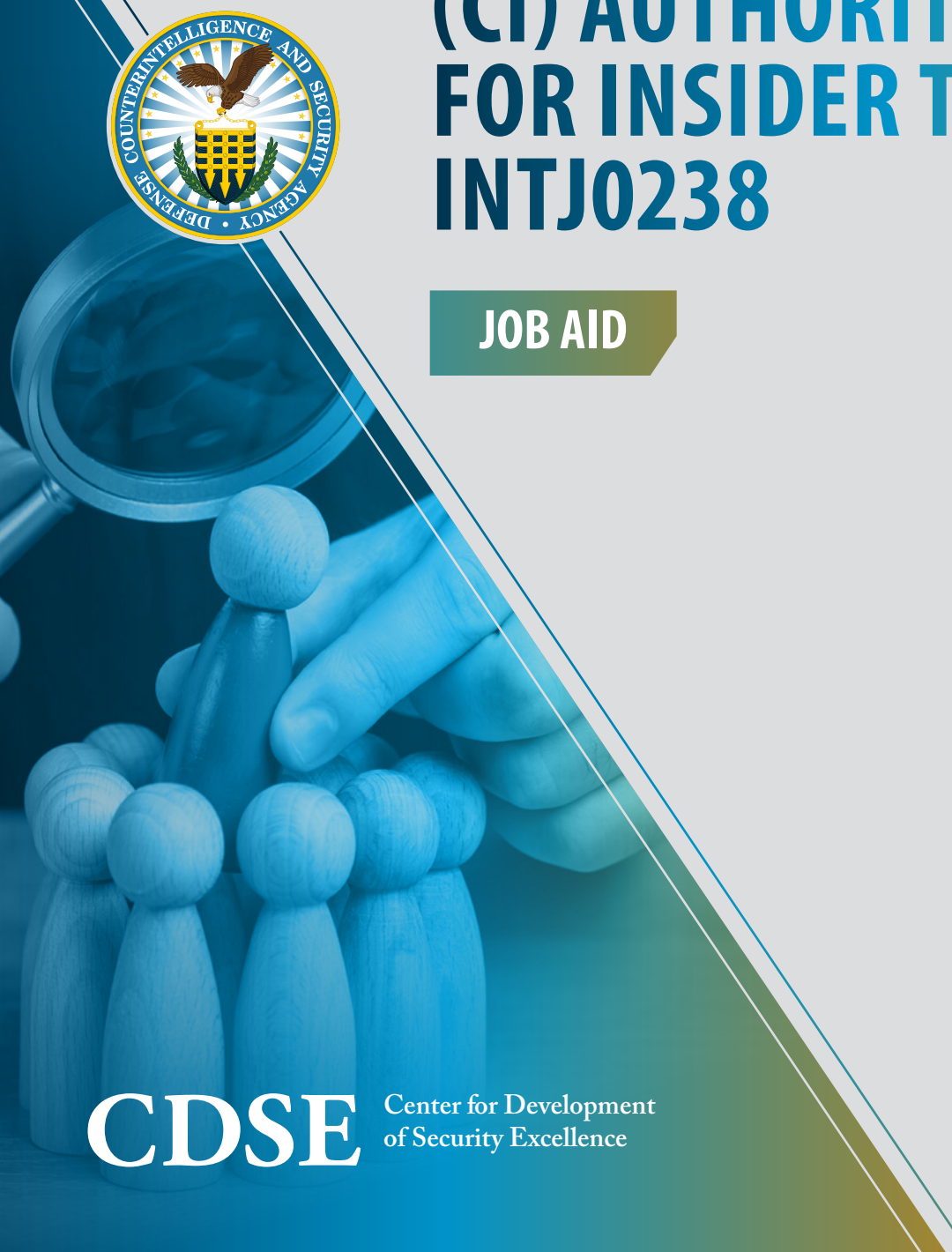
June
2024

COUNTERINTELLIGENCE (CI) AUTHORITIES FOR INSIDER THREAT INTJ0238

JOB AID



CDSE Center for Development of Security Excellence

NATIONAL POLICY

THE ESPIONAGE ACT OF 1917

- Established during World War I and utilized through the Cold War (Golden Age of Espionage) during an intense rivalry of the United States and the Soviet Union along with their respective allies. Today, The Espionage Act of 1917 provides a basis for 18 U.S. Code Chapter 37 – Espionage and Censorship and is more commonly used in Unauthorized Disclosure and Improper Storage criminal cases.

EXECUTIVE ORDER 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

- Executive Order (EO) 13587 was established on October 7, 2011, by President Barack Obama to implement an insider threat detection and prevention program consistent with guidance and standards developed by an Insider Threat Task Force.

- Requires an interagency Insider Threat Task Force (commonly referred to as the National Insider Threat Task Force (NITTF) to develop a Government-wide program (Insider Threat Program)) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, considering risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, other safeguarding capabilities and practices within agencies.

- The heads of agencies that operate or access classified computer networks shall be responsible for appropriately sharing and safeguarding classified information on computer networks.

- The task force is responsible for performing assessments of agency insider threat programs to ensure compliance with established policies and standards.

NATIONAL INSIDER THREAT POLICY PRESIDENTIAL MEMORANDUM 2012

- Published by the NITTF and promulgated to the Executive Branch of the Government via Presidential Memorandum by President Barack Obama. This policy leverages existing federal laws, authorities, policies, systems, and resources to counter the threat of insiders who may use their authorized access to compromise classified information.

- Integrated capability to monitor and audit information for insider threat detection and mitigation and was mandated for all relevant departments and agencies. This included: user

activity monitoring on classified networks, evaluation of personnel security information, employee awareness training and reporting responsibilities, gathering information for centralized analysis, and reporting and response.

- Development and implementation of information sharing policies and procedures so that insider threat programs access, share, and integrate information from throughout the department, including counterintelligence, security, information assurance, and human resources. Additionally, both the term "Insider" and "Insider Threat" were defined.

THE NATIONAL DEFENSE AUTHORIZATION ACT (NDAA) OF 2018

- Attempts to mitigate stove-piping information in Personnel Security Programs (PSP) by bringing these formerly disjointed personnel security efforts all under the umbrella of the Defense Counterintelligence and Security Agency (DCSA).
- Personnel Security Investigations were moved from the Office of Personnel Management (OPM) to the DCSA.
- The Department of Defense Adjudications and Vetting Services (AVS) will report to the Director of DCSA. These changes, along with the already in-existence DITMAC, will allow DCSA to provide end-to-end vetting processes for DOD and DOD associated personnel. Additionally, the DOD will utilize private sector data, such as credit scores and credit status, criminal records and drug screening, as well as private sector information to verify educational achievement and employment for background investigations. The NDAA also calls for a plan for expanding the continuous evaluation program to uncleared DOD insiders.

DOD POLICY

DEPARTMENT OF DEFENSE DIRECTIVE (DODD) 5240.06 COUNTERINTELLIGENCE AWARENESS AND REPORTING (CIAR)

- Was established May 17, 2011, to identify and report indicators of illicit foreign collection activity, cyber activities, espionage indicators, or other factors contributing to insider threat vulnerability.
- The directive applies to the entire DOD, not just to the components that can access classified networks. It also includes contractors, volunteers, and non-DOD entities that have authorized access to DOD resources.
- This directive also mandates that DOD insider threat programs will comply with all applicable laws and DOD policy issuances, including those regarding whistleblower, civil liberties, and privacy protections. Personally identifiable information (PII) and personal health information (PHI) will also be protected in accordance with DOD policy.
- Failure to safeguard PII and PHI can result in administrative penalties ranging from reprimand to removal from Government service. Additional criminal penalties include a $5,000 fine.

DEPARTMENT OF DEFENSE DIRECTIVE (DODD) 5205.16 - THE DOD INSIDER THREAT PROGRAM

- Indoctrinated September 30, 2014, and established the DOD Insider Threat Program. It applies EO 13587 and the National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs to the DOD. The directive requires the integration and synchronization of multiple programs across the DOD to identify, mitigate, and counter the insider threat.

DEPARTMENT OF DEFENSE INSTRUCTION (DODI) 5240.04 – COUNTERINTELLIGENCE (CI) INVESTIGATIONS

- Established April 1, 2016, and defines full-field CI investigations and preliminary CI investigations under the purview of the Under Secretary of Defense for Intelligence and Security (USD(I&S)).

DEPARTMENT OF DEFENSE INSTRUCTION (DODI) 5205.83 – DOD INSIDER THREAT MANAGEMENT ANALYSIS CENTER (DITMAC)

- Established March 30, 2017, and oversees the mitigation of insider threats within the department. DITMAC does this by integrating and centrally analyzing threat related information on the threat that insiders may pose to the DOD.

DEPARTMENT OF DEFENSE INSTRUCTION (DODI) 5240.22 – COUNTERINTELLIGENCE SUPPORT TO COUNTERTERRORISM AND FORCE PROTECTION

- Established October 12, 2022, and manages DOD participation in the Joint Terrorism Task Forces (JTTFs) and Force Protection detachments (FPDs).
- Oversees a DOD Global Watch capability—a collaboration between Defense criminal investigative organizations (DCIOs), Military Department CI organizations (MDCOs), the Pentagon FP Agency (PFPA), and the FBI—that coordinates, synchronizes, and de-conflicts inter-service or interagency information pertaining to criminal, terrorism, Force Protection (FP), and foreign intelligence entity threats and incidents with a DOD nexus.

ADDITIONAL RESOURCES

For additional Insider Threat and Counterintelligence resources, please visit our CDSE Toolkits.

Insider Threat Toolkit

Counterintelligence Toolkit