the ThreatLab
Integrating Research Into Practice

Fundamental Skills for the Counter-Insider Threat (C-InT) Analyst

AUTHORS

Gregory Wilson, Lorien Megill, Leissa Nelson, & Stephanie Jaros

OPA Report No. 2021-064 | PERSEREC-PA-21-14

OPA
OFFICE OF PEOPLE ANALYTICS
PERSEREC
DEFENSE PERSONNEL AND SECURITY RESEARCH CENTER

Authors

DEFENSE PERSONNEL AND SECURITY RESEARCH CENTER

Stephanie Jaros

Leissa Nelson

PERATON

Gregory Wilson

NORTHROP GRUMMAN

Lorien Megill

Sponsors

The Defense Personnel and Security Research Center (PERSEREC) is a Department of Defense (DoD) entity dedicated to improving the effectiveness, efficiency, and fairness of DoD personnel suitability, security, and reliability systems. PERSEREC is part of the Office of People Analytics (OPA), which is a component of the Defense Human Resources Activity under the Office of the Under Secretary of Defense (Personnel and Readiness).

Within the National Counterintelligence and Security Center (NCSC), the primary mission of the National Insider Threat Task Force (NITTF) is to develop a Government-wide insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation.

The DoD Counter-Insider Threat Program provides leadership, management, and oversight of the policy, resources, and operational capabilities to prevent, detect, deter, and mitigate the threat posed by an insider. As part of this, the program works to ensure a well-equipped, trained, and vigilant workforce and a program/capabilities informed by social and behavioral science research.

Point of Contact

dodhra.threatlab@mail.mil

Suggested Citation

Wilson, G., Megill, L., Nelson, L., & Jaros, S. (2022). *Fundamental skills for the counter-insider threat (C-InT) analyst* (OPA Report No. 2021-064, PERSEREC-PA-21-14). Seaside, CA: Defense Personnel and Security Research Center/Office of People Analytics.

Contents

List of Figures

List of Tables

Introduction

Across the United States Government (USG), agencies have a history of programs, policies, and security professionals in place to protect classified assets. This protection was solidified and expanded in 2011, when Executive Order (EO) 13587 was signed, requiring structural reforms to improve the security of classified networks and responsible sharing and safeguarding of classified information. EO 13587 established general responsibilities for the heads of departments and agencies (D/As) that operate or access classified networks. One of these responsibilities included implementing insider threat detection and prevention programs consistent with the guidance and standards of the National Insider Threat Task Force (NITTF) that was also established by EO 13587.

Since EO 13587, executive branch D/As in general, and the Department of Defense (DoD) in particular, have been working to provide structure and training for individuals in the role of counter-insider threat (C-InT) analyst[1] who support the insider threat programs (InTP). While there are some training standards in place, including the third-party accredited Certified Counter-Insider Threat Professional (CCITP) program, there exist some gaps in the standards and training available for C-InT professionals. For example, the Office of Personnel Management (OPM) has not designated a job series for C-InT analysts, and there are no university degree programs in C-InT Studies (although The Threat Lab has created packaged curricula with nine graduate courses focused on C-InT Studies, four of which have been pilot tested). Instead, D/As are expected to provide on-the-job training and ensure their analysts operate within policy and regulations; produce clear, actionable recommendations; and protect the sensitive data with which they have been entrusted.

In light of these challenges, the NITTF and the DoD C-InT Program asked The Threat Lab, a program within the Defense Personnel and Security Research Center (PERSEREC), to create a Reference Guide intended to serve as a source of information about some of the knowledge and skill areas that are fundamental to the C-InT analyst. Development of this guide is part of a larger effort to professionalize the growing C-InT analyst workforce, formalize and define the role of C-InT analyst, and provide centralized resources for C-InT analyst training. As a result of the relative lack of standards and training, this Reference Guide should be viewed as an initial effort to help new and existing analysts working in USG C-InT programs better understand the principles and parameters underlying their role. As the field grows and matures, the Reference Guide should be revisited to reflect those changes.

To produce this Reference Guide, we conducted nine semi-structured interviews with C-InT professionals who were analysts, managers, or contributing subject matter experts (SMEs) across a variety of government agencies in C-InT programs and hubs.[2] In addition to the nine interviews, we also held six consultations with a variety of SMEs familiar with the training needs of C-InT analysts. In total, our research included 17 SMEs offering a range of viewpoints. **Appendix A** contains a more detailed explanation of methods used to research and write this Reference Guide.

This Reference Guide is a targeted presentation of information that the SMEs we interviewed identified as being important for a C-InT analyst's success. It does not cover all topics in the same level of detail. For example, the sections on the behavioral threat models and strategies for clear communication provide in-depth information because the topics tend to change relatively infrequently and are applicable across a broader range of D/As. For topics touching on policies and procedures that are more likely to change or are more agency specific, we provide

[1] C-InT analysts work in D/A insider threat programs and hubs in support of the National Insider Threat Program mission of "deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies" (Exec. Order No. 13587, 2011).

[2] "Hub" is the term used across the Federal Government to describe the personnel and centralized capability to execute a C-InT program.

high-level overviews and recommendations for other resources. We also do not address software tools or online search methods because that environment changes quickly, and this Reference Guide would soon be out of date.

Tradecraft

Tradecraft is a well-defined term in fields that are related to and often work alongside C-InT (e.g., counterintelligence [CI] and law enforcement [LE]). As part of overall professionalization efforts, one of the initial goals of this Reference Guide was to develop a meaningful definition of "tradecraft" for C-InT. However, the C-InT professionals we interviewed for this project did not currently apply the term to describe any part of their work and struggled to offer a definition that applied to their field when asked.

The related fields that do use the term tradecraft use it to describe investigative or intelligence-gathering methods. For example, CI tradecraft includes methods for analysis, surveillance, disguise, clandestine communication, interviewing and interrogation, and source recruitment. C-InT analysts, on the other hand, do not have investigative authority; their role is to perform inquiries and create recommendations that are then referred to those with the authority to act (e.g., CI, Security, local management, human resources [HR], or the Federal Bureau of Investigation [FBI]). It is, therefore, unsurprising that tradecraft might be difficult to define in the C-InT context.

Instead, as it is currently understood, the work of a C-InT analyst centers on managing the professional relationships and process of an inquiry rather than on field investigation. C-InT inquiries focus on threat assessment and policy violations and are not investigations in the same sense as CI or LE investigations. As the field develops and matures, the concept of tradecraft should be reassessed, likely on a broader scale than this project, to determine whether a common definition and set of tradecraft techniques can be identified.

Reference Guide Structure

This Reference Guide defines the role of the C-InT analyst in successful hub operations. It includes sections on C-InT policy, a C-InT analyst's role and key skills, and relevant foundational behavioral models.

The Guide also includes five appendices with additional materials. **Appendix A** details the research methods used to develop the Reference Guide. **Appendix B** lists documents that provide guidance on federal C-InT operations. **Appendix C** lists training and development resources for C-InT analysts. **Appendix D** lists additional resources that address C-InT topics. **Appendix E** is a glossary of abbreviations and key terms used in this document.

Policy

To help provide context and because federal insider threat policies are the foundation for all C-InT work, the first section of this Reference Guide focuses on policy. It summarizes key elements and concepts from major policy documents but does not reproduce those documents in extensive detail. The **References** section at the end of this document and **Appendix B** include links to the full policies.

Defining Insider Threat

In 2012, a Presidential Memorandum established the National Insider Threat Policy and the Minimum Standards (hereinafter, "Minimum Standards"), which describe the operation and scope of InTPs across D/As. In the Minimum Standards, insider threat is defined as:

> The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. (2012)

In this definition, "wittingly or unwittingly" means the damage caused by an insider can be intentional or unintentional. In other words, individuals might set out to do harm or they might cause harm by their inaction, inattention, or negligence. Whatever the cause, the mission to deter, detect, and defend extends beyond protecting the disclosure of classified and sensitive information by clearance holders. Increasingly, it also includes risks to personnel, facilities, and infrastructure from personnel, their families and associates, and others with access to facilities.

Establishing D/A Insider Threat Programs

When InTPs were first established under EO 13587, the NITTF assessed agency programs to determine whether they met the established Minimum Standards and where programs fell according to developmental milestones. In coordination with its National Security Council steering committee, the NITTF created three phases to classify programs, depending on the minimum standards they met:

1. Program Establishment (PE)
2. Initial Operating Capability (IOC)
3. Full Operating Capability (FOC)

For the NITTF to determine a hub as having attained FOC, the hub had to demonstrate it met all twenty-six Minimum Standards. The NITTF has since shifted its focus to the Maturity Framework it published in 2018. The framework lists elements that "have been identified as a capability or attribute exhibited by an advanced insider threat program" (NITTF, 2018). In recognition of this shift in focus, the **Policy** section of the Reference Guide discusses the Maturity Framework in more detail than the Minimum Standards.

Maturity Framework

The Maturity Framework was developed through working group sessions made up of USG C-InT professionals. The draft framework was modeled on industry best practices for capability maturity models and "vetted through a series of NITTF-hosted focus groups" (NITTF, 2018). The resulting 19 maturity elements (MEs) expand on the six areas from the original 2012 Minimum Standards. MEs are intended for use by D/A managers as benchmarks for the overall development and maturity of an InTP; however, many of the elements can also be viewed as describing specific functions performed by C-InT analysts.

Maturity Elements

The Maturity Framework and MEs establish how a good InTP works and define C-InT analyst tasks in such a program. C-InT analysts would benefit from studying the MEs and understand the implications for their work. For example, **ME5** reads, *"Includes stakeholders from a broad range of functional areas and others with specialized disciplinary expertise to strengthen InTP processes"* (NITTF, 2018, p. 8). While this ME refers to the need for a hub to include a broad range of functional areas, it also speaks to the fundamental C-InT activities of coordinating and translating between disciplines. As another example, **ME7**, which reads, *"Provides training and materials to all employees addressing the full range of insider threats to create a culture of insider threat awareness and prevention within the D/A"* (NITTF, 2018, p. 9), describes the outreach and education work performed by C-InT analysts to foster a risk-aware workforce and promote employee reporting. More detail on each of the MEs can be found in the published NITTF Insider Threat Program Maturity Framework (2018). Table 1 lists the 19 maturity elements.

Table 1

NITTF Insider Threat Program Maturity Framework Maturity Elements

Senior Official / InTP Leadership	**ME1:** Exists as a dedicated effort, positioned in the D/A to ensure access to leadership to build support, identify resources, and integrate insider threat objectives within the D/A's mission and functions. **ME2:** Employs metrics to determine progress in achieving program objectives and to identify areas requiring improvement. **ME3:** Ensures InTP adapts to changes in law, policy, organizational structure, and information technology (IT) architecture. **ME4:** Employs risk management principles tailored to address the evolving threat environment and mission needs.
Program Personnel	**ME5:** Includes stakeholders from a broad range of functional areas and others with specialized disciplinary expertise to strengthen InTP processes. **ME6:** Provides continuing education and training in appropriate fields and disciplines to help professionalize the insider threat cadre.
Employee Training & Awareness	**ME7:** Provides training and materials to all employees addressing the full range of insider threats to create a culture of insider threat awareness and prevention within the D/A.
Access to Information	**ME8:** Develops automated or scheduled processes for regular and timely receipt and integration of information from all relevant D/A stakeholders. **ME9:** Establishes procedures to receive notification with predictable frequency of information relevant to insider threat from other USG and federal partner data holders. **ME10:** Employs documented processes to validate information sources and identify and assess the use of new information sources.
Monitoring User Activity	**ME11:** Establishes a user activity monitoring (UAM) capability on all USG endpoints/devices and government-owned IT resources connected to USG computer networks accessible by cleared D/A personnel. **ME12:** Ensures UAM requirements are incorporated into D/A IT planning, design, and accreditation processes. **ME13:** Establishes capability to monitor the activity and conduct independent audits of InTP personnel with access to insider threat information and tools.

Information Integration, Analysis, & Response	**ME14:** Employs data integration methodologies and advanced analytics to help detect anomalous activity and potential insider threats. **ME15:** Employs behavioral science methodologies to help identify indicators of potential insider threats. **ME16:** Employs risk scoring capability based on behavioral and workplace factors to assist with detection of anomalous activity and potential insider threats and in the application of tailored mitigation strategies. **ME17:** Documents procedures and agreements with other USG InTPs to request or refer information on insider threats of mutual concern. **ME18:** Employs case management tools to ensure integrity and effectiveness of the insider threat inquiry and response processes. **ME19:** Conducts routine exercises to improve integration, analysis, and response procedures and processes.

Note. Adapted from "Insider Threat Program Maturity Framework," by NITTF, 2018 (https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf).

Executive Branch D/A Policy Differences

Insider threat policies across the Executive Branch D/As naturally vary depending on the historical mission, authorities, and unique challenges of each D/A. This diversity means that each D/A develops and operates its C-InT hub under different conditions. As a result, the Reference Guide does not address D/A policies. The Minimum Standards and MEs better represent the common policy ground between D/As.

Differences Between Title 50 and Non-Title 50 D/As

When the National Insider Threat Policy was issued, some national security and intelligence agencies (i.e., Title 50 agencies) already had in place some of the relevant C-InT capabilities as parts of other discrete disciplines (e.g., Security, CI; 50 U.S.C., 2011). However, stovepipes existed among these disciplines, necessitating the implementation of the InTP construct to help ensure cooperation.

In contrast, those non-Title 50 federal agencies that may have previously had a lesser emphasis on security, faced special challenges in creating new insider threat capabilities to meet EO 13587 requirements. Much of the employee population of these agencies may not require clearance for access to classified information, leading to smaller security capabilities and potentially less security awareness among non-Title 50 employees. In addition, EO 13587 is an unfunded mandate, which creates additional challenges to establishing new or expanding existing capabilities.

Differences in Policy and Authority to Use Publicly Available Electronic Information (PAEI)

Another important area where policies vary across D/As and from hub to hub is in the use of publicly available electronic information (PAEI). PAEI is "information that is available to the public on an electronic platform such as a website, social media, or database (whether for a fee or not)" (Intelligence and National Security Alliance, 2019). In other words, PAEI includes social media platforms and online, open-source content. Although there is federal policy that permits the use of publicly available social media information for personnel security purposes (Security Executive Agent Directive 5), there is a lack of federal or DoD policy permitting the use of social media collections for insider threat inquiries. That being said, open source has always been permitted, and hubs should find the right authority to cite if they pursue this type of information collection. It is also advisable to consult with agency or hub legal authorities before seeking or acting on PAEI.

Defining the Role and Key Skills of a C-InT Analyst

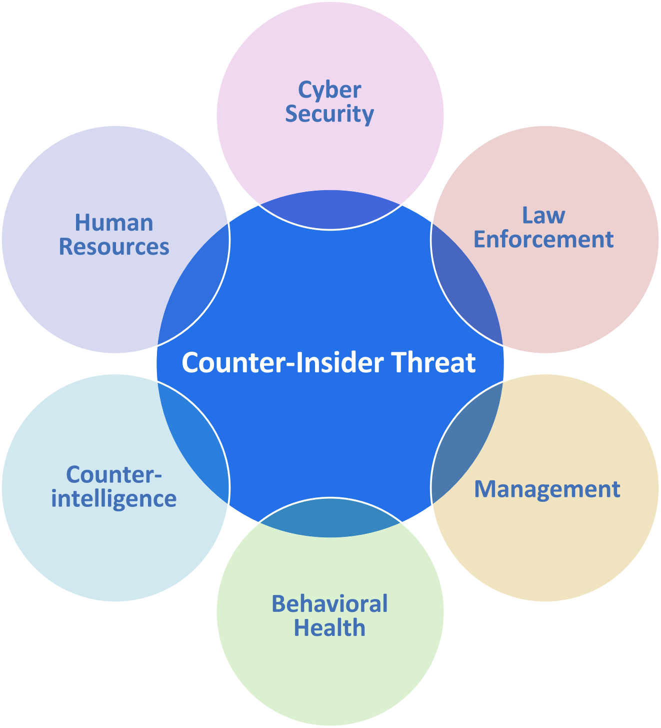
The job of the C-InT analyst is challenging. Analysts can have a proactive or a strategic role and are called to deter, detect, and mitigate the risk of insider threat, without being the individuals responsible for actually taking the mitigating actions. Depending on the D/A authorities, the job series of that D/A's C-InT analysts, and the placement of the InTP within its organizational structure, analysts may never go into the field to conduct physical surveillance or monitor the gathering of information. They monitor and respond to incidents of anomalous behavior and develop a whole-person understanding of individuals who are potentially on the critical path to an insider threat event (Shaw & Sellers, 2015) — see the Foundational Behavioral Models section of this guide for more information on the critical path. The C-InT hubs were specifically created to span and connect separate but complementary roles, or disciplines, (e.g., CI, LE, cybersecurity, HR, labor relations, threat assessors, behavioral psychologists, personnel security, lawyers, auditors, and managers) within a D/A. Analysts are key actors in this coordination.

Although members of these separate disciplines all work toward the same goal, each area of expertise speaks its own language. Outside of the hub, each type of expert has an independent role to perform that is guided by a distinct set of professional standards and specific training. C-InT analysts have the unique job of translating, fostering collaboration, and coordinating work across functions as well as being primarily responsible for developing mitigation plans. While C-InT has its own approach to problems, its own perspectives, and its own tools, C-InT analysts must collaboratively leverage expertise from members of each of the disciplines relevant to an inquiry and cohesively bring their capabilities together to accomplish deterrence, detection, and mitigation.

As C-InT programs developed, C-InT analysts took on a connecting role at the center of operations. Figure 1 illustrates this idea, showing the C-InT analyst connecting the distinct and relevant areas of expertise to create an informed picture that is as complete as possible. As part of an inquiry, C-InT analysts seek to get all of the stakeholders in the room, collect all relevant information, work with everyone to analyze the threat based on the evidence, and develop a mitigation plan to address the behavior of concern. "Getting everyone in the room" may actually mean getting everyone on a conference call. It could also mean getting the same information to all experts in a timely manner to broker an exchange of information and expertise within and across the disciplines and with external stakeholders.

Figure 1

C-InT Connecting the Work of Existing Disciplines Toward a Common Mission



Collaboration, Coordination, and Translation

Based on our research and SME interviews, we discovered that, while tradecraft for C-InT is not yet well defined, there are three foundational skills that are key to the work of C-InT analysts Those skills are: collaboration, coordination, and translation. SMEs identified these skills as fundamental and crucial for C-InT analysts to work effectively.

First, C-InT analysts must be expert *collaborators* across disciplines. They must understand the differences in how each area of expertise (e.g., HR, LE, CI) approaches the C-InT mission, and they must bring people and data together to enhance cooperation. Information sharing across disciplines is anchored in written policies, procedures, and guidelines in alignment with the Minimum Standards. The C-InT analyst can work to create a healthy collaborative environment that helps to facilitate effective information sharing by building and sustaining collegial relationships among disciplinary partners.

C-InT analysts must also *coordinate* the shared work of the different experts affiliated with the hub. Anomalous behavior is the central focus of inquiries, but as part of that, analysts work to develop a “whole person” understanding of the situation. The whole-person approach refers to examination of the incident and its context and a careful weighing of information regarding the behavior to identify whether significant risk exists. Analysts actively develop an understanding of the anomalous behavior based on available information and the complementary access of each discipline—to resources, information, and possibly the subject of the inquiry (although the identity of the subject is not always known). The multi-directional view managed by the C-InT analyst lends context to the risk assessment. Coordination requires the analyst to consolidate information by structuring complex data from different sources. It also requires an understanding of foundational behavioral paradigms, such as the Critical Path model (Shaw & Sellers, 2015). Through coordination, analysts build compelling relationships that help articulate shared goals and understanding and encourage partners to take recommended action.

Even with a shared understanding, it can often feel as though each expert is speaking a different language. For example, HR’s way of understanding a problem is naturally different than LE’s. *Translation*, the third essential skill, involves the C-InT analyst brokering understanding between these groups to avoid conflicts and to exchange data. Translation includes facilitating joint meetings, writing inquiry findings, performing educational outreach, and briefing findings and mitigation plans to internal and external stakeholders. C-InT analysts must translate between the experts in different areas so that shared goals and strategies are intelligible to all sides.

The crucial skills of collaboration, coordination, and translation, coupled with the vital training necessary to work in the C-InT space, enable analysts to ensure that all input providers can see their contributions reflected in analytic products and mitigation plans. Note that an InTP that has met the G. Access to Information category Minimum Standard and MEs 8–10 has the tools in place to ensure internal collaboration and coordination.

Three Key Skills for a C-InT Analyst’s Work

- **Collaboration** — Brokering trust to facilitate and motivate an atmosphere of cooperation; this includes articulating shared goals, being a steward of “the big picture,” performing educational outreach, and acting as a resource to distributed disciplines
- **Coordination** — Brokering information and resources across multiple disciplines to facilitate the shared C-InT mission; this includes developing mitigation plans, making everyone’s contributions visible, and working with legal counsel to protect privacy and civil liberties
- **Translation** — Brokering understanding and communication across multiple disciplines; this includes facilitating joint meetings, using behavioral models to frame data and information, producing analytic findings, and briefing findings and mitigation plans to internal and external stakeholders

C-InT Work and Trading Zones: Collaboration, Coordination, and Translation in Action

When two or more groups with different abilities come together to pursue shared goals or solve a shared problem, what develops can be referred to as a “trading zone” (Gorman, 2018). The shared problem requires the groups to negotiate and exchange resources, tools, products, and information. However, differences in expertise cause communication barriers. The groups might have different professional languages, value systems, or ways of asking questions. Additionally, there are different considerations that affect different groups, such as the legal considerations LE adheres to if enforcement action is required (e.g., restraining orders, making terrorist threats).

Even when groups have good intentions, negotiating different perspectives and ways of knowing can be difficult. Disciplines and groups not only prefer their own ideas and tools, but they also may actually distrust the ideas and tools of other people with different expertise. For C-InT analysts to succeed in detecting, deterring, and mitigating insider threat, they must help the varied disciplines overcomes these barriers.

One historical example of a trading zone is the shared work to develop radar during WWII (Galison, 2010). Radio engineers with hands-on knowledge and physicists with a theoretical approach came together to develop air defense systems that ultimately saved lives and helped turn the tide of the war. To do so, they had to build a new way of communicating that bridged their separate jargon, taken-for-granted assumptions, and ways of working on problems.

A notable example where communication and understanding in a trading zone fatally broke down, is that of the space shuttle Challenger disaster (Vaughan, 1996; Herndl et al., 1991). Staff engineers familiar with past O-ring damage in shuttle boosters during cold weather launches recommended scrubbing the January 28, 1986, launch. Managers were concerned with cost, schedule, and previous launch program delays. The engineers argued for another delay based on their specific judgment of possible catastrophic failure, but they could not overcome barriers to communication and understanding. The managers decided to proceed with the launch, and seven astronauts were killed in front of a national television audience.

Trading zones are most likely to succeed when groups develop a shared “interlanguage” (Galison, 2010) to bridge separate ways of understanding. One important aspect of the C-InT analyst’s role is managing the trading zone between disciplines by working to understand different languages, perspectives and needs and what each group has to offer and by making information sharing possible.

Building a whole-person understanding of a behavior of concern is not just compiling a list of what all of the hub-affiliated experts know. Building this view means knowing what the information from each discipline means in its own context (e.g., what the HR information means in the HR context) and translating that information into a shared C-InT interlanguage, so it takes on a shared meaning and considers all available and relevant information to determine whether a risk exists.

Deter, Detect, and Mitigate

A C-InT analyst’s skills are leveraged in service of the mission described as deter, detect, and mitigate. The particular processes through which each D/A executes this mission will be hub specific. Mastering a hub’s processes will involve significant on-the-job training for the analyst, which could include shadowing a more experienced colleague. However, although hubs across D/As have distinct processes, they follow roughly the same general pattern. This section will examine the general practices and processes analysts perform for deterrence, detection, and mitigation. An explanation of the inquiry process is included as part of the section on detection.

Deter

“Deter” stands separate from the timeline of working a C-InT inquiry. Deterrence includes all ongoing activities that make the C-InT program's mission visible, understood, and respected. Deterrence can also include things outside the C-InT program such as policies that prohibit cell phones in sensitive areas or cybersecurity training on handling sensitive documents. C-InT hubs make themselves known through outreach and education; system logon banners; promotion of reporting programs; and efforts to build trust and rapport with employees, stakeholders, and other groups that are in contact with the organization and its facilities. In particular, establishing and maintaining trust is important to a successful reporting program, especially because many early threat indicators are visible to coworkers and supervisors. Educating the organization on how to recognize suspicious and problematic behavior is also important; everyone needs to know what to report and where to report (including understanding what email or tip lines may be available). Deterrence is the result of the recognizable presence of a professional, vigilant, and trusted C-InT program.

Detect

Detection includes both monitoring and reporting. Many D/As employ user activity monitoring (UAM) to detect suspicious computer system use (e.g., large file transfers, foreign email contacts, restricted file access). Cyber may refer a flagged incident or pattern to the C-InT hub for follow-up.

Other sources for referrals may include:

- Personnel security (e.g., through continuous evaluation monitoring for security clearances)
- Local LE
- Security managers
- Concerned managers or coworkers (including through tip lines or dedicated emails)
- Other USG D/A InTPs

When a report is received, it may go directly to an analyst or to a hub manager who assigns inquiries to analysts. At this point, an inquiry may be initiated.

Initiating an Inquiry

If the individual exhibiting the anomalous, concerning behavior with a nexus to insider threat is under that hub's authority, the analyst begins an inquiry (i.e., a review of relevant information about the reported anomalous behavior) to determine whether there is an imminent threat. If there is an imminent threat of, for example, workplace violence, the analyst will refer the inquiry to LE.

If there is no imminent threat, the analyst's immediate goal is to validate the anomaly and determine if it meets a threshold for further action. During the inquiry, the analyst may find that the issue does not meet a required threshold for concern or that the evidence does not support the basis for concern. For example, an inquiry into a person's suspected gambling problem may not produce evidence of financial problems, reckless behavior, or problematic work behavior. The inquiry might also reveal that the incident has already been resolved or reported to the appropriate oversight entity inside or outside the organization.

Once the anomalous behavior is confirmed as meeting a threshold for further action, the analyst begins building context around the anomaly, completing an assessment plan to document the facts of the inquiry. The assessment plan identifies organizational databases to be searched and documents findings from the results of those searches. Different hubs rely on different internal databases. C-InT analysts may have access to databases and records that their collaborating disciplines do not, and vice versa. Analysts may identify information (e.g., court records) that other hub-affiliated experts should pursue. Some cooperating disciplines (e.g., the Inspector General or an Employee Assistance Program [EAP]) may have relevant sensitive records that analysts could request using a documented procedure.

The analyst will also work with SMEs and other disciplines to gather more data to document what else is known about other relevant incidents, predispositions, stressors, or concerning behaviors. If there is an obvious behavioral issue, the analyst may refer the inquiry to a behavioral or clinical psychologist or similar expert.

If the incident is of sufficient concern, the hub may convene a panel of SMEs to discuss their respective knowledge of and concerns regarding the incident. Behavioral psychologists and threat assessors may offer opinions on the level of threat or appropriate mitigation strategies. The C-InT analyst will also suggest mitigation strategies based on the facts of the inquiry. The analyst will prepare a memo documenting the discussions and conclusions of the panel. The analyst will also prepare an analytic finding that documents facts and mitigation recommendations. This finding becomes part of the permanent record of the incident.

Privacy is a concern throughout the process. Because every inquiry is different, analysts should confer with legal counsel or civil liberties and privacy officials as needed and according to hub standard operating procedures (SOPs) to ensure they operate within the legal framework. Transparency and accountability are also important, both to safeguard employee information and in the event of an audit.

Center for Development of Security Excellence (CDSE's) Best Practices for Inquiries

The *Insider Threat Mitigation Responses* (INT210.16) course from the Center for Development of Security Excellence (CDSE; n.d.) identifies the following elements in the C-InT inquiry process:

- Establish the goal of the inquiry and threat analysis.
  - Identify what question the team is trying to answer.
  - State your purpose and break the problem into manageable pieces.
- Conduct a fair and unbiased assessment.
- Acknowledge your own assumptions.
  - Are they justifiable?
  - How do they shape your point of view?
- Seek alternate viewpoints.
  - What are the strengths and weaknesses of your own perspective?
- Ground and support your claims with evidence.
  - Are claims based on relevant information?
  - Do claims go beyond the evidence at hand?
  - Have you considered all relevant information?
  - Is there opposing information out there?

The primary goal of any inquiry is accuracy and fairness to the person of concern. This process involves thoughtful planning, careful execution, and self-reflexive quality checks in pursuit of a productive whole-person understanding.

Mitigate

Mitigation may mean removal from access or employment or, ideally, early intervention when stakes for individuals and organizations are lower. A C-InT program that strives to intervene and mitigate problems early can make the organization and its members stronger and healthier. See the CDSE's *Insider Threat Mitigation Responses* (INT210.16) course (n.d.) for in-depth training on mitigation concepts and approaches.

Building a Mitigation Plan

As part of an insider threat inquiry, analysts help develop a mitigation plan tailored to the facts available to them. Developing a mitigation plan may involve multidisciplinary input from across the organization, including security, cybersecurity, HR, legal, labor relations, mental and behavioral health, CI, and LE. The responsibility for implementing the mitigation plan will vary depending on a variety of factors, specific to each D/A. However, the InTP is ideally not responsible for taking the recommended action. Instead, they will hand the agreed-upon mitigation plan off to someone else in the D/A or to another external D/A to implement. Hub personnel may be responsible for briefing managers on the findings of the inquiry and the recommended mitigation plan. Because the C-InT analyst is unlikely to be the person implementing the recommendations, these briefings, findings, and mitigation plans require clear and persuasive communication from the analyst.

Depending on the facts of the inquiry, mitigation may require different parts of the organization to act. Mitigation actions may focus on the individual, for example:

- Referring to counseling or an EAP
- Referring to security, which may result in the suspension of a clearance or restricted access to facilities
- Referring to CI, LE, or HR

Or mitigation actions may address organization-wide vulnerabilities and remediation, for example:

- Limiting downloadable file size on computer systems
- Reconfiguring hardware to prevent thumb drive use
- Increasing activity monitoring
- Enacting changes in D/A SOPs, policies, guidelines, etc.
- Requiring new security training or updating or revising other types of training
- Changing building security procedures

An inquiry can also result in actions addressing both the individual and organizational levels. The C-InT program should avoid the appearance of being a “gotcha” program. Employees are more likely to report incidents and indicators if they trust that the C-InT program is looking out for both the employees and the organization and is seeking to prevent problems before they escalate. Mitigation responses should include ongoing monitoring to ensure new concerns do not arise, and responses should be periodically reevaluated.

Note: Some inquiries require referral to outside authorities such as the FBI, affiliated CI groups, the DoD Insider Threat Management Analysis Center (DITMAC), local LE, or the Defense Counterintelligence and Security Agency (DCSA). Criminal activity and illegal disclosure have specific reporting requirements. SOPs and other guidelines identify reporting thresholds and agencies that must be notified. **DoD C-InT hubs** have criteria and procedures for notifying DITMAC, Military Department CI, or the FBI. **Other federal agency hubs** have criteria and procedures for notifying the FBI or other appropriate external entities. **Industry C-InT programs** have criteria and procedures for notifying the FBI and the DCSA.

Awareness of Privacy and Ethics for C-InT Analysts

C-InT analysts will have access to sensitive information that can be subject to constitutional and privacy protections. There are no existing ethics and professional responsibility training or guides specifically for USG C-InT programs; however, C-InT analysts still have professional and ethical obligations to safeguard the rights of the individuals exhibiting anomalous behaviors in inquiries, and C-InT analysts are subject to the ethical guidelines of their D/A. Furthermore, ethical and legal conduct is essential for C-InT programs to build trust within their organizations. The C-InT professionals we interviewed for this study emphasized that, without trust, employees will not report concerns or violations or will not seek help for problems impacting their own work. If employees do not trust that inquiries by their organization's C-InT program are handled according to high standards, they will not support the program.

C-InT analysts should be aware that there are specific First Amendment, civil liberty, Whistleblower Protection Act, and Privacy Act protections that cover employees regardless of whether they are subject to a C-InT inquiry. The First Amendment protects free speech and the right to peaceful assembly and association. The Whistleblower Protection Act protects certain disclosures by Federal employees/applicants who are reporting fraud, abuse, or illegal activity. The Privacy Act requires that federal agencies only collect personal information that is legally authorized and necessary. Each hub should have SOPs, specific training, and access to legal experts to clarify the lines between protected speech and information that can be part of a C-InT inquiry.

The Fourth Amendment provides protections against unlawful searches. Unlawful data collection during a C-InT inquiry can be a form of unlawful search. Note that there is no reasonable expectation of privacy if employees use government computers and systems they access while on official duty. Each hub will have SOPs, specific training, and access to legal experts to clarify what types of information are permissible to gather or retain.

C-InT analysts should consult with the legal counsel, civil liberties and privacy officials, whistleblowing officials, or LE agencies affiliated with their hub as often as the facts of the inquiry require. The CDSE course *Insider Threat Privacy and Civil Liberties* (INT260.16), offers more information on this topic—see **Appendix C** for more information on this and other courses for C-InT analysts.

Communicating as a C-InT Analyst

As described in general terms above, communicating and translating information across groups of people with different areas of expertise are foundational skills for a C-InT analyst. As translators, C-InT analysts often broker communication between disciplines and help craft many inputs and opinions into cohesive and clear messages. They have to communicate clearly and concisely with multiple audiences in mind. Communication tasks include writing analytic findings and reports; briefing managers, supervisors, and potentially D/A leadership; and teaching and conducting educational outreach to promote a risk-aware workforce. C-InT analysts must be proficient in synthesizing and communicating disparate ideas both in writing and verbally. Therefore, they must intentionally and continually hone their communication skills.

Writing Advice for C-InT Analysts

A key aspect of the C-InT analyst's role is communicating in writing to the people who will make decisions or execute plans. Analysts must be able to clearly convey the "who," "what," "where," "when," "why," and "how" so that identified anomalous behaviors are understood and effectively mitigated. Intelligence professionals in other roles may write reports that include speculation on how to interpret information, but C-InT analysts are called on to concisely capture the facts of research and deliberative conversations using standardized formats and without speculation. The CDSE offers two 16-week courses to improve overall communication skills:

- *Writing and Communication Skills for Security Professionals* ED201.10
  https://www.cdse.edu/Training/Virtual-Instructor-led-Courses/ED201/
- *Effective Communication in DoD Security* ED512.10
  https://www.cdse.edu/Training/Virtual-Instructor-led-Courses/ED512/

Writing well is difficult. Improvement comes only with practice and feedback. Effective analytic writing is a skill that analysts develop throughout their careers. There is not enough in this section to immediately perfect anyone's writing, but practicing and incorporating the key points detailed here can bring about a significant improvement.

Analytic Writing Technique

To improve analytic writing technique, keep the following points in mind.

- Understand the purpose of your document and write with that purpose in mind.
- Understand the audience of your document and what they need to learn or accomplish.
- Understand that your document will likely become part of an ongoing record, so future readers will need clear information and context.
- Always use the "bottom line up front" (BLUF) approach. First, give the reader the main takeaway they need to make a decision, then support that bottom line with evidence.
- Do not speculate beyond the facts at hand. Do not add your own judgments. Use language such as "appears to be." This is especially important because analytic findings become part of the permanent record.
- Include only what is relevant. If you are including, for example, two-year-old traffic tickets, explain why they are meaningful to the inquiry.
- Do not cut and paste large blocks of text from databases or search results when you can summarize and weed out unneeded information that may be obscuring key points.
- Ensure that all documents from your C-InT hub have a consistent tone and vocabulary regardless of the author. Understand which parts of documents need a consistent approach and which parts allow flexibility.

Writing in Active Voice

The best way to write clear and concise sentences is to write in the active voice and use strong subjects and verbs. The active voice identifies who is performing the action. In the passive voice, the subject receives the verb's action, which can change the clarity and meaning of what you are writing. For example:

> **Active:** The employee made threats against her supervisor.
>
> **Passive:** Threats were made against the supervisor.

Although both sentences mean roughly the same thing, in the passive sentence, the subject of the sentence is "threats" and not "the employee." The passive sentence hides the responsibility of the employee for her actions. When writing an analytic report or communicating mitigation recommendations, it is important to be clear and up front about the person or people who completed the actions being described.

Here is another example:

> **Active:** The EAP referred the employee to a debt counselling program.
>
> **Passive:** The employee was referred by the EAP to a debt counselling program.

Perhaps either of these sentences would work in a report, but it is also important to write with strong verbs and strong subjects. To find a strong verb, ask what the main action of the sentence is. In the above example, "referred" is a stronger verb than "was referred." The strong verb should be as close to the front of the sentence as possible. In this example, it is also important to identify who is doing the referring and use that as the strong subject. With those goals in mind, the active voice sentence works better.

> The EAP [**strong subject**] referred [**strong verb**] the employee to a debt counselling program.

Revision

Because the human mind does not naturally think in clear and concise sentences, the first draft that we put down on paper can usually be simplified. Part of the writing process is returning to our initial written thoughts and revising them for clarity and conciseness. The example below walks through the process of revising a sentence that appeared in earlier drafts of this Reference Guide.

In an early draft of this guide, the following sentence appeared:

> **Original:** In 2015, Eric Shaw and Laura Sellers published a critical path method for understanding and evaluating insider threat risks that has become influential.

This sentence, unfiltered from the brain of the author directly onto the page, keeps adding information and is overly complicated. There is a lot for the reader to absorb.

We could improve the sentence by revising it to read this way:

> **Revision:** The Critical Path model has become an influential method to understand and evaluate insider threat risks.

An even cleaner version of the sentence would read like this:

> **Better still:** The Critical Path model [**strong subject**] influences [**strong verb**] the understanding and evaluation of insider threat risks.

Writers must hunt for the clearest meaning and rearrange phrases to build a sentence the reader can easily understand. The subject and verb in the cleanest version of the example sentence above are present in the original version, but revision was required to eliminate extra information and shape the sentence in the clearest way. When writing, we must always keep the reader in mind and streamline the information we include. When possible, edit out information that does not help the reader understand or accomplish the task at hand.

One way to better understand the audience of a document is to think about expectations. Anytime somebody looks at a scoreboard, opens a dictionary, or listens to a graduation speech, they have expectations. They have learned that information will be presented in certain ways in certain situations. Most of a person's understanding of whether a communication is successful comes from how well their expectations for that type of communication are met. Look for successful examples before you try any new type of writing. The examples will help you understand the expectations for a particular type of communication. Copy what works. Determine what parts of the examples you should not change and what parts allow variability.

Example Insider Threat Hub Documents

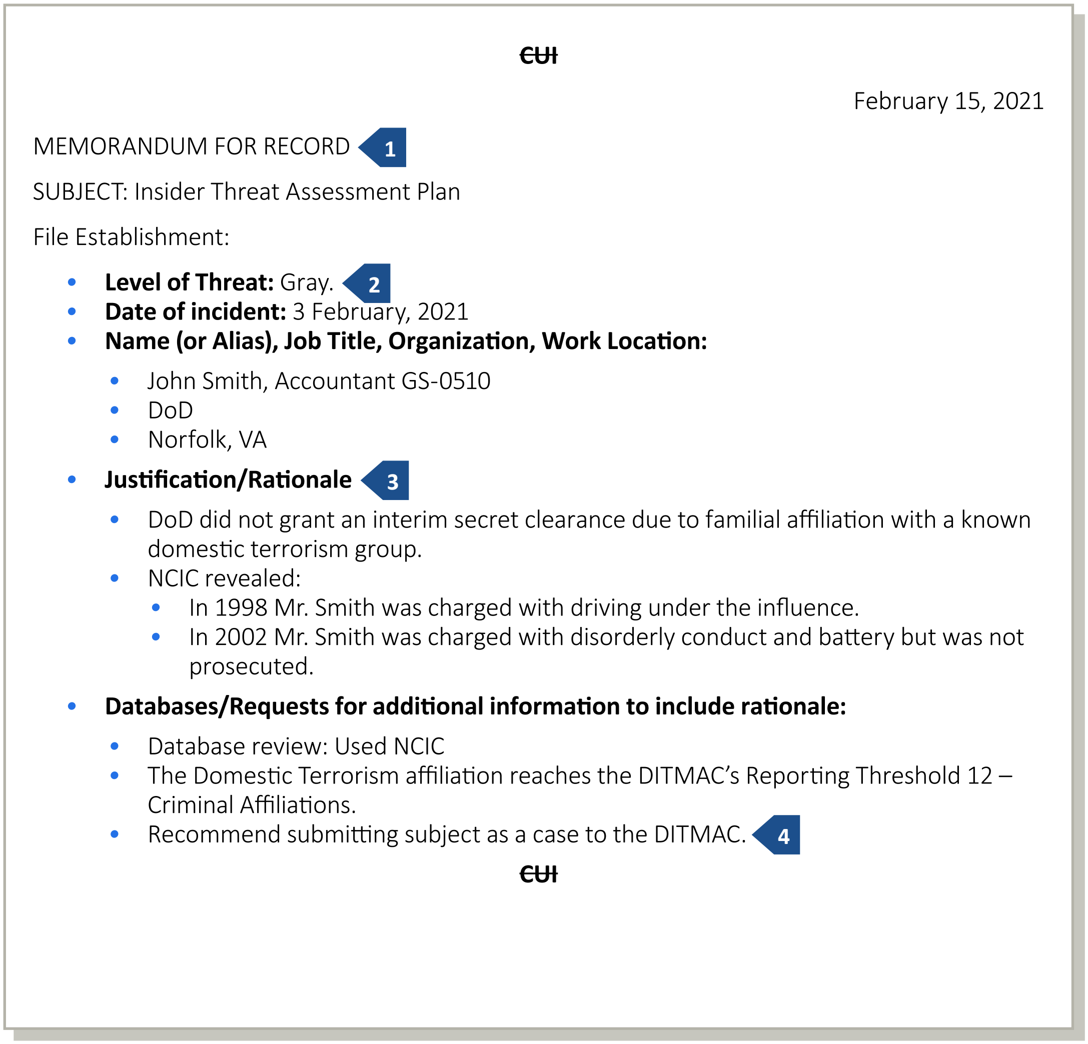
Figures 2 and 3 are example analytic writing products. These samples are fictional documents created to show some of the best practices outlined in this Reference Guide as well as the standards, conventions, and formats that these analytic writing products could use. The Confidential Unclassified Information (CUI) markings are retained to convey the importance of appropriate document marking, but do not reflect the actual status of the documents. These examples are modeled after items from a DoD InTP. They provide representative and realistic examples for the ways C-InT analytic writing can take shape, but they should not be taken as templates or guides on how to complete analytic writing products. The format of writing products adopted by non-DoD and other DoD C-InT hubs may be different. For any analytic findings, be sure to adhere to the formatting and best practices utilized by your hub.

Figure 2 shows an example Insider Threat Assessment Plan that is well structured for clarity and concision.

1. The plan is a brief memo of record that identifies criminal affiliations that turned up during a National Crime Information Center (NCIC) database check for a new employee or new clearance applicant and the subsequent information uncovered in the C-InT inquiry.
2. This color-coding is DoD-specific, other agencies may use different means to identify threat level.
   a. Brown is the lowest priority (e.g., employee access has already been removed).
   b. Purple is the next higher level (e.g., employee is still working, but mitigation is in place, and the threat is low).
   c. Gray is for threats with high concern (e.g., employee has clearance and/or access and is exhibiting concerning behavior).
   d. Blue is the highest priority (e.g., there is a threat that demands immediate action).
3. The memo briefly explains the facts uncovered and justification for the recommendation to refer to DITMAC.
4. It recommends that the incident meets the reporting threshold for referral to DITMAC. This memo would be retained by the hub, so detail is specific without speculation.

Figure 2

Sample Analytic Writing 1



~~**CUI**~~

February 15, 2021

MEMORANDUM FOR RECORD

SUBJECT: Insider Threat Assessment Plan

File Establishment:

- **Level of Threat:** Gray.
- **Date of incident:** 3 February, 2021
- **Name (or Alias), Job Title, Organization, Work Location:**
  - John Smith, Accountant GS-0510
  - DoD
  - Norfolk, VA
- **Justification/Rationale**
  - DoD did not grant an interim secret clearance due to familial affiliation with a known domestic terrorism group.
  - NCIC revealed:
    - In 1998 Mr. Smith was charged with driving under the influence.
    - In 2002 Mr. Smith was charged with disorderly conduct and battery but was not prosecuted.
- **Databases/Requests for additional information to include rationale:**
  - Database review: Used NCIC
  - The Domestic Terrorism affiliation reaches the DITMAC's Reporting Threshold 12 – Criminal Affiliations.
  - Recommend submitting subject as a case to the DITMAC.

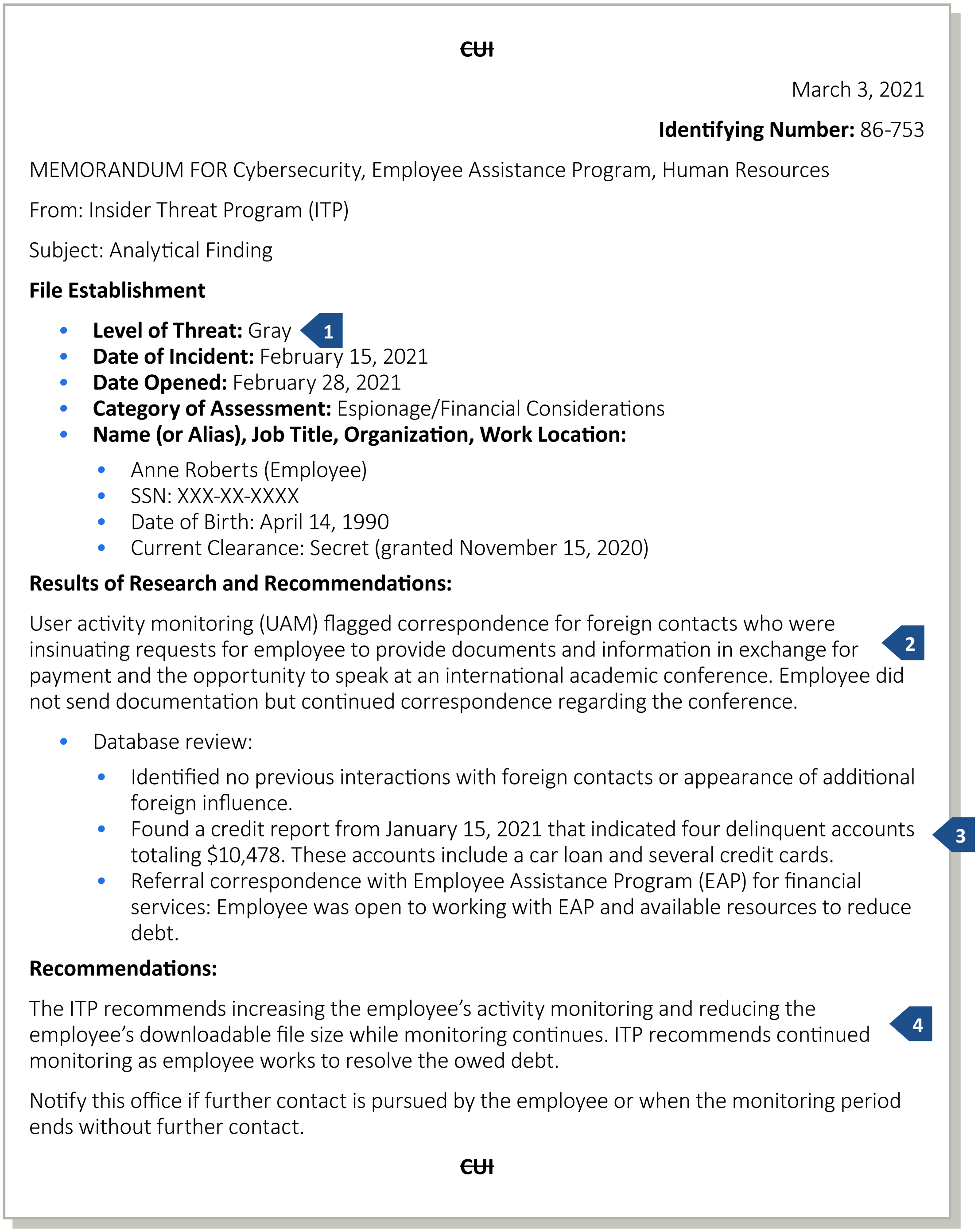
~~**CUI**~~

Figure 3 shows an example enterprise-level analytic finding composed for clarity and concision.

1. Like the previous example, this report ranks the level of threat according to the DoD-specific color coding.
2. For this example, an alert identified that the employee had been involved in correspondence with foreign contacts seeking to obtain information.
3. Additional research uncovered that the employee had delinquent accounts.
4. The C-InT program recommended ongoing monitoring of the situation and reduced access for the employee.

Figure 3

Sample Analytic Writing 2



~~CUI~~

March 3, 2021

Identifying Number: 86-753

MEMORANDUM FOR Cybersecurity, Employee Assistance Program, Human Resources

From: Insider Threat Program (ITP)

Subject: Analytical Finding

File Establishment

- **Level of Threat:** Gray
- **Date of Incident:** February 15, 2021
- **Date Opened:** February 28, 2021
- **Category of Assessment:** Espionage/Financial Considerations
- **Name (or Alias), Job Title, Organization, Work Location:**
  - Anne Roberts (Employee)
  - SSN: XXX-XX-XXXX
  - Date of Birth: April 14, 1990
  - Current Clearance: Secret (granted November 15, 2020)

Results of Research and Recommendations:

User activity monitoring (UAM) flagged correspondence for foreign contacts who were insinuating requests for employee to provide documents and information in exchange for payment and the opportunity to speak at an international academic conference. Employee did not send documentation but continued correspondence regarding the conference.

- Database review:
  - Identified no previous interactions with foreign contacts or appearance of additional foreign influence.
  - Found a credit report from January 15, 2021 that indicated four delinquent accounts totaling $10,478. These accounts include a car loan and several credit cards.
  - Referral correspondence with Employee Assistance Program (EAP) for financial services: Employee was open to working with EAP and available resources to reduce debt.

Recommendations:

The ITP recommends increasing the employee's activity monitoring and reducing the employee's downloadable file size while monitoring continues. ITP recommends continued monitoring as employee works to resolve the owed debt.

Notify this office if further contact is pursued by the employee or when the monitoring period ends without further contact.

~~CUI~~

Briefing Advice for C-InT Analysts

Remember, C-InT programs themselves are not in a position to take the recommended mitigation actions, so the analyst must communicate findings to the appropriate decision makers in a way that clearly conveys the importance of acting. Often, analysts brief leadership outside the hub who need to take action or direct that action be taken. If the audience is less familiar with C-InT operations, the meaning of the findings and the rationale of the recommendations may need to be explained in more detail (i.e., how the proposed mitigation will address the problem, given the perceived level of threat).

For the C-InT analyst, “briefing” can mean different things. It can mean writing a longer explanatory report, speaking about a document during a meeting or phone call, or presenting PowerPoint slides for an in-person audience. Sometimes C-InT analysts speak directly; sometimes they support a supervisor who is briefing materials the analysts produced.

As with writing, it is important to watch examples of effective briefings, understand the expectations, and copy what is successful. *Do presenters read aloud from their slides or notes during the briefing? Do presenters speak off the cuff? Do people put up slides or hand out a document and then summarize the main points? Are there interruptions and questions during the briefing?* The first step to preparing is knowing what you are preparing for. Understand the special attention required if classified information is involved, such as in counterterrorism or espionage cases. In these instances, all briefs should be conducted in a Sensitive Compartmented Information Facility, as applicable, and written summaries should be prepared using classified computers and systems.

Once you understand how you are expected to give a briefing, make a plan. Prepare the materials you will need to express the key points and recommendations and practice your presentation. The more important the briefing is and the less experience you have, the more you need to practice.

Foundational Behavioral Models

The C-InT field is multidisciplinary, and it benefits from ideas and approaches developed across many professions and areas of study. The disciplines that interact with the C-InT mission space refer to theoretical models or representations in their areas of expertise that help them to better understand their work and responsibilities. A theoretical model depicts the relationship between structured concepts that help to explain how or why a situation or phenomenon occurs. Models create explanatory categories from existing data or make predictions based on existing research and supported with new data.

In the C-InT domain, there are currently three foundational models of human behavior that serve as reference points. This guide offers a basic introduction and references for further reading to help C-InT analysts begin to understand these models.

The three behavioral models help explain how threats evolve and how people move towards threat behavior. Knowledge of these patterns helps C-InT analysts assess who poses a threat and how mitigation strategies can be applied. The three models are the Critical Path model developed by Shaw and Sellers (2015), the Pathway to Violence model developed by Calhoun and Weston (2003), and the Insider Threat Risk Ontology developed by Greitzer et al. (2016; see also Greitzer et al., 2019). Greitzer et al.'s model is more complex and comprehensive than the first two; it is growing in popularity as C-InT professionals try to better understand threat behavior.

Critical Path Model to Insider Risk

Eric Shaw and Laura Sellers (2015) identified "factors that increase the risk that insiders will undertake hostile acts against their organizations" (p. 1). Assessments performed after espionage or workplace violence incidents often find that there were warning signs that should have tipped off managers, security personnel, or coworkers. Using empirical studies, Shaw and Sellers (2015) proposed a four-part model to help develop awareness of potential warning signs. The model, described in Figure 4, is composed of personal predispositions, stressors, concerning behaviors, and problematic organizational responses.

Figure 4

Factors along the Critical Path

Factors Along the Critical Path to Insider Risk	
1. Personal Predispositions	• Medical/psychiatric conditions • Personality or social skills issues • Prior misconduct or disciplinary action • Criminal activity, addictions, or dependency on alcohol or narcotic usage
2. Stressors	• Personal • Professional • Financial
3. Concerning Behaviors	• Interpersonal • Technical • Security • Financial • Personnel • Mental health/addictions • Social network • Travel

Factors Along the Critical Path to Insider Risk	
4. Problematic Organizational Responses	• Inattention • No risk assessment process • Inadequate investigation • Summary dismissal or other actions that escalate risk
Hostile Act	

Note. Adapted from "Application of the Critical-Path Method to evaluate insider risks," by Shaw, E., & Sellers, L., 2012, *Studies in Intelligence, 59(2)*, pp. 1-8 https://www.hsdl.org/?abstract&did=768010. Copyright 2012 by Studies in Intelligence.

Personal Predispositions are baseline characteristics that can increase the likelihood of insider threat behavior. Underlying medical, mental health, personality, social skills, or social network issues (e.g., association with corrupt, competitive, or adversarial groups) can be initial vulnerabilities. Shaw and Sellers (2015) cite a 2010 article looking at the cases of 24 people convicted of espionage, where 20 of those people had alcohol abuse issues (p. 3).

Stressors are "negative or positive events that result in changes in personal, social, or professional responsibilities that require people to spend effort and energy to adjust" (Shaw & Sellers, 2015, p. 4). We all face stressful events, such as divorce, family illness, financial difficulties, job loss, rejection, personal setbacks, and even new opportunities, but these events can lead some people down the critical path, especially in combination with vulnerable personal predispositions.

Shaw and Sellers (2015) cite the example of Thomas Dolce, who worked for the Army as a civilian. Over a four-year period (from 1979–1983), he experienced the death of his mother as well as his wife's cancer diagnosis, long illness, and eventual death. During this time, Dolce's longstanding interest in South Africa led to over 40 occurrences of his passing secret weapons analysis documents to South African embassy officials (Valentine, 1988). Individual employees may be resilient to one or two life stressors, but multiple, compounding factors can make good employees and their organizations vulnerable.

Insider threats can be unintentional—for example, the careless handling of information or assets resulting from stress or distraction; however, multiple or severe factors like financial stress can put employees at risk of becoming insider threats.

Shaw and Sellers (2015) describe **Concerning Behaviors** as a common indicator of insider threat behavior:

> Studies of inside offenders have shown that most were known to have committed some form of concerning or problematic behavior before acting directly against their organization. These actions included violations of policy and standard procedure, professional conduct, accepted practice, rules, regulations, or law through action or inaction (failure to report) that had been observed by managers, supervisors, and coworkers. (p. 1)

For example, Shaw and Sellers (2015) point out that Aaron Alexis had multiple weapons violations leading up to his attack on the Washington Navy Yard. Certain types of acting out, as well as withdrawing and isolating, are likely visible to coworkers, who should engage their organization's C-InT program. Once notified, C-InT analysts can look into whether additional factors suggest trouble is brewing.

Problematic Organizational Responses can make situations worse and increase insider risk. Problematic responses include ignoring existing problems, showing a lack of empathy, and not having the right policies and procedures in place to prevent or react to potential or unfolding problems (e.g., not having an EAP, dispute resolution processes, or feedback mechanisms to report hostile working conditions).

Perceived mistreatment can also tip an employee toward hostile action. Unresolved grievances with the organization or colleagues (e.g., feeling cheated by non-promotion or seeing a suspension and loss of pay as unjust) can be a significant factor in employees becoming insider risks and workplace violence threats. Shaw and Sellers (2015) relate the story of a fired chief information officer who carried a grudge for years before directing hacking attacks against his former company.

Identifying Precursor Behaviors

Shaw and Seller's research also shows that individuals often engage in precursor behaviors before committing consciously damaging acts. These behaviors may include:

> …surveillance or research; solicitation of the cooperation of witting or unwitting others; the acquisition of resources or skills; rehearsal of activities to gauge a plan's safety and effectiveness; and attempts at authorized or unauthorized access to obtain, replicate and transfer targeted information; deception or other forms of operational security… (2015, p. 5)

These end-stage behaviors are often noticed by coworkers or managers. A workforce that is well educated on the warning signs of potential insider threat can report concerning behaviors they notice to their organization's C-InT program. An active program can intervene before threats become catastrophic. A vigilant and sensitive C-InT program, with a risk-aware workforce, can divert employees off the critical path.

Pathway to Violence

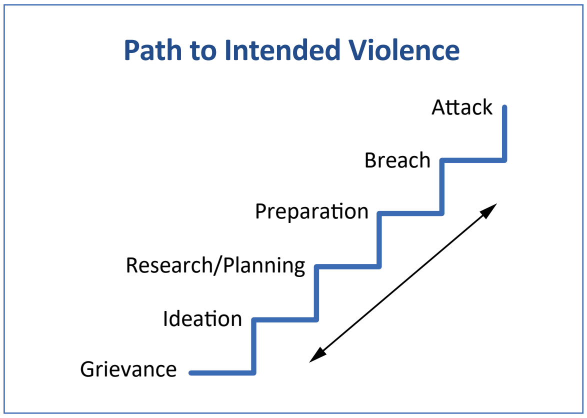
Another foundational behavioral model is Frederick Calhoun and Stephen Weston's (2003) Pathway to Violence model. We discuss it here as one relevant model pertaining to moving towards violent acts, which are a particularly concerning type of insider threat.

Calhoun and Weston's research (2003) revealed violent actors typically follow specific stages along a path (see Figure 5).

1. Initially, an individual has a **grievance** that develops into violent **ideation**.
2. They then **research** and **plan** a way to act on their ideation. For example, an employee who feels they were unfairly terminated may fantasize about exacting revenge on a boss and coworkers. This individual may then plan specific times to find and access the boss and coworkers together on the worksite.
3. A violent employee's **preparation** may include purchasing a gun and ammunition, visiting a shooting range to practice, and making final communications with family.
4. The employee may **probe** the attack site and check to see if their access card still opens outside doors and if they can drive into the parking lot unnoticed during work hours.
5. If the **breach** is successful, they will use that tested method to access the worksite and execute the **attack**.

Figure 5

Pathway to Violence based on Calhoun, T., & Weston, S. (2003). Contemporary threat management. San Diego: Specialized Training Services.



Although this Pathway to Violence model has a different focus than Shaw and Sellers' Critical Path model, each offers a compatible framework to understand unwanted insider behavior. While the critical path focuses on four components that can propel an individual to engage in insider threat, the pathway to violence focuses on the cognitive escalation of how an individual goes from a grievance to engaging in insider threat. Both models make it clear that no one becomes a problem out of the blue (although there are examples of individuals who come into the government with malicious intent, such as Ana Montes). Tensions build and problematic behaviors escalate according to recognizable patterns.

Insider Threat Risk Ontology

Frank Greitzer and his collaborators (2016, 2019) have published several articles developing a more expansive model (or ontology) of insider threat factors. An ontology is a list that tries to represent all items that exist in a context or system and often tries to capture the causal interactions or hierarchical relationships between those items. Ontologies with well-defined items and relationships can be the basis for computer models designed to predict or weight the likelihood of outcomes. This ontology is not a pathway model like the previous two models we discussed. In compiling this list of factors, Greitzer and his collaborators also collected information on how these factors interact and influence each other.

A detailed model like this may someday become the inner structure of an automated artificial intelligence tool for identifying threat behavior. For now, it provides a more thorough set of factors and categories than the Shaw and Sellers model. Greitzer et al.'s work will be useful for analysts who want to go beyond the Shaw and Sellers model to explore a more complex and comprehensive set of elements and interactions.

Table 2 shows one version of Greitzer's insider threat ontology. The ontology is divided into individual human factors and organizational factors "based on a systematic review, analysis and synthesis of existing research, case studies and guidelines that have been produced by the insider threat research community" (Greitzer et al., 2016, p. 2).

The individual factors are divided into categories of concerning behaviors, life narratives, ideologies, dynamic states, and static traits. Each category contains sub-categories that provide a detailed description of possible insider threat indicators.

The organizational factors are divided into categories of security practices, communication issues, work setting (management systems), work planning and control, and mitigating factors. These categories represent the organizational context that can contribute to, interact with, influence, or mitigate the human factors that characterize insider threat.

Table 2

Sociotechnical Indicators of Insider Threat Risk (2016)

INDIVIDUAL HUMAN FACTORS	ORGANIZATIONAL FACTORS
Concerning Behaviors • Boundary Violation – Concerning work habits, attendance issues, blurred personal/professional boundaries, threatening/intimidating behaviors, boundary probing, social engineering, minor policy violations, travel policy violations, unauthorized travel, unauthorized foreign travel, change in pattern of foreign travel, security violations • Job Performance – Cyberloafing, negative evaluation • Technical/Cyber Violation – Concerns about: authentication/ authorization, data access patterns, network patterns, data transfer patterns, command usage, data deletion/modification, suspicious communications **Life Narrative** • Job Performance – Cyberloafing, negative evaluation • Financial Concerns – Lifestyle incongruities (unexplained affluence, etc.), risky financial profile (bankruptcy, large expenses-to-income ratio, bounced/bad checks, credit problems) • Personal History – Demographics, employment, education background, major life events, health status, marital history, U.S. Immigration/citizenship status **Ideology** • Disloyalty – Behaviors or expressions of disloyalty to the organization or to the U.S. government • Radical Beliefs – Radical political beliefs, radical religious beliefs • Unusual Contact with Foreign Entity –Unreported contact with foreign nationals **Dynamic State** • Affect – Excessive anger/hostility, disengagement, mood swings • Attitude – Lack of motivation, overly competitive, expresses feelings of disgruntlement with job, overly critical, resentful, defensive **Static Trait** • Personality Dimensions – Neuroticism, disagreeableness, low conscientiousness, excitement seeking, honesty-humility on six-factor personality scale • Other Personality Traits – Characteristics associated with maliciousness or vulnerability to exploitation (Machiavellianism, narcissism, psychopathy, sadism, authoritarianism, social dominance orientation) • Temperament – Various temperament issues that may be observed/reported by coworkers (Big ego, callousness, lack of empathy, lack of remorse, manipulativeness, rebelliousness, poor time management, preoccupation with power/grandiosity)	**Security Practices** • Communication/training • Policy clarity • Hiring • Monitoring • Organizational justice • Implementation of security controls **Communication Issues** • Inadequate procedures/directions • Poor communications **Work Setting (Management Systems)** • Distractions • Insufficient resources • Poor management systems • Job instability • Lack of career advancement • Poor physical work conditions • Organizational changes **Work Planning and Control** • Job pressure/job stress • Time factors/unrealistic time constraints • Task difficulty • Change in routine • Heavy or prolonged workload • Insufficient workload • Conflict of work roles • Work role ambiguity • Lack of autonomy • Lack of decision making power • Irregular timing of work shifts • Extended working hours • Lack of breaks **Mitigating Factors** • Flexible work schedule • Employee Assistance Plan • Effective staff training and awareness • Reporting mechanism

Note. Adapted from “Constructs Comprising Individual Human Factors” and “Constructs Comprising Organizational Factors,” by Greitzer et al., 2016, *Developing an Ontology for Individual and Organizational Sociotechnical Indicators of Insider Threat Risk* (https://www.researchgate.net/publication/310751829_Developing_an_Ontology_for_Individual_and_Organizational_Sociotechnical_Indicators_of_Insider_Threat_Risk). Copyright 2016 by The Eleventh International Conference on Semantic Technology for Intelligence, Defense, and Security (STIDS).

Summary

This Reference Guide defines key skills required by analysts and provides valuable information to define and support the work of C-InT analysts and C-InT hubs. The **Introduction** discusses the idea of tradecraft in C-InT work and lays out the structure of the document. The **Policy** section describes the origins of the federal policies that establish minimum standards and evaluation criteria for C-InT programs. This section also discusses the diversity of policies and procedures across different federal C-InT hubs.

The **Defining the Role and Key Skills of a C-InT Analyst** section describes the major facets of the work C-InT analysts perform and stresses the complexity and importance of this work. It also defines the three fundamental skills (i.e., collaboration, coordination, and translation). This section also discusses the process of working an inquiry in the context of the C-InT mission to deter, detect, and mitigate and includes a brief discussion of the privacy and ethical concerns relevant to a C-InT analyst. This section also stresses the importance of effective communication for C-InT analysts and offers instructions for better analytic writing and briefing.

The **Foundational Behavioral Models** section describes the three models that have had a significant influence on C-InT work (i.e., Critical Path, Pathway to Violence, and Insider Threat Risk Ontology). These models provide the framework for deterring, detecting, and mitigating insider threats.

Since the inception of the NITTF in 2011, the role of the C-InT analyst has been evolving with the development of C-InT programs. As is evident by the lack of an OPM job category for the C-InT analyst, the role and its importance lack visibility. Because insider threat events directly impact the government, national security, and personnel too frequently, this Reference Guide aims to provide a center of gravity for the recognition, understanding, and professionalization of the C-InT analyst role.

References

Calhoun, T., & Weston, S. (2003). *Contemporary threat management*. Specialized Training Services. https://www.specializedtraining.com/showproduct.aspx?ProductID=74&SEName=contemporary-threat-management

Center for Development of Security Excellence (CDSE). (n.d.). *Insider threat mitigation responses: INT210.16*. CDSE eLearning Courses. https://www.cdse.edu/Training/eLearning/INT210/ [Information referenced from these online courses was accurate at the time of this report's publication.]

Exec. Order No. 13587, 198, 3 C.F.R. 276 (2011, October 7). https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

50 U.S.C. (2011). Title 50 – War and national defense. United States Code, 2011 Edition. U.S. Government Publishing Office. https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50.htm

Galison, P. (2010). Trading with the enemy. In M.E. Gorman (Ed.) *Trading zones and interactional expertise: Creating new kinds of collaboration* (pp. 25-52). MIT Press.

Gorman, M. E. (2018). Trading zones and moral imagination as ways of preventing normalized deviance. In R.E. Freeman, S. Dmytriyev, & A.C. Wicks (Eds.) *The moral imagination of Patricia Werhane: A festschrift* (pp. 121-132). Springer, Cham.

Greitzer, F. L., Imran, M., Purl, J., Axelrad, E. T., Leong, Y. M., Becker, D. E., ... & Sticha, P. J. (2016). Developing an ontology for individual and organizational sociotechnical indicators of insider threat risk. *Semantic Technology for Intelligence, Defense, and Security (STIDS) Conference*, November 15-16, 2016. George Mason University. https://www.researchgate.net/publication/310751829_Developing_an_Ontology_for_Individual_and_Organizational_Sociotechnical_Indicators_of_Insider_Threat_Risk

Greitzer, F. L., Lee, J. D., Purl, J., & Zaidi, A. K. (2019). Design and implementation of a comprehensive insider threat ontology. Procedia Computer Science, 153, 361-369. https://doi.org/10.1016/j.procs.2019.05.090

Herndl, C. G., Fennell, B. A., & Miller, C. R. (1991). Understanding failures in organizational discourse: The accident at three mile island and the shuttle challenger disaster. In C. Bazerman & J. Paradis (Eds.) *Textual dynamics of the professions: Historical and contemporary studies of writing in professional communities* (pp. 279-305). The University of Wisconsin Press.

Intelligence and National Security Alliance, Insider Threat Subcommittee. (2019, January). The use of publicly available electronic information for insider threat monitoring. INSA. https://www.insaonline.org/wp-content/uploads/2019/02/FINAL-PAEI-whitepaper.pdf

National Insider Threat Task Force. (2018). Insider threat program maturity framework. NITTF https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf

Office of the Director of National Intelligence. (2016, May 12). Security executive agent directive 5. https://www.odni.gov/files/NCSC/documents/Regulations/SEAD_5.pdf

Presidential Memorandum, National insider threat policy and minimum standards for executive branch insider threat programs. (2012, November 21). https://obamawhitehouse.archives.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand

Shaw, E., & Sellers, L. (2015). Application of the critical-path method to evaluate insider risks. *Studies in Intelligence*, 59(2), 1-8. https://www.hsdl.org/?abstract&did=768010

Valentine, P.W. (1988, October 12). Md. Man admits to espionage for South Africa. *The Washington Post*. https://www.washingtonpost.com/archive/politics/1988/10/12/md-man-admits-to-espionage-for-south-africa/04e06ad8-983a-4915-a7e5-100284d5a36d/

Vaughan, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. University of Chicago Press.

Appendix A: Methods

To produce this Reference Guide, we conducted nine semi-structured interviews with counter-insider threat (C-InT) professionals who were hub analysts, managers, or contributing subject matter experts (SME) across a variety of government agencies. "Hub" is the term used across the Federal Government to describe the personnel and centralized capability to execute a C-InT program. In addition to the nine interviews, we also had six consultations with a variety of SMEs familiar with the training needs of C-InT analysts. In total, our research included 17 SMEs offering a range of viewpoints.

We identified SMEs initially through the recommendations of senior C-InT community advisors and then through snowball sampling. For the snowball sampling, we asked participating SMEs to recommend others who would have different and valuable perspectives. Overall, we sought to consult SMEs who represented different organizations and different levels and types of engagement with C-InT analysis. In what seems to be a majority male field, we intentionally sought to diversify the gender balance of the SME pool. We spoke with 11 male and 6 female SMEs.

We also researched available training materials, policies, and procedures related to C-InT analysis. We reviewed existing training materials for C-InT analysts and conducted a gap analysis. This research and analysis found that instructors in intelligence studies degree programs and industry training experts were unhappy with the training materials available for counterintelligence (CI) analysts when applied to C-InT. They also stated that there were very few C-InT-analyst-specific materials. We determined a substantial gap did exist in available training materials for C-InT analyst careers and that most professional C-InT training occurs on the job with no standardization across the profession. The SMEs we spoke with shared that many of the C-InT professionals they work with came to the field with training in traditional intelligence gathering, law enforcement (LE), or other related fields.

In addition, we completed a policy and literature review focused on C-InT analysis and used the major topics of this background research to develop an initial outline for the Reference Guide and to develop the protocol that guided the SME interviews. Expert accounts of hub operations and discussions of the meaning of tradecraft in the context of C-InT cleared up several misconceptions the authors brought to the project and strongly shaped and streamlined the content. This Reference Guide is based on the results of these reviews and interviews.

Appendix B: Guidance Documents

This appendix includes documents that provide guidance for insider threat hub operations. Although there are many DoD directives, manuals, and instructions, there are far fewer guidance documents that apply to hubs across the government. All of the documents listed here are completely unclassified. For individuals in government services, there are additional CUI foundational guidance documents.

Guidance Document	Link
Committee on National Security Systems Instruction (CNSSI) 4009, "National Information Assurance (IA) Glossary," April 26, 2010	CNSSI-4009.pdf (rmf.org)
Defense Federal Acquisition Regulation Supplement (DFARS) (current edition)	Federal Register :: Suggested Search - Defense Federal Acquisition Regulation Supplement (DFARS)
Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended	Executive Orders | National Archives
Executive Order 13526, "Classified National Security Information," December 29, 2009	The President Executive Order 13526 | National Archives
Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011	Executive Order 13587 -- Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information | whitehouse.gov (archives.gov)
National Archives and Records Administration, Transmittal Number 28, "General Records Schedule 5.6: Security Records," July 2017	The General Records Schedules Transmittal 28 (archives.gov)
National Insider Threat Task Force (NITTF) Advisory: Insider Threat Program Personnel Training, NITTF-Advisory-2021-001, 15 March 2021	NITTF_Advisory_2021-001_Insider_Threat_Program_Personnel_Training.pdf (dni.gov)
National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990	nsd42.pdf (fas.org)
Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," November 21, 2012	Presidential Memorandum -- National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs | whitehouse.gov (archives.gov)
Public Law 104-191, Section 264, "Health Insurance Portability and Accountability Act of 1996," August 21, 1996	PLAW-104publ191.pdf (congress.gov)

Guidance Document	Link
Public Law 114-328, Section 951, "National Defense Authorization Act for Fiscal Year 2017," December 23, 2016	PUBL328.PS (congress.gov)
Public Law 115-91, Title 9, Subtitle B, "Data Management and Analytics," December 12, 2017	PUBL091.PS (house.gov)
Public Law 95-452, Title 5, U.S.C., as amended through Public Law 115-254, "The Inspector General Act of 1978," October 5, 2018	452.pdf (house.gov)
Section 552a of Title 5, United States Code (also known as "The Privacy Act of 1974")	Privacy Act of 1974 (justice.gov)
Section 922 of Public Law 112-81, "National Defense Authorization Act," December 31, 2011	PUBL081.PS (congress.gov)
Title 10, United States Code	U.S. Code: Title 10. ARMED FORCES | U.S. Code | US Law | LII / Legal Information Institute (cornell.edu)
Title 45, Code of Federal Regulations	Code of Federal Regulations - Title 45: Public Welfare and Title 46: Protection of Human Subjects (hhs.gov)
United States Code, Title 5, Section 552a (also known as the "Privacy Act of 1974")	5 U.S. Code § 552a - Records maintained on individuals | U.S. Code | US Law | LII / Legal Information Institute (cornell.edu)

Appendix C: Training Resources

There are a number of in-person and online training courses available to increase your C-InT analysis knowledge, skills, and abilities.

Certifications & Programs

Center for Defense and Security Excellence (CDSE) Insider Threat (InT) Training Programs

The CDSE currently offers two InT programs: the Insider Threat Program Operations Personnel Program (INT311.CU) and the Insider Threat Program Management Personnel Program (INT312.CU).

- **InT Program Operations Personnel Program (INT311.CU):** This program is targeted towards analysts and other operations personnel working in InT programs within DoD components, federal agencies, and industry. For more information on the Operations Personnel Program, visit Insider Threat Program Operations Personnel Program INT311.CU (cdse.edu).
- **InT Program Management Personnel Program (INT312.CU):** This specialized program is targeted towards personnel managing an InT program. For more information on the Management Personnel Program, visit Insider Threat Program Management Personnel Program INT312.CU (cdse.edu).

For more information on the CDSE InT certifications and other training resources, visit Insider Threat (cdse.edu).

Certified Counter-Insider Threat Professional (CCITP) Program

The CCITP Program is a joint program between the Office of the Under Secretary of Defense for Intelligence and Security (OUSD[I&S]) and National Insider Threat Task Force (NITTF). The program is designed to enhance the professionalization of federal insider threat program practitioners. The CCITP validates practitioner knowledge, skills, and abilities as defined in the Insider Threat Essential Body of Knowledge (EBK). The CCITP consists of two National Commission for Certifying Agencies (NCCA) accredited certifications: CCITP-Fundamentals (CCITP-F) and CCITP-Analysis (CCITP-A).

- **CCITP-F:** This certification is targeted towards personnel working directly in an InT hub; however, the CCITP-F is open to anyone who works in or is *affiliated with* an InT hub, as determined by each organization's Program Reviewer. The CCITP-F assesses an individual's understanding and skills as annotated in the CCITP EBK to perform the tasks outlined in the CCITP Essential Body of Work (EBW).
- **CCITP-A:** This certification is targeted towards personnel working directly in an InT hub and performing analysis functions. The CCITP-A establishes a common standard of InT analysis, focusing specifically on the analysis of C-InT information and development of mitigation recommendations; it assesses an individual's understanding and skills as annotated in the CCITP EBK to perform the tasks outlined in the CCITP EBW.

For more information on the CCITP-F and CCITP-A certifications, visit Counter-Insider Threat (defense.gov).

In-Hub/Live Training Events

Defense Intelligence Agency (DIA) Insider Threat Training

The Defense Intelligence Agency (DIA) currently offers a week-long Insider Threat Detection and Analysis Course (ITDAC) introducing students to fundamental concepts, approaches, and policy in insider threat. Students walk through case studies, exercises, and discussions and take an exam assessing their understanding of introduced concepts.

eLearning

CDSE eLearning Courses

In addition to its **InT Program Operations Personnel (INT311.CU)** and **InT Program Management Personnel (INT312.CU)** programs, the CDSE offers several standalone InT courses, which are also eligible for Continuing Education Unit (CEU) or Professional Development Unit (PDU) credit.

- Insider Threat Awareness Course INT101.16
- Establishing an Insider Threat Program for Your Organization INT122.16
- Developing a Multidisciplinary Insider Threat Capability INT201.16
- Insider Threat Mitigation Responses INT210.16
- Preserving Investigative and Operational Viability in Insider Threat INT220.16
- Insider Threat Records Checks INT230.16
- Insider Threat Basic Hub Operations INT240.16
- Critical Thinking for Insider Threat Analysts INT250.16
- Insider Threat Privacy and Civil Liberties INT260.16
- Maximizing Organizational Trust INT270.16
- Cyber Insider Threat INT280.16
- Behavioral Science in Insider Threat INT290.16
- Continuous Monitoring Course CS200.16
- Counterintelligence Concerns for National Security Adjudicators CI020.16
- Unauthorized Disclosure (UD) of Classified Information and Controlled Unclassified Information (CUI) IF130.16

For more information on these courses and other training resources, visit Insider Threat (cdse.edu).

External Training Module

The NITTF features an external **Insider Threat Training Module:** This module was developed by an Intelligence Community partner. It addresses a variety of C-InT topics such as: information leaks and spills, espionage, sabotage, and targeted violence. https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf/ncsc-nittf-training

Other Resources

CDSE Training Resources

In addition to programs and courses, the CDSE also offers a variety of C-InT training resources, including:

- Case studies
- Job aids
- Security awareness games
- Security posters, shorts, and training videos
- Toolkits
- Webinars

To browse CDSE training resources, visit Insider Threat (cdse.edu).

The Threat Lab

The Threat Lab, founded in 2018 by PERSEREC, develops a variety of products and services to help realize the DoD C-InT Program Director’s vision to incorporate the social and behavioral sciences in the mission space.

Visit https://www.dhra.mil/PERSEREC/Selected-Reports/ to access selected PERSEREC Reports. You can also stay updated regarding Threat Lab events and products by emailing DoDHRA.ThreatLab@mail.mil to be added to The Threat Lab distribution list.

Appendix D: Additional Resources

This appendix includes additional resources to continue building your understanding of analytic and intelligence techniques and increase your knowledge of insider threat mitigation.

Resource	Link
Beneda, J., & Jaros, S. L. (2020). *The PAR capabilities and the convergence of workplace violence prevention, counter-insider threat, and personnel vetting policies in DoD.*	https://apps.dtic.mil/sti/citations/AD1094489
Bradley, P., Chambers, W., Davenport, C., & Saner, L. (2017). *A national research agenda on insider threat.*	http://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_179892.pdf
Bulling, D., & Scalora, M. (2013). *Threat assessment glossary.*	https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1122&context=publicpolicypublications
CIA Center for the Study of Intelligence. (2009). *A tradecraft primer for structured analytic techniques for improving intelligence analysis.*	https://www.hsdl.org/?abstract&did=20945
Center for Development of Security Excellence. (n.d.). *Insider threat essential body of knowledge: Deskside reference.* CDSE	https://www.cdse.edu/Portals/124/Documents/jobaids/insider/Essential-Body-of-Knowledge.pdf
Cybersecurity and Infrastructure Security Agency. (2020). *Insider threat mitigation guide.*	https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf
DoD Intelligence and Security Professional Certification. (2018). *All-source counter-insider threat (C-InT) assessment and mitigation essential body of work (EBW).*	https://dodcertpmo.defense.gov/Portals/62/C-InT%20EBW%20as%20of%2011_28_2018.pdf
DoD Intelligence and Security Professional Certification. (2018). *Counter insider threat essential body of knowledge (C-InT EBK).*	https://dodcertpmo.defense.gov/Portals/62/C-InT%20EBK%20as%20of%2011_28_2018.pdf
Ettinger, J. (2019). *Cyber intelligence tradecraft report.*	https://apps.dtic.mil/sti/pdfs/AD1090501.pdf
Griffin, C. P. (Director.) (n.d.). *Pathway to violence* [Video]. The Department of Homeland Security.	https://www.cisa.gov/pathway-violence-video
Mandel, D. R. (2020). Assessment and communication of uncertainty in intelligence to support decision making: Final report of research task group SAS-114.	https://doi.org/10.31234/osf.io/vxh9r

Resource	Link
National Insider Threat Task Force. *Additional insider threat resources.*	https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf/ncsc-nittf-resource-library/briefings-to-the-insider-threat-community
NITTF. (2017). *Insider threat competency resource guide.*	https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Advisory-CRG-Aug-30-2017.pdf
NITTF. (2017). *Insider threat guide: A compendium of best practices to accompany the national insider threat minimum standards.*	https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf
NITTF. *Insider threat program maturity framework.*	https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf
Stephen, A., Girven, R. S., & Bruce, J. B. (2016). Assessing the value of structured analytic techniques in the US intelligence community. RAND Corporation, Santa Monica	https://apps.dtic.mil/sti/pdfs/AD1024447.pdf

Appendix E: Glossary

This appendix includes definitions for abbreviations and key terms used throughout the guide.

Abbreviation	Definition
Analysis	The process by which information is transformed into intelligence; systematically examining information to identify significant facts, make judgments, and draw conclusions
BLUF	Bottom Line Up Front: A writing strategy where the conclusions or findings in a document are presented first
CCITP	Certified Counter Insider Threat Professionals
CCITP-A	Certified Counter Insider Threat Professionals Analysis
CCITP-F	Certified Counter Insider Threat Professionals Fundamentals
CDSE	Center for Development of Security Excellence
CI	Counterintelligence
C-InT	counter-insider threat
CUI	Controlled Unclassified Information (CUI): Government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies
D/A	Department/Agency
DCSA	Defense Counterintelligence and Security Agency
DIA	Defense Intelligence Agency
DITMAC	DoD Insider Threat Management Analysis Center
Discipline	A term used in C-InT hubs to refer to experts affiliated with the hub but who may have a different primary role in the department or agency (e.g., HR, LE, management, employee assistance programs, cybersecurity, CI, and legal counsel); these experts have differing and complementary perspectives and access to information; they may work inside the hub or be called upon for outside expertise and information during inquiries or mitigation planning; discipline can more generally refer to a specific area of professional practice or academic field where group identity, beliefs, and agreement of standard practices is strong; often used interchangeably with the term "Pillars"
DoD	Department of Defense
EAP	Employee Assistance Program
EBK	Essential Body of Knowledge
EBW	Essential Body of Work
EO	Executive Order
FBI	Federal Bureau of Investigation
Finding	A document that presents evidence discovered during an inquiry; used to support recommendations and mitigation plans

Abbreviation	Definition
FOC	Full Operating Capability: A maturity benchmark from the 2012 Insider Threat Minimum Standards that represents an advanced stage of development for an insider threat program
HR	Human Resources
Hub	The term used across the Federal Government to describe the personnel and centralized capability to execute a C-InT program
Inquiry	The fact-finding and analysis process to determine the facts of any incident
Insider	• DoD Directive (DoDD) 5205.16: Any person with authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD. • NISPOM DoD 5220.22-M: Cleared contractor personnel with authorized access to any Government or contractor resource, including personnel, facilities, information, equipment, networks, and systems. • EO 13587: Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks, or systems.
Insider Threat	• NISPOM DoD 5220.22-M: The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information. • EO 13587: The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.
InTP	Insider Threat Program
IOC	Initial Operating Capability: A maturity benchmark from the 2012 Insider Threat Minimum Standards that represents an interim stage of development for an insider threat program
ITDAC	Insider Threat Detection and Analysis Course
LE	Law Enforcement
ME	Maturity Element

Abbreviation	Definition
Mitigation	Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident. Includes solutions that involve analysis of threat activity and vulnerability data, which provide timely and accurate responses to prevent attacks, reduce vulnerabilities, and fix systems
Model	A set of structured concepts that help explain recurring problems or predict likely outcomes in recurring situations
NCCA	National Commission for Certifying Agencies
NCIC	National Crime Information Center: A computerized index of criminal justice information (i.e.- criminal record history information, fugitives, stolen properties, missing persons). It is available to Federal, state, and local LE and other criminal justice agencies
NITTF	National Insider Threat Task Force
OPA	Office of the People Analytics
OPM	Office of Personnel Management
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
PAEI	Publicly Available Electronic Information
PE	Program Establishment: A maturity benchmark from the 2012 Insider Threat Minimum Standards that represents an early stage of development for an insider threat program
PERSEREC	Defense Personnel and Security Research Center
Pillars	See “Discipline”
Privacy Act	The Privacy Act of 1974 (5 USC 552a) establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies; requires that agencies provide public notice of their systems of records through publication in the Federal Register; prohibits the disclosure of information from a system of records without the written consent of the individual who is the subject of the information search, unless the disclosure is pursuant to one of 12 statutory exceptions
SME	Subject Matter Expert
SOP	Standard Operating Procedure
Threat	An adversary having the intent, capability, and opportunity to cause loss or damage
UAM	User Activity Monitoring
USG	United States Government

Abbreviation	Definition
Whistleblower Protection Act	The Whistleblower Protection Act of 1989 and the subsequent Whistleblower Protection Enhancement Act of 2012 protect certain disclosures by Federal employees/applicants who are reporting fraud, abuse, or illegal activity, and prohibit retaliation
Whole-Person Approach	A way of conducting inquiries that refers to examination of a sufficient period of the individual history and a careful weighing of information about that individual and their behavior to identify whether significant risk exists