THE SECURITY CLEARANCE **DEFENSE KIT**

A Guide for Federal Employees

Your Clearance is Your Career. Protect It.

SOLOMON LAW FIRM, PLLC

202-980-2326 www.fedemploylaw.com

Nationally Recognized Employment Law Firm

Welcome to the **Security Clearance Defense Kit**, provided by Solomon Law Firm, PLLC. This guide is designed to help federal employees understand the security clearance process and how to protect their careers. Navigating security clearance issues can be complex. We are here to provide guidance and support.

Holding a security clearance is a privilege that comes with immense responsibility. For many federal employees and contractors, losing your clearance doesn't just mean losing access to files—it means losing your job.

Sanctions for mishandling information can be severe, ranging from suspension to criminal prosecution. This guide outlines the critical definitions, prohibited acts, and rights every cleared professional must know to remain compliant under Executive Order 13526.

UNDERSTANDING THE SECURITY CLEARANCE PROCESS

The security clearance process is a comprehensive evaluation conducted by the federal government to determine if an individual is eligible for access to classified information. This process involves a thorough background check, including a review of your personal history, financial records, and any potential security concerns.

The key stages of the process typically include:

- **Application:** Completing the necessary forms, such as the SF86 and getting fingerprinted.
- **Investigation:** Background checks and interviews are conducted.
- **Adjudication:** A determination is made based on the investigation.
- **Continuous Evaluation:** Ongoing monitoring for potential security concerns.

THE LEVELS

Know What You Are Handling. The classification of information is specific to the severity of damage that could be expected if the information were disclosed to an unauthorized recipient.

- **TOP SECRET (TS):** Information that could reasonably be expected to cause **exceptionally grave damage** to the national security if disclosed.
- **SECRET (S):** Information that could reasonably be expected to cause **serious damage** to the national security if disclosed.
- **CONFIDENTIAL (C):** Information that could reasonably be expected to cause **damage** to the national security if disclosed.

The Department of Energy (DoE) issues two additional types of clearance: the “Q” Clearance and the “L” Clearance based on the Atomic Energy Act of 1954. DoE has the power and responsibility for all nuclear energy information for the United States.

- **The Q Clearance** is the highest DoE clearance equivalent to Top Secret. It permits access to Top Secret Restricted Data (RD), Formerly Restricted Data (FRD) and certain National Security Information concerning nuclear weapons programs and other high-risk national security programs.
- **The L Clearance** is a lower-level DoE clearance equivalent to Secret or Confidential. It allows an employee access to Confidential Restricted Data in addition to both Confidential and Secret FRD, National Security Information or facility access.

Several positions require extra protection beyond classification, so the Government uses control systems or compartments. These include Sensitive Compartmented Information (SCI) or Special Access Programs (SAP).

Positions that require an SCI designation are often found within the intelligence community to protect sources and methods. Access requires usually Top Secret clearance, eligibility for SCI, a “need to know” and being “read in” to a specific compartment.

Positions that require a SAP protect particularly sensitive defense, intelligence or national security programs. As with SCI, one needs a “need to know” and be formally “read in’ to the SAP after program nomination and approval.

A Public Trust position does not require a security clearance but does entail a suitability analysis (which focusses on character, conduct and reliability rather than access to classified information). While you will not have access to classified

information with such a position, you may have access to sensitive but unclassified information. Such positions can include public safety and health workers, federal police officers, and immigration, customs, border and port protection agents.

THE DOS AND DON'TS

How to Avoid "Negligence": You do not have to be a "spy" to face sanctions. Officers and employees are subject to penalties if they knowingly, willfully, or even *negligently* violate security protocols.

🚫 THE PROHIBITED ACTS (DON'T)

- **DON'T** disclose classified information to unauthorized persons.
- **DON'T** use personal devices or email to transmit or store classified information.
- **DON'T** remove classified information from official premises without specific authorization.
- **DON'T** assume prior clearance equals current access (access depends on “need to know” and program access – not past roles).
- **DON'T** improperly classify (or continue to classify) information in violation of the Executive Order (e.g., to conceal inefficiency or prevent embarrassment).

✅ THE ESSENTIALS (DO)

- **DO** ensure you have a "need-to-know" before accessing information, even if you are eligible.
- **DO** ensure that any person you share info with has both eligibility and a signed nondisclosure agreement.
- **DO** handle classified information on approved classified networks or devices and in only approved secure areas (such as SCIFs)
- **DO** only use authorized storage and transmission systems.
- **DO** make sure documents are properly marked with the right classifications including both portion markings and control markings (SCI, SAP, etc.)
- **DO** report spillage of classified information immediately to appropriate authorities.
- **DO** receive contemporaneous training on proper safeguarding.
- **DO** challenge improper access if there are unknown individuals in secure areas or requesting information without clear authorization

THE SANCTIONS

The Cost of Non-Compliance: If you are found to have unlawfully disclosed classified information, agencies can impose a wide range of administrative sanctions, including:

- **Reprimand**
- **Suspension without pay**
- **Removal (Termination of Employment)**
- **Revocation or suspension of security clearance**
- **Loss or denial of access to classified information**

CRIMINAL LIABILITY Beyond administrative penalties, mishandling classified information can involve criminal penalties under federal statutes, including the Espionage Act of 1917, 18 U.S.C. §§ 793, 794, and 798, which applies to cases involving both criminal intent (espionage) but also gross negligence. The Espionage Act is often invoked for leaks, mishandling of classified material or espionage. Section 793 also applies to "national defense information," which is broader than just "classified information."

18 U.S.C. § 1924 provides criminal penalties for a knowing disclosure of classified information by a federal employee or contractor.

YOUR RIGHTS

The Right to Challenge: If you are an authorized holder of information and have a good faith belief that it is improperly classified (or classified at the wrong level), you have the right to challenge the classification.

Protection from Retribution: Agencies are required to establish procedures to ensure that:

1. Individuals are **not subject to retribution** for raising a classification challenge.
2. Your challenge is reviewed by an **impartial official or panel**.
3. You are informed of your right to appeal decisions to the Interagency Security Classification Appeals Panel.

Right to Due Process: If an Agency suspends, denies or revokes your clearance, you do have limited due process rights within the Executive Branch, which can include written and/or oral responses as well as hearings in some cases. There is no right to

judicial review, however, and courts will usually dismiss security clearance cases for lack of jurisdiction as the Supreme Court has held that security clearance determinations are the province of the Executive Branch.

PROTECTING YOUR SECURITY CLEARANCE

Be Honest and Transparent:
Always provide accurate and complete information on your security clearance application. Any attempt to conceal or misrepresent information can lead to denial or revocation of your clearance. Lying about an issue is usually worse than the underlying issue (i.e. cover-up is worse than the crime).

Maintain Financial Responsibility:
Manage your finances responsibly and avoid excessive debt. Address any financial issues promptly and be proactive in resolving them.

Seek Help When Needed:
If you are struggling with substance abuse or mental health issues, seek professional help. Addressing these issues proactively can demonstrate your commitment to maintaining your security clearance.

Report Any Potential Security Concerns:
If you become aware of any potential security concerns, such as espionage or unauthorized disclosure of classified information, report them to the appropriate authorities immediately.

FACING A SECURITY CLEARANCE ISSUE?

If your clearance is being revoked, suspended, or investigated, you need experienced legal counsel. Solomon Law Firm represents federal employees and contractors in security clearance defense and disciplinary actions.

Contact Us Today: www.fedemploylaw.com | **202-980-2326**