Law Enforcement and Insider Threat Short

Student Guide

May 2026

Center for Development of Security Excellence

Contents

Welcome

Welcome, and thank you for joining the Law Enforcement and Insider Threat Q&A session. Insider Threat Hub teams are made up of professionals from:

- Law Enforcement
- Security
- Human Resources
- Legal
- Counterintelligence
- Behavioral Science
- Cybersecurity

Each of these groups contributes important and unique information to the risk management process.

Insider Threat Hub teams exist to deter personnel from becoming an insider threat, detect existing insider threats, and analyze potential threats to validate reports and develop context on the subject and situation. Insider Threat Hub teams mitigate the risks personnel may pose and work to move them off the critical pathway through early intervention, proactive reporting, and referrals.

Law Enforcement professionals recognize the indicators of criminal activity, coercion, or misconduct that may intersect with insider risk. They ensure credible threats are identified early and properly investigated, and they coordinate with legal authorities to protect the organization. For these reasons and more, Law Enforcement professionals are essential to an effective Insider Threat Hub team.

Today, you will hear from a Law Enforcement professional and will have an opportunity to ask questions to summarize the role Law Enforcement personnel play in deterring, detecting, analyzing, and mitigating potential insider threats.

Law Enforcement Representative Introduction

I'd like to introduce our Law Enforcement representative, Mr. Daniel D'Ambrosio. As the Senior Lead Law Enforcement and Counterintelligence Subject Matter Expert for the Defense Counterintelligence and Security Agency (DCSA), Mr. D'Ambrosio supports analysis and mitigation of insider threats to the DOW by ensuring the team has access to knowledge of CI and law enforcement-related activities, emergent insider threat cases, and best practices. He has experience in both developing and operating insider

threat programs, pulling from over 30 years of federal law enforcement and CI senior executive leadership experience in his former NCIS Agent role.

General Law Enforcement and Insider Threat

Let's first focus on establishing the basic relationship between Law Enforcement and insider threat.

What is the mission of a Law Enforcement Insider Threat Hub?

Mr. D'Ambrosio: At its core, the mission of a hub like this is to get out in front of problems. We're here to find, understand, and reduce the risks that come from people inside the organization, including sworn officers, civilian employees, contractors, and volunteers who might misuse their official access for the wrong reason—whether that's for personal gain, with bad intent, or to break the law. This includes preventing, detecting, and responding to activities that compromise sensitive information, violate public trust, endanger officer safety, or undermine the integrity of law enforcement operations. And a huge part of our job is also about building the right culture. We want to create an environment where everyone is security-conscious and acts with integrity. By fostering a strong ethical climate and encouraging vigilance, the hub aims to minimize the potential for insider threats to materialize and ensure that all personnel are aware of their responsibilities in safeguarding sensitive information and maintaining public trust.

What insider threat indicators are most relevant in a law enforcement setting?

Mr. D'Ambrosio: When we talk about law enforcement, there are a few red flags that really stand out. A primary red flag is not necessarily unauthorized access, but rather it's often less about hacking and more about what you could call "professional curiosity" going too far—an officer has legitimate access, but they start looking up things that they have no business looking at. This often involves self-queries or browsing the system for information on family members, friends, or partners. Another key indicator is disreputable association. That's a broad term covering connections to friends or family with criminal records, individuals with ties to terrorism, or transnational criminal elements. Other signs that warrant investigation include unexplained wealth, data exfiltration, significant behavioral changes like paranoia or stress, and a repeated disregard for policy. But it's really important to stress these are just warning signs. They aren't proof of guilt; they just tell us that we need to take a closer, impartial look.

Upon validating such indicators, a formal process must begin immediately with the referral to either internal affairs (IA) or Office of Professional Responsibility (OPR) depending on agency makeup and possibly the Office of the Inspector General

(OIG) for deconfliction, especially if any criminality is suspected. Concurrently, both the Insider Threat Hub lead and the officers' supervisory chain of command must be notified to ensure proper coordination and further facilitation with IA, OPR, or OIG. To maintain the integrity of the inquiry. A secure case file is opened to document all activities and all relevant data is preserved to protect the chain of custody. Finally, a preliminary risk assessment is conducted in consultation with legal counsel to determine the immediate threat level and implement appropriate interim mitigation measures.

What are unique challenges of insider threats in law enforcement?

Mr. D'Ambrosio: Law enforcement insider threats present unique challenges due to several factors, including broad access to sensitive information such as criminal history, databases, informant identities, operational plans, and the authority and power that the officers possess, which can be misused for personal gain. The potential for a code of silence within law enforcement, high levels of trust and autonomy granted to officers, and the high impact potential of an insider threat compromising investigations, endangering the public, also contribute to these challenges. Furthermore, law enforcement insiders are often familiar with security measures, making it easier to circumvent them, and the heightened stress they experience can make them vulnerable to radicalization.

To address these challenges, a robust insider threat program is essential, including comprehensive screening, continuous monitoring, security awareness training, and a culture of ethical conduct.

Law Enforcement's Indicators and Response Processes

Let's move on to a new topic: Law Enforcement's indicators of insider threat and their response processes.

How do you conduct a law enforcement insider threat assessment?

Mr. D'Ambrosio: Conducting a law enforcement insider threat assessment is a systematic process that starts with collecting relevant data from a wide variety of sources. This includes technical data like system logs, body camera audits, and CAD/NCIC usage, as well as human-centric information from HR files, internal affairs records, peer reports, and observed behavioral indicators. This collected data is then thoroughly analyzed to identify patterns, anomalies, or red flags that may point to a potential insider threat. Following the analysis, a formal risk assessment is performed to evaluate the severity of the potential threat and its impact on public safety, officer safety and operational integrity. Crucially, this assessment must be closely coordinated with IA, OPR, OIG, or any other entity conducting a parallel

criminal investigation, as the assessment's findings could be discoverable. Therefore, collaboration with both in-house counsel and the relevant prosecutor's office is essential. The entire process concludes with meticulous documentation and a comprehensive report summarizing the findings and recommending mitigation measures, ensuring all data is handled securely and confidentially.

What steps do you take when you identify a sworn officer as a potential insider threat?

Mr. D'Ambrosio: Upon identifying a sworn officer as a potential insider threat, the first step is to validate the initial indicators to confirm their credibility. Immediately after, and especially if criminality is suspected, the matter should be referred to IA, OPR, or OIG for deconfliction to ensure investigative efforts are not compromised. It is also vital to concurrently notify both the Insider Threat Hub lead and the officer's supervisory chain of command. Simultaneously, a secure case file must be opened to document all investigative activities, and imminent steps must be taken to preserve all relevant logs and data to maintain clear chain of custody. Following consultation with legal counsel to ensure all actions are within policy guidelines, a preliminary risk assessment is conducted to determine the immediate threat posed by the officer. This assessment will guide the implementation of appropriate interim measures to mitigate any identified risks.

How do you assess risk involving officers with access to firearms and tactical systems?

Mr. D'Ambrosio: Assessing risk for officers with access to firearms and tactical systems requires a comprehensive, multifaceted approach. The evaluation must consider a range of factors, including behavioral indicators like increased aggression, personal stressors such as financial or relationship problems, and any history of disciplinary issues or threats of violence. A particularly critical factor to include is whether the officer is aware they are under investigation, as this knowledge is a significant stressor that can exacerbate other risk indicators.

The assessment should also cover duty-related concerns about judgement, weapon proficiency, and any threat-enabling capabilities, such as knowledge of security vulnerabilities. To structure this evaluation, a risk assessment matrix should be used to systematically score these factors and generate an overall risk level.

This assessment, which should be conducted with input from mental health professionals and other subject matter experts, directly informs the necessary mitigation measures. Depending on the determined risk, actions could range from increased supervision and mandatory counseling to reassignment or the temporary removal of the officer's access to firearms and tactical systems.

When law enforcement is involved, what are the goals of an interrogation?

Mr. D'Ambrosio: An interrogation seeks to ascertain the methods, motives, and identities of criminals, as well as the identity of victims. It is an important function of a criminal investigation where suspects are questioned to obtain information that will aid in a conviction. The goals of an interrogation include obtaining a confession. While not the only goal, a confession can be a significant piece of evidence. Secondly, gathering evidence. Interrogations aim to uncover facts and details about the crime. Thirdly, identifying participants. It helps to determine who was involved in the crime. And lastly, exonerating the innocent. It provides an opportunity for a person to clear their name.

How do you mitigate risks involving officers under personal or financial stress?

Mr. D'Ambrosio: Mitigating risks involving officers under personal or financial stress requires a proactive and compassionate approach. This includes monitoring officers for any significant behavioral changes, reviewing HR and IA records for any flags or concerns, and coordinating with the agency's wellness programs to provide access to counseling and financial planning. Increasing supervision and temporarily restricting access to sensitive information or systems may also be necessary in certain situations, always ensuring that any actions taken are in accordance with agency policy and legal requirements, and that the officer's well-being and due process rights are protected.

Law Enforcement Misconduct and Compliance Risks

With response processes in mind, this is a good time to address your questions about misconduct and compliance risks.

How do you handle misuse of law enforcement databases?

Mr. D'Ambrosio: When handling the misuse of law enforcement databases, the very first thing we do is jump into the system logs to see what actually happened. We need to confirm if someone really did something they shouldn't have and figure out how big the problem is. A highly effective proactive measure is to configure an automatic alert for when an officer queries themselves, as this is a common form of misuse. This alert can serve as the predication to initiate a review and can even be set to immediately disable the user's access upon a self-query. From there, I check those lookups against their actual case work—you know, is there a legitimate reason they were searching for that person or was it something else?—while meticulously documenting all findings including user ID's, timestamps, and the specific data accessed. Following verification, the next crucial step is to consult agency policy and

legal counsel to determine the appropriate course of action. Based on the severity of the violation and established protocol, the matter would then be escalated to IA, OPR, or OIG, or the appropriate chain of command. Throughout this entire process, the primary objectives are to ensure the integrity of the system logs, prevent further unauthorized access, and uphold the privacy of individuals whose information may have been compromised.

How do you handle reports of fraternization with criminals or gang-affiliated individuals?

Mr. D'Ambrosio: So, if a report comes across our desk that an officer might be getting a little too friendly with known criminals or gang-affiliated individuals, the very first call we make is to internal affairs or OIG. We need to let them know what's going on and make sure our investigation doesn't accidentally step on any toes or interfere with something they're already working on. They can immediately address preliminary questions, such as running records checks on the associate, to see if they are a wanted person or appear in a gang or terrorist database. They can also help determine the context of the encounter. Was it on or off duty, and could it be related to the officer's official assignment? This initial coordination is vital as it can quickly establish whether further inquiry by the insider threat team is necessary or if IA will pursue the matter unilaterally. If the inquiry proceeds, the next step is to meticulously document the original allegation and attempt to verify the report through independent sources like surveillance footage, social media, or witness statements. This involves coordinating with the Criminal Intelligence unit and reviewing the officer's communications. The process culminates in a comprehensive risk assessment to determine the potential threat posed by the association, which may lead to a formal interview with the officer. Throughout every step, the integrity of ongoing investigations and the protection of sensitive information must be the top priority.

Describe your experience with cross-agency information sharing.

Mr. D'Ambrosio: I've experienced coordinating with federal, state, and local law enforcement partners on various investigations and I'm thoroughly familiar with 28 CFR, Part 23 and its requirements for collecting, retaining, and disseminating criminal intelligence information. My approach is guided by principles like need-to-know, mission-to-know, proper classification and handling of information, secure communication protocols, and ensuring data integrity. I meticulously document all instances of information sharing, including the date, time, recipient, purpose, and information shared. I'm also familiar with using formal agreements like Memorandum of Understanding (MOUs) to govern information sharing, relationship between agencies, outlining the scope of the sharing, security requirements, and data usage

restrictions. For instance, in a past investigation involving a potential terror threat, I coordinated with the FBI's Joint Terrorism Task Force (JTTF) sharing relevant intelligence information in accordance with established protocols and legal guidelines.

Describe your understanding of 28 Code of Federal Regulations (CFR), Part 23 and how it applies to insider threat hub activities.

Mr. D'Ambrosio: 28 CFR Part 23, also known as the Criminal Intelligence Systems Operating Policies, establishes guidelines for the operation of criminal intelligence systems, funded as a whole or in part by the Department of Justice. It governs how criminal intelligence data is collected, retained, and disseminated to ensure that the information is accurate, relevant, and necessary to a legitimate law enforcement purpose, also providing guidance on privacy protection and the rights of individuals who are the subject of intelligence gathering. My understanding is that it is critically important for safeguarding individual rights while ensuring that law enforcement agencies have the tools they need to prevent and investigate crime.

In insider threat inquiries, 28 CFR Part 23 applies when the inquiry involves a collection, retention or dissemination of criminal intelligence information, ensuring that the information is collected only with reasonable suspicion, retained only as long as relevant, and disseminated only to those with a need-to-know. I'm committed to complying with 28 CFR Part 23 in all of my activities.

Competencies and Tools for Insider Threat Hub Team Members

It's also important to understand the competencies and tools required of law enforcement personnel to perform their role in insider threat hub teams.

How do you balance officer privacy with investigative needs?

Mr. D'Ambrosio: Balancing officer privacy with investigative needs is a critical ethical and legal consideration, and my approach would be guided by several principles. These include strict adherence to agency policies and relevant laws, ensuring proper legal authority for any investigative action, accessing and reviewing only data directly relevant to the specific insider threat concern—a need-to-know—and employing the least intrusive investigative methods necessary to assess the threat. Transparency and meticulous documentation are also crucial, along with seeking oversight from legal counsel or a designated privacy officer. It's essential to remember that officers have a right to privacy and any intrusion on that right must be justified and conducted with the utmost respect for due process, ensuring the intrusiveness of the investigation is proportional to the severity of the potential threat.

What tools are used in a law enforcement environment?

Mr. D'Ambrosio: I have experience using a variety of tools commonly found in law enforcement environment, including records management systems for managing case files and incident reports, and computer-aided dispatch for monitoring calls for service and tracking officer locations. I'm also familiar with reviewing NCIC-333 access logs to identify unauthorized database queries and user activity monitoring tools to monitor user activity on law enforcement systems. Furthermore, I understand how security information and event management systems can be used to detect potential security threats, and I have experience using license plate readers data to track vehicle movements, and video management systems to review surveillance footage. I'm also proficient in using insider threat case management platforms, social media analysis tools, and link analysis software to identify potential threats and gather intelligence, in addition to standard office software like Microsoft Office suite.

How do you prioritize multiple insider threat cases within a hub?

Mr. D'Ambrosio: Prioritizing multiple insider threat cases within a hub requires a systematic and risk-based approach. Cases involving an imminent threat of violence to self or others or potential for harm to the public would be given the highest priority. This includes cases involving access to weapons, threats of violence or indicators of mental instability, as well as a compromise of critical law enforcement systems or data. Cases involving the potential compromise of ongoing investigations, potential violations of public trust or ethical misconduct, and potential long-term risk to the agency also require high priority. I would use a risk assessment matrix or similar tool to systematically evaluate these factors and assign a priority level to each case, ensuring that the most pressing threats are addressed promptly and effectively.

How do you handle a situation where a supervisor attempts to block your investigation?

Mr. D'Ambrosio: That's a really tricky and serious situation. If it feels like a supervisor's getting in the way, the first thing we have to do is figure out why. It is important to make a clear distinction. You have to ask, are they actively trying to shut this down—which is obstruction and a huge deal—or do they just disagree with the direction? Maybe they don't see the evidence the same way you do, and that's a different kind of conversation, and as such not supportive of the investigation going forward.

The phrase "attempting to block" infers obstruction and this must be handled differently than simple disagreement. If the supervisor is merely unsupportive, due to a disagreement over the justification the appropriate initial response is to calmly and

respectfully cite the relevant agency policy, or legal authority that supports the investigation and explains its necessity. However, if the supervisor's actions are determined to be active obstruction, the response must be immediate and formal.

You must meticulously document the supervisor’s actions, including the date, time, location, and specific statements made. This documentation should be immediately provided to the insider threat hub lead to notify them of the interference. If the obstruction persists, the matter must be elevated through the established administrative or command level channels with referral to IA, OPR, or the OIG. Throughout this entire process, it is essential to see guidance from legal counsel to protect the integrity of the investigation and ensure all actions are appropriate while remaining professional and focused on protecting the agency from harm.

Conclusion

I’d like to wrap up this Law Enforcement and Insider Threat information session by thanking our Law Enforcement representative for joining us today. He really helped us summarize the role Law Enforcement personnel, like himself, play in deterring, detecting, analyzing, and mitigating potential insider threats.

Mr. D’Ambrosio: It was my pleasure. Thank you for having me.

We now know that Law Enforcement personnel provide support that is invaluable to Insider Threat Hub teams and greatly benefits risk mitigation efforts.