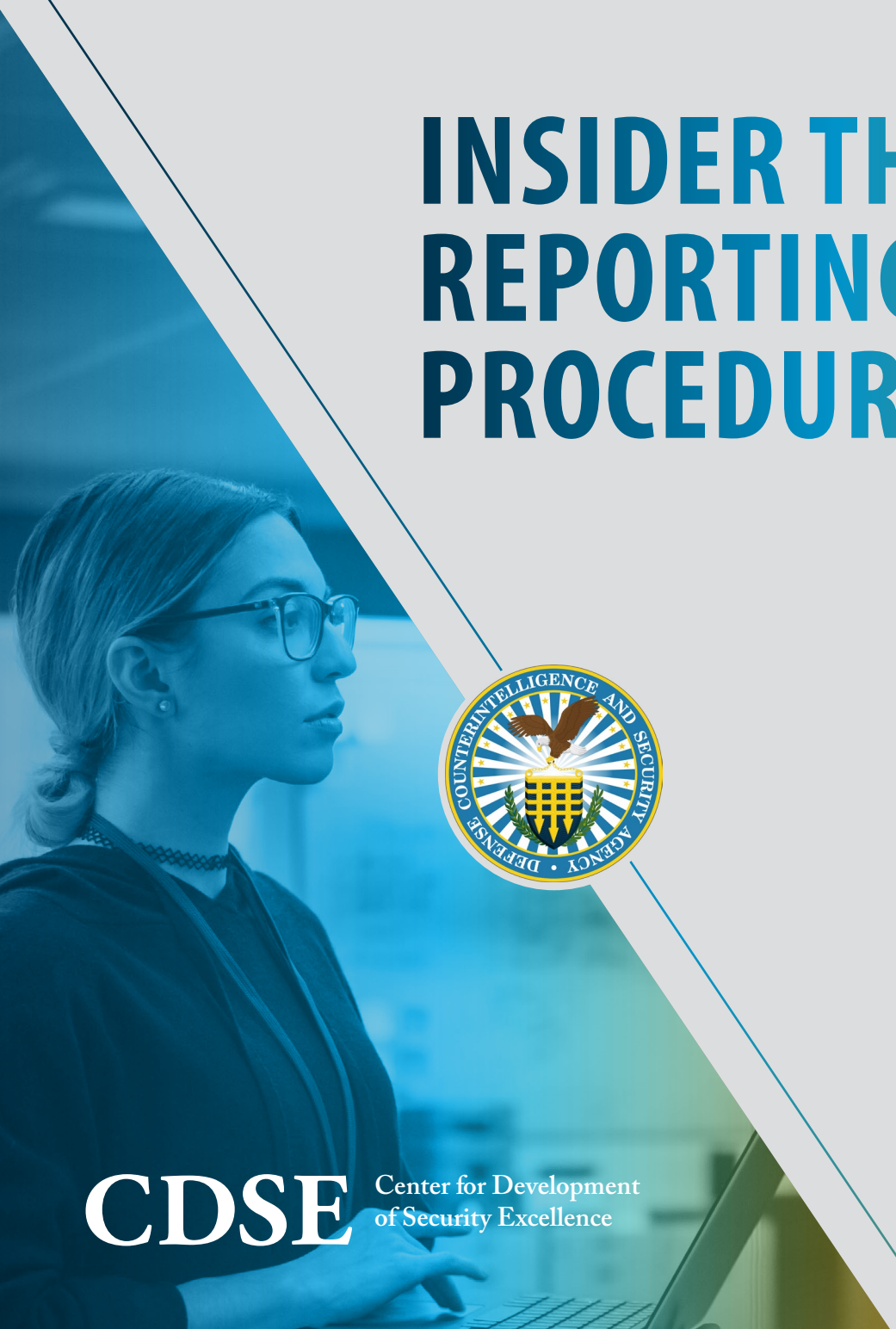
June
2023

INSIDER THREAT REPORTING PROCEDURES

JOB AID



CDSE Center for Development of Security Excellence

INTRODUCTION

This job aid provides the workforce with Insider Threat Reporting Procedures and highlights the necessary steps to take after identifying **potential risk indicators (PRI)**, concerning behavior, and/or potential threats. Historical reporting is associated with a negative stigma, but reporting can help reduce impacts from an insider threat. Some of these impacts include financial instability, resource degradation, national security concerns, reduced military strength and mission readiness, potential injury to persons, and loss of life. It is critical to report PRI and concerning behavior in a timely manner to deter and mitigate internal threats. This job aid will also provide references and resources to better understand insider threats.

DEPARTMENT OF DEFENSE (DOD) REPORTING PROCEDURES

After identifying PRI, concerning behavior, and/or potential threats, DOD government employees to include contractors, are mandated to report to their respective insider threat programs. Every insider threat program should take a multi-disciplinary approach to effectively deter, detect, and mitigate insider threats. This approach, in accordance with **DOD Directive DODD 5205.16**, includes working collaboratively with various subject matter experts to include law enforcement, counterintelligence (CI), mental health, security, civilian and military personnel management, legal, and cybersecurity personnel. Incidents meeting specific thresholds must be reported to the **Defense Insider Threat Management and Analysis Center (DITMAC)** and/or the Federal Bureau of Investigations (FBI) under **Section 811** of the **Intelligence Authorization Act of FY1995**. Additional reporting requirements (e.g., DOD Directive 5240.06, Counterintelligence Awareness and Reporting (CIAR), DODD 5205.16, Insider Threat Program 32 Code of Federal Regulations Part 117) under CI and security policies, must be adhered to regardless if an insider is involved.

CLEARED CONTRACTOR REPORTING PROCEDURES

Cleared industry personnel are mandated to report PRI, concerning behavior, and/or potential threats to their respective Insider Threat Program Senior Official (ITPSO) or Facility Security Officer (FSO). The ITPSO or FSO will then report threats to the Defense Counterintelligence and Security Agency (DCSA) Industrial Security Representative and/or DCSA CI special agent for incidents meeting specific thresholds. If the thresholds include known or suspected espionage, the ITPSO or FSO will report directly to the FBI.

Information related to the National Security Adjudicative Guidelines must also be reported per 32 Code of Federal Regulations Part 117 (i.e., The National Industrial Security Program Operating Manual (NISPOM) Rule.) Employees are also required to report suspicious contacts and other reportable behaviors in accordance with 32 Code of Federal Regulations Part 117, NISPOM.

FEDERAL AGENCY REPORTING PROCEDURES

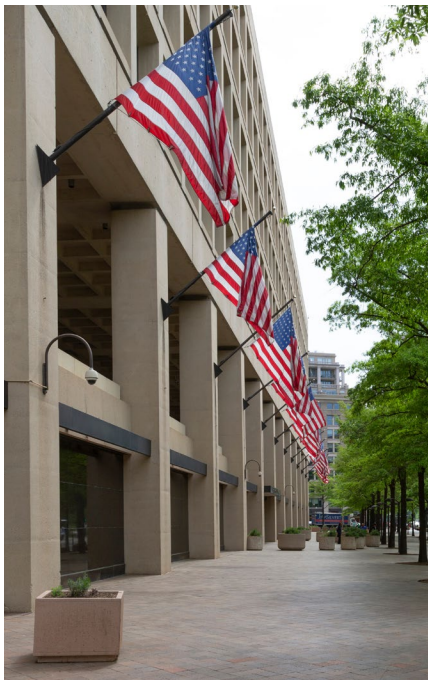
Federal civilian employees must report to their agency's Insider Threat Program, security office, or their supervisor. Federal agency reporting procedures vary based on the agency specific procedures. Incidents meeting specific thresholds must also be reported to the FBI under Section 811 of the Intelligence Authorization Act of FY1995. Cleared employees are required to report potential threats. Failure to report potential threats may result in the following:

Consequences for DOD employees* may include:

- Punitive action under Article 92, Uniform Code of Military Justice for employees subject to UCMJ
- Disciplinary action for civilian employees

Consequences for cleared contractor employees may include:

- Loss of employment
- Loss of security clearance
- Criminal charge



** Per DoDD 5205.16, Insider Threat Program; DoD 5220-22-M, National Industrial Security Program Operating Manual; and DoDD 240.06, Counterintelligence Awareness and Reporting (CIAR)*

DEFINITIONS

DOD Insider Threat Management and Analysis Center (DITMAC)

A cross-functional team of analysts that aggregate, integrate, review, analyze, and share information that indicate a potential insider threat. The DITMAC will exercise this information management capability with the ability to assess risk; refer issues for further consideration, investigation, and potential action; synchronize responses; and oversee resolution of identified issues across the Department within DoD-approved resources.

EO 13587

Any person with authorized access to any United States government resource to include personnel, facilities, information, equipment, networks, or systems.

Insider

DOD Directive (DODD) 5205.16 Insider Threat Programs: Any person with authorized access to DOD resources by virtue of employment, volunteer activities, or contractual relationship with DOD.

32 Code of Federal Regulation Part 117, NISPOM: Cleared contractor personnel with authorized access to any USG or contractor resource, including personnel, facilities, information, equipment, networks, and systems

EO 13587 National Insider Threat Policy and the Minimum Standards: Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.

Section 811 Referral

Section 811 of the Intelligence Authorization Act of 1995 (50 USC §402a) is the legislative act that governs the coordination of counterespionage investigations between executive branch (EB) agencies and departments and the FBI. Section 811 referrals are the reports – made by EB agencies or departments to the FBI under Section 811(c)(1)(a) – that advise the FBI of any information, regardless of origin, which may indicate that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or agent of a foreign power

RESOURCES

Counterintelligence Awareness and Reporting

Developing a Multidisciplinary Insider Threat Capability INT201.16

Counterintelligence Awareness and Reporting for DOD CI116.16

A Glossary of Basic Insider Threat Definitions

Insider Threat Potential Risk Indicators (PRI)

Insider Threat Program (ITP) for Industry

REFERENCES

DOD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended

DoDD 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, Incorporating Change 3 on August 31, 2020 (whs.mil)

32 Code of Federal Regulation Part 117, NISPOM

32 CFR Part 117 NISPOM Rule

Reporting concerning behaviors and risk indicators allows insider threat programs to take proactive measures that will hopefully lead to positive outcomes for individuals and mitigate risk for organizations.

 # Supporting Through Reporting