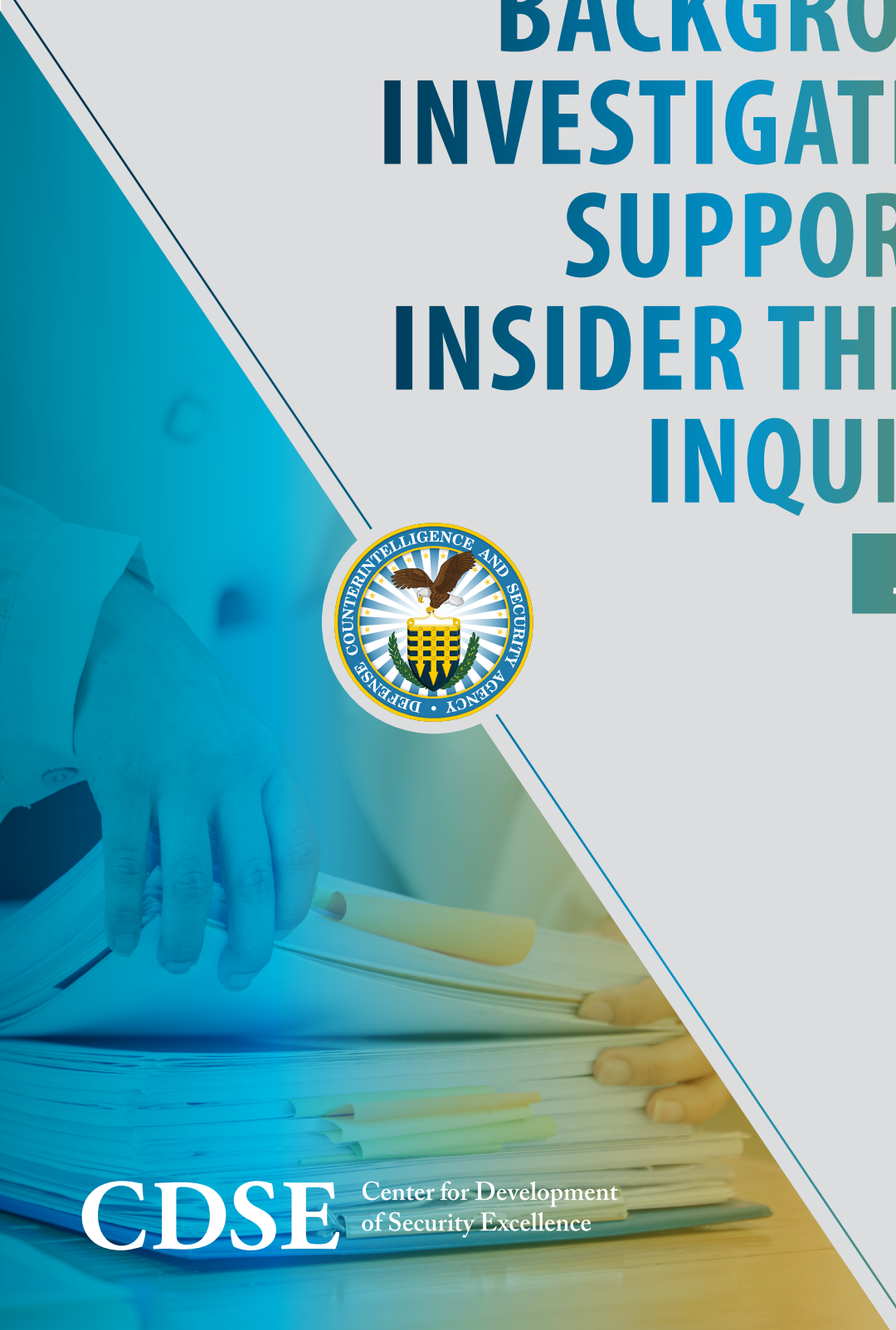
May
2024

FEDERAL BACKGROUND INVESTIGATIONS SUPPORT TO INSIDER THREAT INQUIRIES

JOB AID



CDSE Center for Development of Security Excellence

The purpose of this job aid is to demonstrate the linkage between federal background investigations and insider threat programs. Insider threat programs conduct inquiries to deter, detect, and mitigate actions by employees who may pose a risk of becoming a threat to national security. Inquiries may benefit from information obtained from a federal background investigation. Inquiries may also benefit from incorporating threat-specific interrogatories.

What Are Federal Background Investigations?

Federal background investigations are the first step in the personnel vetting process. The results of these investigations influence determinations on suitability for government employment, fitness to perform work under a government contract, eligibility to serve in a national security sensitive position, acceptance or retention in the armed forces, eligibility for access to classified information, and/or eligibility for logistical or physical access to a federally controlled facility or information technology systems.

During a background investigation, information is gathered through various methods to provide a holistic picture of the applicant so an adjudicator can grant or deny the applicant's eligibility to occupy national security sensitive positions, access to classified information, suitability for civilian employment, fitness for selected positions, and/or credentials for access to DOD systems and facilities.

Investigative methods can include in-depth interviews with the applicant and individuals such as the applicant's current and former supervisors and co-workers, neighbors, and friends, as well as reviewing employment records, law enforcement and court actions, alcohol and drug counseling records, and financial records. These investigative methods are used to verify and develop information regarding the applicant's character, conduct, trustworthiness, integrity, and loyalty to the United States.

Insider Threat Detection

Insiders with eligibility for access to classified information or physical access to facilities and information technology systems may commit espionage, unauthorized disclosure, or violent acts. To prevent this, insider threat programs must conduct and analyze all available information in an unbiased manner to fully understand whether reported behaviors and actions warrant further investigation or referral. This action or "inquiry" is essential for detection. Detection is most effective when insider threat programs utilize a multi-disciplinary approach.

Inquiries analyze information gathered from previously obtained employee consent or agency authority to share governmental or publicly available information. This might include law enforcement investigations, personnel security investigations, and histories of adjudicative action. This may also include conducting interviews with complainants, voluntary witnesses, management, and voluntary subject employee interviews. Interviews must be approved by the Insider Threat Program Senior Official and Program Manager after consulting with the general counsel and appropriate investigative authorities.

If an interview is an approved course of action for the inquiry, then there are interrogatories that could be considered for a deeper understanding of the behavior in question.

INTERROGATORIES FOR POTENTIAL RISK INDICATORS

Each scenario below presents an insider as a subject with potential risk indicators (PRIs) or reportable behaviors. Some indicators align with the national security adjudicative guidelines. These behaviors are considered problematic for individuals who require national security eligibility, access to classified information, or access to facilities and/or information technology. Consider the series of questions associated with each scenario to help clarify if a subject poses any risk.

SCENARIO: Access Attributes

While having administrator privileges, subject transmitted classified information to unauthorized individuals.

QUESTIONS

- Can you provide your account of the events leading to the transmission of classified information to an unauthorized person?
- What motivated or compelled you to transmit this information despite knowing it was classified and unauthorized for release?
- Were you aware of the legal and ethical implications of transmitting classified information to unauthorized individuals?
- Did you receive any training or guidance regarding the handling and dissemination of classified information prior to this incident?
- Can you explain any external pressures or influences that may have influenced your decision to transmit the classified information?

SCENARIO: Violent Extremist Mobilization/ Allegiance to the U.S. (Guideline A)

Subject was a self-professed Jihadist who expressed their desire to kill various groups of Americans.

QUESTIONS

- What led to these feelings or thoughts?
- Have you discussed these thoughts or feelings with anyone else either online or in person?
- Do you have any immediate plans or intentions to act on these desires, and if so, can you provide details?
- Are there any underlying issues or challenges in your life that may be contributing to these thoughts or feelings?

SCENARIO: Foreign Considerations (Guidelines B & C)

Subject's mother was born in a heightened risk country (HRC). Subject developed an interest in this HRC, in part, due to their mother's heritage. From 1995 to 2010, subject made many trips to this HRC. In 1997, they met and married their spouse in the country. After graduating from college in 1997, subject lived and worked in the HRC until they joined the U.S. Army in 1998.

QUESTIONS

- Please verify your mother's current citizenship.
- Has your mother ever been employed by a foreign government, agency, department, or military?
- How often does your mother visit her native country?
- Do you have any relatives, friends, or associates residing in the country?
- Is there any person, group, or organization in a foreign country to which you owe a duty, obligation, or responsibility that you would be expected to honor or perform if you were asked to do so?
- As a citizen of the United States, do you or have you ever possessed or used a passport or travel identity card from a country other than the U.S.?
- Do you currently have a passport or travel identity card from a country other than the U.S.?
- Please confirm your spouse's current citizenship.
- How did you meet your spouse?
- Have any of your spouse's relatives ever been employed by a foreign government, agency, department, or military?
- Who did you visit during your trips to the country? Where do you stay during your visits? What types of activities did you do while there?
- Tell me about your time living in the country. Where did you reside? Who was your employer?
- On any of your trips to or while residing in this country, were you ever contacted by a foreign government, foreign business, foreign organization, foreign group, or foreign person that asked you for information or help in any matter?
- On any of your trips to or while residing in this country, were you ever arrested, charged, held, or taken into custody for any reason?
- On any of your trips to or while residing in this country, were you ever questioned, interviewed, or interrogated by any foreign government employee or official?
- Have you ever had contact with anyone representing a non-U.S. intelligence/security service?

SCENARIO: Criminal/Violent Conduct (Guidelines D & J)

Subject established a terrorist militia group. The group possessed illegal firearms, M4s, and the binary explosive Tannerite.

QUESTIONS

- Can you provide insights into the ideology and beliefs of the militia group you are affiliated with?
- What motivated you to establish this militia group?
- What roles or activities are you involved in within the group?
- How does the group recruit new members, and what criteria do they look for?
- Have you participated in any violent or illegal activities on behalf of the group?
- What are your thoughts on the use of violence to achieve the group's objectives?
- Do you have concerns about the potential consequences of the group's actions on innocent civilians or society as a whole?

SCENARIO: Financial Considerations (Guideline F)

Subject made materially false and misleading statements on National Institute of Health (NIH) grant applications, fraudulently obtaining approximately $4.1 million in grants from the NIH.

QUESTIONS

- Explain the inconsistencies between the information provided on your application and what was found during the investigation.
- What was your motivation behind providing false information on your application?
- Was it your intent to defraud the federal government?
- Are there any other instances in which you've provided misleading information on an application or to authorities?

SCENARIO: Professional Performance (Guideline E)

Subject is ineligible for rehire at a previous employer.

QUESTIONS

- Can you provide some context regarding your departure from your previous employer?
- Were you aware of any issues or concerns raised by your previous employer that may have led to your ineligibility for rehire?
- Did you have any personality conflicts with anyone?
- What steps, if any, have you taken to address or rectify the circumstances that resulted in your ineligibility for rehire?

SCENARIO: Substance Abuse (Guidelines G & H)

Subject was arrested for public intoxication.

QUESTIONS

- Can you provide your account of the events that led to your arrest?
- Were there any circumstances or factors that contributed to your decision to consume alcohol to the point of intoxication in a public setting?
- How do you believe your behavior during this incident reflects on your professionalism and suitability?
- Have you previously received any training or guidance regarding responsible alcohol consumption and behavior outside of work hours?
- Do you believe this incident will affect your ability to fulfill your job responsibilities effectively?
- What steps do you plan to take to address any personal issues or concerns that may have contributed to your public intoxication?

SCENARIO: Security/Compliance Incidents (Guideline K)

While deployed in Azerbaijan, subject was investigated for a security violation and removed from their command.

QUESTIONS

- Tell me about the incident that led to the security violation investigation.
- What actions did you take leading up to and during the incident in question?
- Had you previously received training or guidance regarding security protocols and policies?
- Are you aware of any potential impacts or consequences resulting from the security violation?
- Did you knowingly violate security policies?

SCENARIO: Technical Activity (Guideline M)

While working as an intern, subject obtained a co-worker's username and password from their supervisor's master account roster. They used the information to access a co-worker's account and view their project files.

QUESTIONS

- What prompted you to access your co-worker's records?
- Did you access anyone else's records?
- Did you share your co-worker's grades or any other information with anyone?
- Did you share the username and password of any other co-workers with anyone?
- Were you aware that accessing these records without authorization violates company policies and potentially legal regulations?
- What actions did you take after accessing the records?

ADDITIONAL RESOURCES

Adjudicator Toolkit

An Insider's Digital Footprint and Associated Risk Job Aid

Case Study Library

Insider Threat Indicators in User Activity Monitoring Job Aid

Insider Threat Potential Risk Indicators Job Aid

Insider Threat Potential Risk Indicators: Active Shooters and the Pathway to Violence Job Aid

Potential Risk in Informal Banking and Finance Job Aid

Security Executive Agent Directive 3 Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position

Security Executive Agent Directive 4 National Security Adjudicative Guidelines

NOTE: If the URLs in this document do not open upon clicking, right-click on the hyperlinked text, copy link location, and paste into a browser. Alternatively, you can open the PDF in a browser.