FEBRUARY 2025

INSIDER THREAT INQUIRY

JOB AID

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

CDSE Center for Development of Security Excellence

INSIDER THREAT INQUIRY

After an Insider Threat Program receives a case referral, analysts will conduct a preliminary review or triage the case referral to determine the accuracy of information and the urgency level for a threat assessment. By identifying protentional risk indicators and thresholds, insider threat analysts will determine if there are gaps in information and will send out various requests for information or make inquiries to various sources. Inquiries may be made to multiple resources within the organization as well as external sources. Once the results of the inquiries are received, the insider threat team can thoroughly make a complete threat assessment and move toward the case mitigation process.

INQUIRY VS. INVESTIGATION

An inquiry is a request for information that examines facts, principles, or research. It can also be defined as a systematic investigation, often of a matter of public interest. The difference between an inquiry and investigation is the level of formality and purpose for the information gathering. It is important to understand that Insider Threat Programs inherently do not have investigative authority. However, Insider Threat Programs may coordinate with other entities that have investigative authority for information gathering or refer a case to an entity that has appropriate investigative authority.

GUIDANCE AND STANDARDS

Executive Order 13587 implements an insider threat detection and prevention program that consists of guidance and standards that require Insider Threat Programs comply with appropriate legal and constitutional requirements. They must also ensure that privacy rights, civil liberties, and whistleblower protections are adhered to while conducting operations. The National Insider Threat Policy outlines general responsibilities of departments and agencies for analysis, reporting, and response. This policy allows gathering and integrating available information to conduct a preliminary review of potential insider threat issues and, where it appears a potential threat may exist, referring the matter as appropriate to counterintelligence, security, information assurance, the Office of Inspector General, or to the proper law enforcement authority.

TYPES OF SECURITY INVESTIGATIONS

The most common security investigations are pre-employment background investigations, federal background investigations, periodic investigations, Personnel Security Investigations (PSI), Single Scope Background Investigations (SSBI), security clearance investigations, Continuous Evaluation (CE), National Agency Check (NAC), and National Agency Check and Inquiries (NACI). Security investigations typically involve applications, public records, interviews, incident reports, employment history, military records, criminal offenses, credit history, and/or debt delinquency. They may also include an investigator's analysis in determining if the individual is reliable, trustworthy, has sound judgement, and may include character traits. Insider Threat Programs adopt an evidence-based structured approach to threat assessments rather than a biased approach. If documented, access to these investigations may identify an accumulation of indicators through time and may suggest a pattern of activity that warrants further inquiry or action.

FOR MORE INFORMATION:

Federal Background Investigations Support to Insider Threat Job Aid

https://www.cdse.edu/Portals/124/Documents/jobaids/insider/BI-INT-Job-Aid.pdf

Course Resources for Preserving Investigative and Operational Viability in Insider Threat INT220.16

https://www.cdse.edu/Training/eLearning/INT220-resources/

CDSE Center for Development of Security Excellence

LEARN. PERFORM. PROTECT.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

INSIDER THREAT INQUIRY