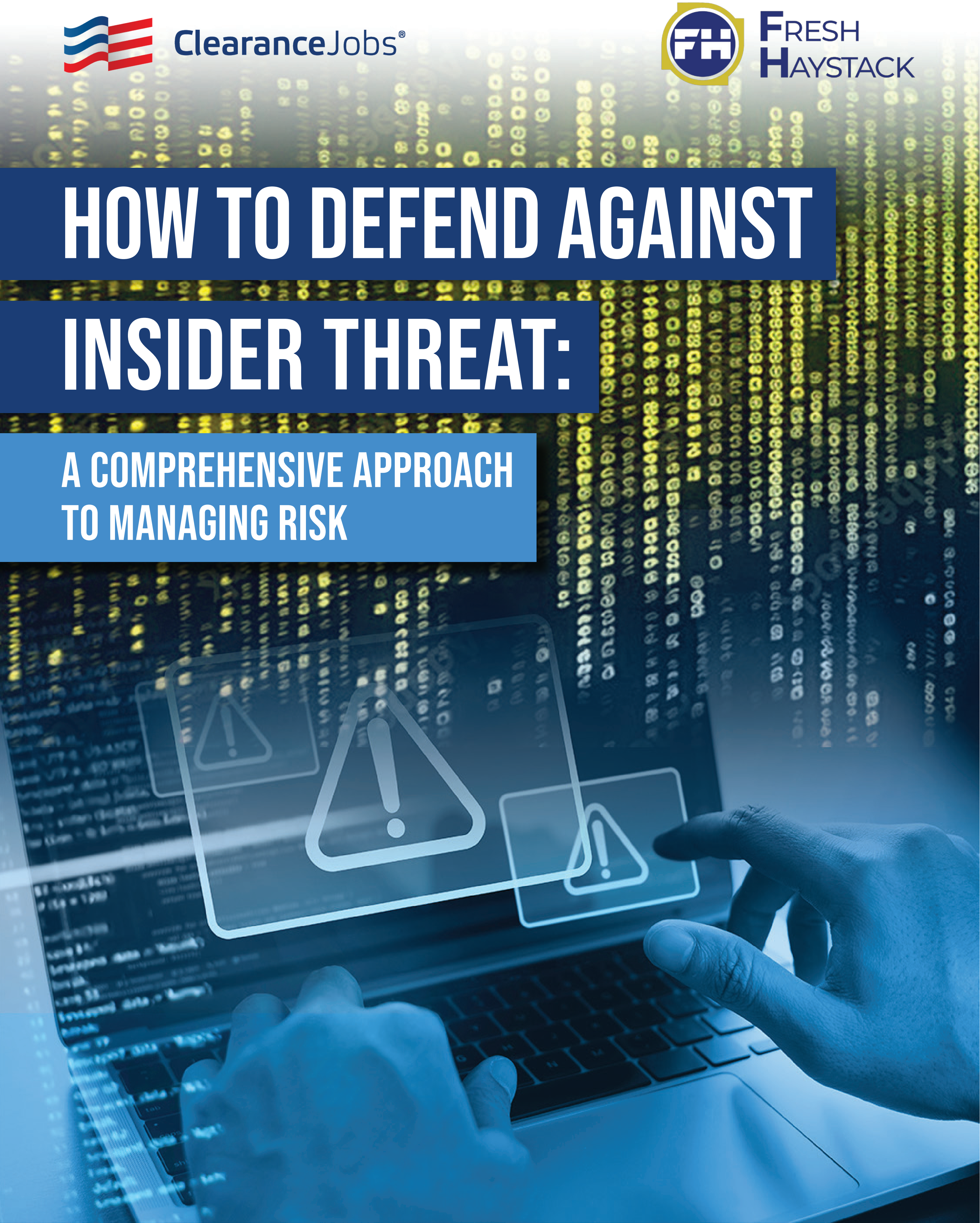
ClearanceJobs®

FRESH HAYSTACK

HOW TO DEFEND AGAINST INSIDER THREAT:

A COMPREHENSIVE APPROACH TO MANAGING RISK



“TRUST BUT VERIFY”

Insider threat and insider risk are critical issues for any company looking to do business with the federal government or stay in business and protect their bottom line. Insider risk is not a new phenomenon, but the past several years have ushered in new risks for companies, agencies, and organizations navigating the world of remote work and hybrid office structures, along with heightened employee stress.

Dr. Eric Lang, director of the DoD Personnel and Security Research Center, or PERSEREC noted 62% of individuals don’t follow security protocols as closely at home as they do in the office, and among insider threat criminal prosecutions, 75% involve remote workers. A key factor is simply the nature of doing work away from the office, and the ease in printing or otherwise misusing proprietary or confidential information.

And because insider threats and risks aren’t just about the malicious actors – but the non-malicious actors – remote work opens up the ‘sloppy’ security practices that can increase risk for companies.

INSIDER THREAT

***The potential for an individual who has or had authorized access to an organization’s critical assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization*.**

- Carnegie Mellon University Software Engineering Institute’s the CERT Definition of ‘Insider Threat’

THE “RULE OF THREE” FOR INSIDER THREATS

1 THREAT TYPES

- Careless User
- Malicious User
- Compromised Credentials

2 THREAT ACTIVITIES

- Fraud
- Data Theft
- System Sabotage

3 MITIGATION GOALS

- Deter
- Detect
- Disrupt

Source: Gartner

INSIDER THREAT TIMELINE

June 2010

Army Specialist Manning leaks classified documents to WikiLeaks.

May 2013

NSA contractor Edward Snowden committed one of the most significant leaks of US Classified National Security Information (CNSI), and then flees to Hong Kong.

Response: Executive Order (EO) 13587 signed in Nov. 2011 by then-President Barack Obama and includes a response to the WikiLeaks Unauthorized Disclosures (UD). Part of the EO was the establishment of the National Insider Threat Task Force (NITTF), which subsequently developed insider threat minimum standards for all Executive Branch programs.

Semptember 2013

Aaron Alexis, a contractor supporting the US Navy, opens fire at the Washington Navy Yard, killing 12 and wounding several others.

April 2014

Army Specialist Ivan Lopez kills four soldiers (including himself) and injures a number of others at Fort Hood (newly renamed Fort Cavazos). In 2009, Army Major Nidal Hasan killed 13 and injured many more in a shooting incident.

May 2016

NISPOM Conforming Change 2 goes into effect, creating requirements across the defense industrial base and addressing insider risk within an organization.

March 2018

The Office of the Director of National Intelligence's National Counterintelligence and Security Center announces the Trusted Workforce 2.0 initiative. It overhauls and improves the security clearance process and updates the policy framework that's been in place since the 1950s.

Response: DoD establishes the DOD Insider Threat Management and Analysis Center (DITMAC) to coordinate information across DOD component hubs and maintain a repository of insider threat-related data. DoD also initiated continuous evaluation efforts.

Response: In 2017, the final report on the 2009 Fort Hood Shooting incident identifies the need to implement Prevention, Assistance, and Response (PAR) capabilities at installations. PAR coordinators would bring together existing functional experts on the installation to identify and assess risk-based activities. This leads to the 2017 National Defense Authorization Act (NDAA) expansion of "covered personnel" to include not just cleared personnel but all personnel with access to DoD resources (personnel, information, facilities, etc.).

January 2021

The unlawful penetration of the Capitol building in Washington, DC results in multiple arrests of current and former military members. These actions are viewed as extremism and result in a review within numerous government entities, including the DoD.

April 2023

Air National Guard Airman First Class Jack Teixeira was arrested for a significant unauthorized disclosure of CNSI. There remains an ongoing investigation into the incident, which coincides with another DoD 45-day review on procedures related to personnel security, information security, physical security, and security training.

Response: As result of the DoD's Counter Extremism Activities Working Group (CEAWG), resources were devoted to centralize capabilities under the DITMAC to help improve the posture of the DoD insider threat programs.

NINE THINGS DEFENSE CONTRACTORS ARE REQUIRED TO DO TO CONFORM TO THE NISPOM:

National Industrial Security Program - Operating Manual

1. Appoint from within the contracting organization the "Insider Threat Program Senior Official" (ITPSO).

2. Ensure the contracting organization has the capability to gather, store, and analyze relevant insider threat information. Evolve processes and procedures to ensure the ITPSO has broad access to this information. This includes access to human resource, security, information assurance, legal, etc). Smaller entities may find this easier to implement than larger entities, as larger entities tend to silo information. The ITPSO will require cross-entity access.

3. Report relevant information covered by the "13 personnel security adjudicative guidelines that may be indicative of a potential or actual insider threat."

4. Ensure DCSA is aware, "through self-certification, that a written program plan is implemented and current." DCSA wishes to ensure that the role of the ITPSO is not simply a figurehead who is trotted-out during each DSS inspection, and thus articulates with a bit of granularity the role of the ITPSO in their ISL 2016-2.
    - ITPSO will be a US citizen employee and a senior official of the company.
    - ITPSO will hold a clearance associated with the Facility Clearance (FCL) and is the responsible individual with respect to the company's insider threat program.
    - The need for the individual to be a senior official is explained, as the individual must have the "authority to provide management, accountability and oversight to effectively implement and manage the requirements of the NISPOM related to insider threat."
    - The FSO (if senior within the company) may be the ITPSO, if not, then the FSO will be an integral member of the implementation program.
    - Larger organizations may appoint a single ITPSO for the corporate-wide program.

5. Annual insider threat self-inspections will be certified as having been conducted to DCSA. These self-inspection reports will be available to DCSA.

6. Contractor entities must have a system and process in place to identify patterns of negligence or carelessness in handling classified materials.

7. Insider Threat Training must be provided to employees whose duties place them within the insider threat program management.

8. All cleared employees are required to receive training on insider threats. Currently employees must receive the training within 12 months, new employees prior to accessing classified materials. This training must be documented, and annual refresher training implemented.

9. Information systems must implement DCSA-provided information system security controls on classified information systems in order to detect activity indicative of insider threat behavior.

FRESH HAYSTACK

ADDRESSING THE INSIDER RISK, WITH INSIDER THREAT DEFENSE

Creating an Insider Threat Program – Adjusting to NISPOM Change 2

Many organizations today are struggling with enterprise-wide risk visibility, including Insider Threat Defense (ITD). As insider threat programs evolve, it’s critical for companies to go beyond the basics and ensure information protection that scales. The human factor creates a hefty risk profile, with a high price. Fortunately for security professionals, there are new technologies to arm companies with the ITD they need to succeed

Gartner

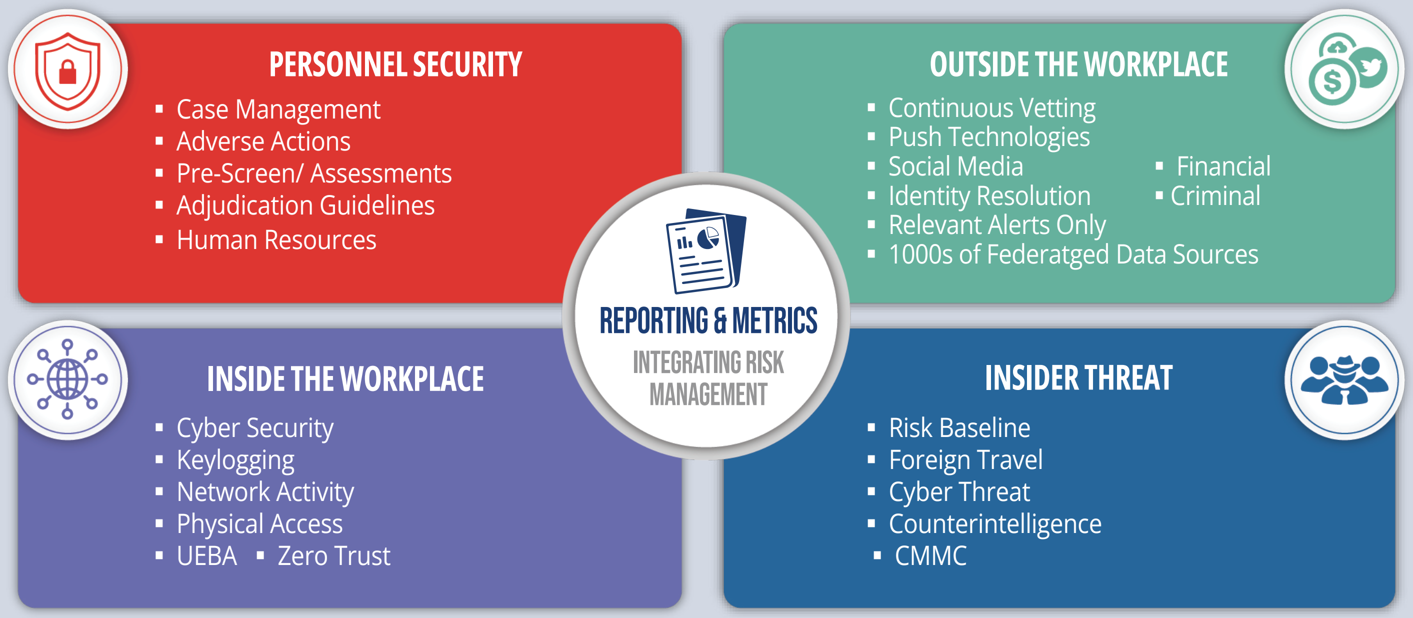
Recognized for **Insider Risk Management**

Fresh Haystack platform by CANDA Solutions, LLC was recognized in the 2022 Gartner® “Market Guide for Insider Risk Management Solutions. ” by Jonathan Care, Paul Furtado, Brent Predovich, April 18, 2022 (*reprint link*) as well as in UEBA (User Entity Behavioral Analytics) Employee Monitoring, 2019.

SOLUTION SPOTLIGHT: INSIDER THREAT DEFENSE WITH WITH FRESH HAYSTACK BY CANDA SOLUTIONS

Successful insider threat risk mitigation requires a holistic approach that breaks silos. Effective insider risk detection requires creating a context for Cyber Security, Financial, Criminal, Foreign Influence, Identity Resolution, Behavioral Risks, Human Factor, Dark Web, Open Source and Social Media analysis. Our system provides notifications/escalations on the facilities, contracts, and associated workforce and 3rd party under risk evaluation. Our solution truly addresses continuous, multi-factor situational risk awareness across the entire enterprise, along with suspicious and reportable activities of selected individuals outside of the workplace in a way that is transparent and protects privacy rights. The ITD module is based on the enterprise’s ability to create a risk baseline based on a variety of data sources across critical programs, personnel, and facilities.

Detection of potentially malicious behavior involves authorized insider threat personnel gathering information from many sources and analyzing that information for clues or concerning behavior. A single indicator may say little. However, if taken together with other indicators, a pattern of concerning behavior may arise that can add up to someone who could pose a threat. It is important to consider relevant information from multiple sources, sort out false positives, to determine if an employee’s behavior deserves closer scrutiny or the individual has no malicious intent and simply needs help. And that is where a successful ITD solution comes in.



PERSONNEL SECURITY

- Case Management
- Adverse Actions
- Pre-Screen/ Assessments
- Adjudication Guidelines
- Human Resources

OUTSIDE THE WORKPLACE

- Continuous Vetting
- Push Technologies
- Social Media
- Identity Resolution
- Relevant Alerts Only
- 1000s of Federatged Data Sources
- Financial
- Criminal

REPORTING & METRICS

INTEGRATING RISK MANAGEMENT

INSIDE THE WORKPLACE

- Cyber Security
- Keylogging
- Network Activity
- Physical Access
- UEBA
- Zero Trust

INSIDER THREAT

- Risk Baseline
- Foreign Travel
- Cyber Threat
- Counterintelligence
- CMMC

THIS APPROACH COMBINES:

» Activities within the Enterprise (Insider Threat actions)

» Activities outside the Enterprise using push technology (true CV) based on configurable risk indicators

» A state-of-the-art case management system view of workforce personnel data

ALL IN ORDER TO PROACTIVELY IDENTIFY AND MITIGATE THE THREATS BEFORE THEY FULLY MATURE.

ANALYTICS & TRUST (OR RISK) SCORE

The Defense Industrial Base (DIB) has been challenged to "Deliver Uncompromised," ensuring greater Counterintelligence and security across their enterprise. Organizations supporting the national security mission must protect critical information and technology from being wittingly or unwittingly lost, stolen, denied, or degraded. Risk assessment has to include ITD, containing set of technical and non-technical process countermeasures to monitor compliance with organization policies and deviations from expected role-based behaviors. Countermeasures inform and defend against workplace behaviors (deliberate or accidental) that may adversely affect business operations. Organizational goals, policies, rules, and legal requirements are destructed to help define triggers that will alert on network activities in violation of business rules and objectives. Triggers are a hybrid of previously-developed, proven triggers – tested in real-world engagements – and custom triggers that can focus on specific high-risk personnel / assets / technology and known tactics, techniques, and practices of illegal activities (e.g., inside traders, fraud, data theft, espionage).

Sensors collect data and alert activity based on trigger definitions and scripts. All relevant data is aggregated from both audit and non-audit sources (e.g., financial, or criminal reporting, foreign travel, social media, dark web, OSINT, etc.) and once an alert occurs, the Fresh Haystack workflow and case management tool guides a repeatable, preconfigured response plan showing the custody, control, transfer, analysis, and disposition of the alert. Our tool triages the alert via a Risk Score to establish priority of effort. Alerts are analyzed against expected role behaviors and other disparate data sources (i.e., HR and Personnel Security records, financial background, criminal, etc.) to determine disposition of the alert.

Data sources can be configured based on the user role in the organization, position sensitivity, location, or other situational knowledge. The Fresh Haystack proprietary AI (Artificial Intelligence) RIDE (Risk Integration & Decision Engine) uses a variety of structured analytic models and methodologies to recognize patterns, regressions, and clustering from disparate data sources (i.e., HR records, financial backgrounds, social media presence, current 'workload', known associates, legal records, non-work-related travel, etc.) to build contextual evidence around the observed anomaly. As a Convolutional Neural Network, RIDE processes additional data/decisions quickly with scalable results as the adoption of the program deepens and requirements or policy change.

If an alert is a false positive or mitigatable, the alert is dropped, and the profile is updated. If the alert activity cannot be explained, the analyst can recommend escalation, quality review, or investigation. Once an alert is escalated, the appropriate investigative authority is integrated as the lead to adjudicate the incident. The Fresh Haystack tool assists in providing a managed escalation process to ensure accountability, traceability, and adherence to chain of custody rules. Many of these activities can be automated or set to require manual review; it is a workflow and policy-based implementation decision that may differ across workgroups, programs, or location.

INSIDER THREAT GLOSSARY:

Behavioral Indicators: Any observable behavior or action by an individual that may signal malicious intent. For example, taking classified material home or on trips.

Insider: Any person with authorized access to an organization's resources to include personnel, facilities, information, equipment, networks, or systems.

Insider Threat: The threat that an insider will use his or her authorized access wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of department resources or capabilities.

Leaks: The intentional, unauthorized disclosure of classified or sensitive information to a person or an organization that does not have a "need to know."

Privileged Access: A category of access that grants an individual privileged user duties to perform elevated functions on a network, system, or application that general users are not authorized to perform. This includes, but is not limited to, individuals who have been granted rights and access to networks, hardware, software, information, or sensitive technical spaces beyond those of the general user population or have the ability to influence others who interact with information systems.

National Counterintelligence and Security Center

ClearanceJobs®

A MODERN MARKETPLACE FOR CAREER OPPORTUNITIES IN NATIONAL SECURITY

ClearanceJobs is your all-in-one recruiting solution. Much like a CRM, our unique system lets you target top candidate leads, converting cool passives to active candidates ready to make a move—to your company.

END-TO-END CLEARED HIRING SOLUTIONS

RECRUITMENT SOLUTION

- Search, directly engage, and easily work cleared candidates through a pipeline.
- Convert passives to active potential hires.

CAREER EVENTS

- Reduce your cost per hire with real-time conversations.
- Choose from in-person or virtual, public or private events.

SOURCING SERVICES

- Save time and free up bandwidth while we fill your pipeline.
- All that's left for you to do is interview and hire.

EMPLOYER BRANDING

- Increase brand awareness to gain cleared candidate trust.
- Amplify your hiring messages using targeted messaging, site advertising and sponsored content.

WANT TO LEARN MORE?

Connect with a ClearanceJobs Recruiting Specialist today at 1.866.302.7264 or visit our website at www.clearancejobs.com