances and access determinations to highly sensitive programs; serving as the "final authority" to designate an authorized investigative agency or authorized adjudicative agency; ensuring reciprocal recognition of access to classified information among agencies of the federal government; ensuring, "to the maximum extent practicable," that sufficient resources are available in each agency to achieve clearance and investigative program goals; and reviewing and coordinating the development of tools and techniques for enhancing the conduct of investigations and the granting of clearances. The NCSC within the ODNI is where these personnel security responsibilities have been located, with the Special Security Directorate within NCSC serving as the executive staff for all SecEA functions. https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent. The DNI has shaped the entire personnel security process for the federal government, issuing a series of policies titled Security Executive Agent Directives (SEAD) that impose standards on the process. SEAD, *available at* https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-policy.

II. THE SECURITY CLEARANCE PROCESS ACROSS THE FEDERAL GOVERNMENT

Because of the above changes, the vetting process to determine eligibility for access to classified information—a security clearance—has been broadly standardized across the federal government. While some variations from agency to agency are allowed, the central process is common to all: a standard form elicits a person's life history and other "security significant" information in great detail across a wide range of topics. An investigation is then initiated, following protocols designed for the level of access sought. The resulting investigative record is reviewed and adjudicated according to criteria set by the ODNI and found in SEAD 4, National Adjudicative Guidelines. The adjudicator looks for evidence of poor judgment, unreliability, and lack of trustworthiness, in order to make a prediction whether the individual "can be relied upon and trusted to exercise the responsibility necessary for working in an environment where protecting the

national security is paramount." SEAD 4, App. A § 1(b). It is an individualized, fact-based, "common-sense" determination that focuses ultimately on whether it is in the country's best interest to grant, continue, or deny that person's access to the nation's secrets.

If the clearance is granted (or regranted), the individual will be subject to the requirements applicable to every clearance holder, including the duty to self-report [refer to Chapter 4, "Self-Reporting Security-Significant Information"]; Continuous Evaluation [refer to Chapter 4, "Continuous Evaluation"]; and reinvestigation (5 or 6 years for a Top Secret clearance; 10 years for a Secret; and 15 for a Confidential). However, there is a strong presumption against the grant or maintenance of a security clearance. ISCR Case No. 15-06440 (App. Bd. Dec. 26, 2017), *citing Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990), *cert. denied*, 499 U.S. 905 (1991). If there are any concerns that granting access is not in the best interest of the United States, the clearance will be denied. The process for appealing that denial is discussed in Chapters 5–9.

A. STANDARD FORM USED TO COLLECT APPLICANT INFORMATION

A standard form is used to collect individuals' information for security clearances: the SF-86, called the e-QIP when accessed online, as it now most always is. The Department of Energy refers to this form as the Questionnaire for National Security Positions (QNSP), while Defense Office of Hearings and Appeals (DOHA) decisions will speak of the Security Clearance Application (SCA), meaning the SF-86 or 85P, as relevant. No matter what it is called, the same information is collected as a first step in the security clearance vetting process, irrespective of the agency and whether the applicant is military, federal civil service, or a federal contractor. The SF-86/e-QIP is discussed at greater length below. [Refer to Chapter 2 on gathering personal information.]

B. BACKGROUND INVESTIGATIONS ARE DEFINED IN FEDERAL REGULATIONS

In 2012, the Security Executive Agent (the DNI) and the Suitability Executive Agent (the Director of OPM) jointly issued the Federal Investigative Standards, which are standard criteria for background investigations in the federal government to determine eligibility for logical and physical access, suitability for federal government employment, fitness to perform work for the federal government as an employee of a federal contractor, and eligibility for access to classified information or to hold a sensitive position. *See, e.g.*, https://www.dcsa.mil/Portals/91/Documents/pv/fso/Tier_Investigations.pdf; https://www.dhs.gov/sites/default/files/publications/federal_investigative_standards_crosswalk_guide.pdf. These standards are now codified at 32 CFR 147.18-24 and Attachments to 32 CFR Part B, A-D. The standards provide a floor for investigations, and they represent a basic standard for all United States government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees, and other individuals who require access to classified information, to include SCI and SAP, and are to be used by government departments and agencies as the investigative basis for final clearance determinations. 32 CFR 147.18. Three standards have been established, each specifically tied to a specific clearance level. *Id.* at § 147.19. Agencies are explicitly allowed to add "any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or reinvestigation." *Id.* at § 147.18. Thus, while every clearance investigation will follow the standards in 32 CFR 147.18-24 and Attachments A–D, each may—and very likely will—include additional elements required by a specific department or agency, such as a polygraph, or to address the facts of an individual case. An investigation may be terminated at any time, if sufficiently derogatory information has been uncovered and is determined by the agency adjudicating the clearance to be credible. SEAD 4, App. A § 2(e). Background Investigations are discussed in greater detail below. [Refer to Chapter 2 on gathering personal information.]

Most—but not all—of the background investigations in the federal government are now handled by the DCSA, not only for DOD but also for other agencies on a contract basis. The State Department's Bureau of Diplomatic Security, Diplomatic Security Service (DSS), for example, conducts personnel security background investigations for the Department of State and other federal agencies. https://www.state.gov/security-clearances. Nevertheless, DCSA provides services to State for its contractors. *See* https://www.dcsa.mil/about/agreements/.

Whether an agency relies on DCSA to perform the background investigation or does its own, the investigation must conform to the basic standards that are set in federal regulations. 32 CFR 147.18. If a position requires a polygraph, standards have been established for their use, as well. [Refer to Chapter 2, "The Polygraph."]