August 2024

Supporting Materials

SUBJECT: NITAM Briefing Recommended Script

BLUF: This script, prepared by the DOD Insider Threat Management and Analysis Center (DITMAC), assists presenters with preparation and provides a template for use during the 2024 National Insider Threat Awareness Month briefing.

SLIDE 1:

Good morning/afternoon and welcome to the 2024 National Insider Threat Awareness Month (NITAM) Briefing. I am [ENTER YOUR NAME/TITLE] and [DESCRIBE your connection to Insider Threat.]

This briefing is intended for a general DOD audience, and it was prepared for public release. I want to make this presentation engaging and informational for you, so please ask questions throughout the presentation and let me know if anything is confusing so that I can clarify. The presentation should take about 1 hour. NITAM, or National Insider Threat Awareness Month, occurs every September and our goal is to raise awareness of insider threat issues in the DOD to deter, detect, and mitigate the risks associated with insider threats.

Before we get started, let's watch a quick video to introduce ourselves to the topic.

*** Present selected video from the following options:

- DCSA Director Video: Expected August 2024.
- TED-Style Video: DVIDS - Video - The Insider Threat (dvidshub.net)
- Informal and Entertaining Video - DVIDS - Video - Insider Threat (dvidshub.net)

The DOD Insider Threat Management and Analysis Center (DITMAC) developed this presentation in collaboration with insider threat programs across the Department to inform the DOD Community about the pathway toward and risk from insider threats. DITMAC serves as the DOD's premier provider of insider threat support services, and serves as an enterprise capability for reporting from all 43 DOD Insider Threat components. DITMAC is a part of the Defense Counterintelligence and Security Agency (DCSA). Oversight and policy support for the DCSA is provided by the Office of the Undersecretary of Defense for Intelligence and Security (OUSD(I&S)).

This year's NITAM theme is Deter, Detect, Mitigate. The theme comes directly from the 2012 Presidential Memorandum *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, which states:

"This Presidential Memorandum transmits the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Minimum Standards) to provide direction and guidance to promote the development of effective insider threat programs within departments and agencies to ***deter, detect, and mitigate*** *actions by employees who may represent a threat to national security. These threats encompass potential espionage, violent acts against the Government or the Nation, and unauthorized disclosure of classified information, including the vast amounts of classified data available on interconnected United States Government computer networks and systems."*

The Presidential Memorandum set the groundwork for DOD insider threat programs and is considered of foundational importance for insider threat initiatives. Deter, Detect, Mitigate is a key theme that touches every aspect of our mission as insider threat professionals and DOD employees.

The Presidential Memorandum defined threats as espionage, violent acts against the Government or Nation, unauthorized disclosure of classified information, and loss or degradation of Departmental resources or capabilities. It created 26 Minimum Standards for insider threat programs and called for the development of a capability to gather, integrate, analyze, and respond to insider threats. It required insider threat programs to establish a technical capability for monitoring user activity on networks, protected civil liberties and privacy, and called for insider threat awareness training.

Deter. Detect. Mitigate. This presentation is structured based off three key take-aways centered around the theme. The first is DETER, which focuses on "early prevention." It is important to think about what type of workplace culture deters insider threats. We will get into this in more detail in the following slides and provide some tips to create a workplace that effectively deters insider threats.

The second key take-away is DETECT and focuses on the insider threat critical pathway. The critical pathway was developed to help us understand how any of our colleagues could face challenges and stresses that may result in taking an insider threat hostile action. It structures our thinking on the topic based on behavioral psychology and the study of past insider threat incidents. The main question we will answer in this part of the presentation is 'How to identify someone who may be at risk from becoming an insider threat?'

The final key take-away is MITIGATE, which focuses on reporting and responding. Remember: when you see something, say something. Early reporting and/or bystander actions can help to prevent insider threat incidents from happening before they cause harm to the DOD and may help your partners to the left and right discover improved coping mechanism and get the support they need. You will learn how to report an insider threat, what to report, and when to report.

Now, let's get into the presentation.

SLIDE 2:

This is the insider threat timeline which shows several major insider threat incidents that have occurred since 2010 and the legal and regulatory changes that have resulted from those incidents. This is not a comprehensive list. As you can see, insider threat is an evolving discipline, and the DOD is adapting to meet the challenges.

So, what is an insider threat? The 2017 National Defense Authorization Act defines an insider threat within the DOD as "*a threat presented by a person who has, or once had, authorized access to information, a facility, a network, a person, or a resource of the Department and wittingly, or unwittingly, commits an act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or a destructive act, which may include physical harm to another in the workplace*."

Let's break that down a little. This 2017 NDAA specifies that an insider threat can be someone who currently has or previously had access to government information. Remember that even after you stop working for the DOD, classified information is still classified, and you still have an obligation to protect it.

This includes getting a pre-publication review on anything you write and plan to publish about your time in the military. Insider threats can be witting or unwitting, meaning that this definition applies to unintentional actions. Additionally, this definition encompasses a wide range of potential insider threats to include espionage, sabotage, cyber threats, unauthorized disclosure and violence.

One critical incident was the Navy Yard Shooting in Washington, D.C. in 2013. Aaron Alexis, a cleared employee of a contract company and a former U.S. Navy enlisted sailor, shot and killed 12 civilian and contractor personnel that September day. Reviews of the shooting concluded that within the DOD there were gaps in information sharing necessary to identify potential **insider threats**, develop a holistic picture of **risk** posed by insiders, and coordinate actions to mitigate risk. After the shooting, the Secretary of Defense created the DOD Insider Threat Management and Analysis Center (DITMAC) to resolve those deficiencies. The Navy Yard shooting demonstrates the serious and life-threatening consequences that can occur when risks from trusted insiders are not identified, adequately assessed, and completely managed.

[Are there incidents or examples that apply to your organization, unit, or installation? Insert applicable examples to relate to your environment.]

(CONVERSATION STARTERS FOR THIS SLIDE) Now, look at this slide. What incidents on here do you recognize? What do you know about these incidents? How have these incidents shaped or changed the way that you think about your role with the DOD?

***Additional details for each incident are available in the talking points.

SLIDE 3:

Let's begin thinking about the first key take-away: "DETER." An important aspect of deterrence is creating a positive, supportive, and trusted organizational culture. As we will learn later, disgruntlement is one of the common factors as to why someone might exhibit increased behaviors of concern. This slide discusses three common challenges that organizations face, and the next slide offers some ways to solve those challenges.

The first challenge is stress. Stress is incredibly common in the workplace. 94% of American workers experience stress in their workplace and 63% say that they are considering quitting because of stress, showing that stress is often a serious challenge in the workplace. Members of the military face especially high stress levels due to the inherent danger of their occupation. The stress doesn't only have to come from the workplace, either. Stress can include life at home, multiple deployments, and a wide range of other challenges that can result in anxiety and frustration for members of the DOD population. This is why knowing and understanding strategies for managing stress is so critical. We must look out for ourselves and our colleagues because the first folks to recognize significant changes in someone will be those who are around them every day.

Another common challenge is justice and fairness. Employees who perceive their workplace to be fair and just are 4.6 times less likely to commit insider threat behaviors. This is why transparency in the workplace is an important aspect of leadership. If employees view an act as unfair, this perception could cause them to feel disgruntled and disconnected from the DOD and more likely to become an insider threat. Perceptions of a fair employee experience also improve performance by up to 26% and retention

by up to 27%, making this a key ingredient to a positive organizational culture (This is according to a Gartner Research Study and cited in an article in the Harvard Business Review).

The third challenge is communication. Communication is an essential life skill that every employee needs to possess and there are things that management can do to foster better communication as well. Poor communication leads to increased turnover and impacts mission readiness and morale. The next slide discusses strategies for improving communication across an organization and between individuals who are a part of a team.

Now, we will go to the next slide to see some strategies and best practices for fostering a positive organizational culture, focusing on these three challenges.

SLIDE 4:

Challenge #1 – Stress –

One stress management technique is to develop healthy responses to stress. Healthy responses include hobbies, social activities, and exercise. Unhealthy responses are alcohol consumption, eating when you feel stress, procrastination, avoidance of responsibility and social interaction, isolation, and excessive screen time.

Stress can be a response to positive events like buying a house, or negative ones, like a financial setback. Under excessive levels of stress, one may be more likely to make careless mistakes, or even find themselves more irritable. It is well known that getting support for stressors and our responses to stress can be preventative in avoiding bad outcomes.

If you are feeling a lot of stress, make sure to communicate with your supervisor. Have open and honest conversations with your supervisor about what you need to feel comfortable and productive in your job. Often, stress can reduce productivity, so it is in your boss's interest to ensure that you have the support you need to do your job well.

Finally, if you are feeling stress, seek support from family, friends, colleagues, and/or professionals. When you feel overwhelmed, do not be afraid to reach out to others for support. As for managers, you can create a strategy at your organization to encourage these types of positive behaviors. Make yourself open to conversations about stress and host events and talks centered around these healthy habits and aiming to raise awareness of the negative consequences of stress in the workplace.

Remember, it's okay to ask for help when you're feeling overwhelmed by stress. There are resources available to support you, such as therapy, support groups, and crisis hotlines. Reaching out for help can be a sign of strength, and it's an important step in taking care of your mental health. Don't hesitate to seek out the support you need to manage your stress and improve your overall well-being.

If you or someone you know is struggling with stress, resources are available. The National Suicide Prevention Lifeline is available at 1-800-273-TALK (8255). The 988 Lifeline is a national network of local crisis centers that provides free and confidential emotional support to people in suicidal crisis or emotional distress. Military OneSource is a 24/7 gateway to trusted information, resources and confidential help; go to www.militaryonesource.mil or call 1-800-342-9647.

[Highlight some stress-management techniques or services available through your workplace.]

[Ask the audience for some stress coping techniques that they employ for themselves.]

Challenge #2 – Justice and Fairness. Best practices for justice and fairness naturally center on supervisors and management and the practices they employ. Supervisors should ensure that employees are informed about important developments happening in the workplace.

Employees also need to feel supported. Sometimes the job of a supervisor is to know what their employees need to get the job done most effectively. At the same time, it's also important for the organization to hold leaders and managers accountable for promoting a culture of justice and fairness in the workplace. Leadership should resolve workplace conflicts by promptly addressing and resolving them in a fair and impartial manner. This can mean ensuring all personnel are held to the same standards, treated in the same way, or given the same opportunities according to their workload and capacity.

Additionally, all employees should receive a fair chance at internal opportunities. The workplace must ensure that employees feel that their contributions are recognized. Examples of employee recognition efforts are presentation of awards, certificates, or simply a private conversation or public recognition of their efforts and contributions.

At the same time, employees have a role in all these practices too. Employees can share news when it is appropriate and authorized to do so. They can also support one another and recognize each other's contributions.

[Use this is an opportunity to highlight some initiatives that your workplace has undertaken to promote and encourage justice and fairness. What should folks do if they perceive a practice as unfair or unjust? How can employees work with their teams and supervisors to build a culture of fairness?]

Challenge #3 – Communication – Communication needs to be a part of every workplace because without it, problems can become worse over time. Communication should be clear and concise to communicate ideas efficiently and in a way that the other is able to understand. Being clear and concise will make it easier for others to understand your feedback, which is important if you want your input to create change and reach a broad audience at your organization.

It is also important to practice active listening. Active listening makes others feel heard and it is important because communication is a two-way street. Here are some tips for active listening. Active listening involves giving the speaker your full and undivided attention. It involves clearing your mind of distractions, judgements, and counterarguments. Avoid the temptation to interrupt with your own thoughts. Show open, positive body language to keep your mind focused and to show the speaker that you are really listening. Also, when active listening, rephrase or paraphrase what you have heard when making your reply and ask open-ended questions designed to encourage additional conversation.

Understanding the communication systems of your organization is critical for communicating effectively because not using proper channels could mean that your valuable feedback will be unintentionally ignored.

Understanding your own self is a part of knowing who you are as a person and how you react in various situations. If you can understand the reasons for your actions or reactions, it will be easier to articulate your position to others and ask for change.

Now, think about how our organization creates opportunities for feedback and dialogue. [What does your organization do to promote healthy and open lines of communication? How can someone make recommendations or improve communication within their team/organization? Consider things such as climate surveys, feedback methods, office hours, open-door policies, etc.]

SLIDE 5:

The next key take-away is "DETECT," which focuses on how we understand the question "What is an insider threat?." [OPEN Discussion for audience to answer the question.]

Let us remember that an insider threat is any trusted insider who presents a risk to DOD assets including personnel, facilities, information, and equipment.

It is also important to remember that the people who commit insider threat actions are our coworkers. They are valuable human beings with whom we have relationships. It is important to remember that the DOD's strategy on insider threats is not about turning people in, it is about turning them around. The DOD is focused on risk factors, readiness, and impact on the mission. The bottom line is protecting our mission and our people, above all else.

On this slide, you can see the Critical Pathway to insider risk, or CPIR. The CPIR is a model that shows the social, economic, political, cultural, and organizational context to insider threat behaviors. This pathway can help us to understand why someone could become an insider threat and the stages of development that a person goes through that contribute to those behaviors. The Pathway starts with a person's personal predispositions. These predispositions do not mean that someone will become an insider threat, but they show areas that may contribute to or increase someone's risk of concerning behaviors. These are the attributes people bring with them and include things like bias and perception based upon life factors to date. These personal predispositions factor into the person's "baseline" behaviors and activities.

Stressors come in many shapes and sizes. Everyone experiences stress throughout the course of their life to varying degrees. The potential risk is how people cope with those stressors and what protective factors they may have in place. Having a positive work culture or home environment may help many people to offset stressors. However, there can be times when significant challenges in personal predispositions and a lack of coping mechanisms can result in those stressors driving someone further down the CPIR. We want to intervene as early in the pathway as possible, and you can support your friends, family, and colleagues at many points before they reach insider threat behaviors. So when you see someone experiencing stress, letting them know you are there for them and offering them support can be a positive mitigator.

An important part of the critical pathway is understanding behavioral indicators. Typically, we will see behavioral indicators manifest as a result of stress, and they appear as a deviation from the individual's baseline. There are dozens of possible behavioral indicators, but a few examples are irregular interpersonal interactions, changes in work performance, and unusual displays of anger. When someone has a dramatic change in their personality that expresses itself through any of the behavioral indicator categories, they may be at an increased risk of becoming an insider threat.

The fourth compounding factor is maladaptive organizational responses which occur when an organization responds to predispositions, stressors, and/or concerning behaviors in a manner that exacerbates the potential for a hostile act. This can happen through lack of action, insufficient action, or overreaction. Units, command teams, and other types of organizational leadership must be prepared to respond appropriately when facing servicemembers or employees showing signs of being on the critical pathway.

[This is a good spot to stop and share an example of how someone can move along the critical pathway, in addition to or instead of the one provided below.]

Let's take the example of Benedict Arnold. Benedict Arnold provided information to the enemy during the American Revolutionary War. He had personal predispositions such as being a show-off, suffering from crippling physical ailments, and was affected by war injuries.

Arnold had numerous stressors that made him more likely to move down the critical path including family deaths, paternal alcoholism, professional reversals, lawsuits, and significant financial stressors.

Arnold exhibited concerning behaviors such as frequent fights and being arrested multiple times. He was relieved for insubordination, wrote a petulant letter to Congress expressing feelings of victimization, insulted members of his court martial, and was convicted of misdemeanors, to name a few. This feeling of being wronged and carrying a grievance is another indicator that a person could be going further down the critical path.

In the end, Arnold unsuccessfully planned to surrender West Point to the British, defected to British forces, and led a British attack on the American forces that he had previously commanded.

Arnold's actions represent one type of hostile act committed by an insider, however, there are many different types of hostile acts broadly categorized as either violence or unauthorized disclosure.

Unauthorized disclosures are broken into four major categories: Public Domain, Data Spill, Espionage, and Improper Safeguarding.

Can anyone provide an example of a public domain unauthorized disclosure? (Allow audience to answer.) A public domain unauthorized disclosure is when someone releases classified information or CUI into the public domain, which includes podcasts, print articles, internet-based articles, books, journals, speeches, TV broadcasts, blogs, social media posts, etc. An example of this is if someone published a book about their experiences in the DOD and accidentally included information about a classified government program. If the book is published, and hundreds or thousands of copies are sold across the country, this could cause serious damage to the government, our reputation, and the American people.

One mitigating factor for an example like this is pre-publication review which should be conducted for any media being published to the public domain from a clearance holder or former clearance holder. Pre-publication review can help to identify information that should be removed before publication to protect the classified information and CUI of the DOD. [Discuss procedures or processes that are unique to your organization.]

Does anyone have an example of a data spill? (Allow audience to answer.) The next type of unauthorized disclosure is a data spill which is the willful, negligent, or inadvertent disclosure of classified information or CUI to an information system not authorized at the appropriate security level or not having the

required CUI protection or access controls. Imagine if someone was texting their coworker and included CUI or secret information in a text message or over an unsecured phone line. Text messaging and phone calls that communicate classified or CUI information over unapproved systems are considered unauthorized disclosures and need to be reported, even if both the sending and receiving parties have the appropriate classification level, signed NDAs, and a written and recorded need-to-know.

The next category is espionage – who can provide an example of this category? (Allow audience to answer.) Espionage involves activities designed to obtain, deliver, communicate, or transmit classified information or CUI intended to aid a foreign power. If you are approached by someone asking for government information whether that is CUI or classified information, you must be vigilant because they may be an agent of a foreign power. Willingly giving them this information is considered espionage, which carries serious consequences.

Counterintelligence professionals are critical to the detection, deterrence, and neutralization of espionage activities that threaten national security. Their expertise, confidentiality, coordination, and legal compliance make them an essential resource for reporting possible espionage. You can report to Counterintelligence by contacting a counterintelligence agent, reporting your issue in iSalute, or by calling 1-800-CALL-SPY (1-800-225-5779) [CONUS ONLY].

Finally, what is an example of improper safeguarding? (Allow audience to answer.) Improper safeguarding involves using inappropriate measures and controls to protect classified information or CUI. An example of this is if someone leaves classified information in an unapproved space like a restaurant or bathroom without personally guarding that information. Even if the information is locked up in a safe or cabinet, it is still an unauthorized disclosure if the safe or cabinet is not specifically approved to store that information.

Targeted Violence is also an example of an insider threat action. Targeted Violence is using physical force to hurt, harm, damage, or kill someone or something. It includes assault, harassment, sexual assault, and sexual harassment, as well as mass shootings and armed violence. The shooting at the Washington Navy Yard that we mentioned earlier is an example of a violent mass shooting insider threat incident that resulted in the deaths of 12 DOD personnel.

SLIDE 6:

The critical pathway is not irreversible. We can support ourselves or others that may be headed down the path toward concerning behaviors and insider threats. So, what do you do when you recognize that someone is going down the critical pathway?

This begins the final key take-away of this presentation: MITIGATE, which can be done by responding and reporting. When you see someone along the critical pathway, whether they have personal predispositions, are experiencing stressors, are demonstrating concerning behaviors, or if you believe they are an insider threat, this slide prescribes some actions you can take to mitigate the risk and get that person to move away from the critical pathway. Using stabilizers can help those in need.

[Option: Describe personal experiences that you may have of assisting someone off the critical path or someone assisting you off the critical path.]

For example, if one of your coworkers is feeling angry and depressed because of the loss of a loved one, some actions you can take are to provide them with resources and demonstrate that you care by talking to them and avoiding stigmatizing them. You can also work with them to develop positive coping strategies such as exercising and finding a new hobby.

Keep in mind that if their behavior makes you believe that they are emotionally unstable, irresponsible, dysfunctional, violent, paranoid, bizarre, anti-social, or aggressive, you are required to report this information to security, as that is the point at which it meets the threshold for reporting. Even if the behavior does not meet the threshold, it is still important to communicate the nature of the problem to supervisors and relevant personnel so that the individual can get the support that they need.

[Walk through some of the examples in each category and ask the audience for their own examples.]

SLIDE 7:

Reporting potential insider threats is extremely important. When you see behaviors of concern, your priority is to protect DOD information whether it is CUI or classified information. If the information is online, close the website and do not look at the information after you have identified that it is or may be classified. If the information is in a physical form, personally protect the information and attempt to move it to a storage area approved for storage at or above the information's classification level.

The second step is to report the details to security as soon as possible so that they can properly handle the situation and ensure that the information is protected, assess the situation, and apply mitigation measures. You can report to the insider threat capabilities at your department or agency. You may additionally report the insider threat information directly to the DITMAC through the DOD Insider Threat Reporting Portal.

[Insert details about your organization and reporting. Add details to the slide by providing Insider Threat or Security contact details and paths. Ask the audience – Do you all know what the proper reporting channels are for our organization? Where would you go if you encountered an insider threat? Who would you talk to? What channels are available to you?]

Reporting is required, whether the incident is intentional or inadvertent. Individuals who commit an insider threat incident are required to self-report. Those who encounter an insider threat incident are also required to report. Classified information discovered on the internet or in physical form must be reported.

It is your duty to report when you see an insider threat. You could be the reason that we are able to turn someone around. You could be the one thing that went right in someone's life that caused them to come off the critical pathway. When you report an insider threat, the DOD can get someone the support and resources that they need.

Feel confident that the DOD is protecting you and your coworkers' privacy rights and civil liberties. The procedures used and the processes followed are carefully managed with maximum sensitivities and considerations for those involved. We must take a proactive approach to insider threats to ensure the safety and security of all of us.

[Add language and examples for your service/organization.]

For example, the DCSA DITMAC only collects information from lawful sources and in full compliance with privacy and civil liberty protections. Insider threat programs look at the holistic picture and the combinations of behaviors that indicate an emerging risk and works to prevent that risk from becoming a threat.

SLIDE 8:

In conclusion, remember the three key take-aways. DETER. DETECT. MITIGATE.

You can DETER the insider threat by incorporating best practices into your workplace and ensuring that your culture is one where people feel that they have support in stressful situations, justice and fairness, and a solid communication structure. Anyone from top leadership all the way down to the newest recruit can take actions to improve in these areas and support one another.

You can DETECT insider threats by understanding the critical pathway and the reasons that someone might display concerning behaviors. Be on the lookout for behavioral indicators and understand the baseline of your coworkers so that you can notice when their actions take a dramatic turn.

Finally, remember that you can MITIGATE the insider threat using stabilizers and by intervening to provide support and understanding to your coworkers before they reach a reporting threshold or move further down the critical pathway. In the case that an insider threat does develop, you now know that you can report through the proper mechanisms.

Remember that you can contact your component insider threat hub at any time for questions and to request support on insider threat matters. The DITMAC contact information is also available on this slide, and we can help facilitate coordination with the appropriate insider threat points of contact. We encourage you to participate in the 2024 DCSA NITAM Conference in person or virtually on September 9th & 10th, which will be held in Arlington, Virgina.

Additionally, if you see an insider threat or concerning behavior, you can report it through the DOD Insider Threat Reporting Portal.

If you want to learn more, you can take the online trainings available at the CDSE website. You can also find the useful and informative BTAC bulletins on the DITMAC page of DCSA.mil.

Remember that while NITAM is only in September, insider threats exist year-round and are constantly changing and evolving. Be sure to stay smart on insider threat and remain vigilant to safely and effectively deter, detect, and mitigate the treats that can be caused by trusted insiders.

Thank you for your time and attention. We have a brief survey that we would like you to please fill out about the presentation today. The survey will allow us to improve this presentation for next year. Please provide detailed and honest feedback. We will review your feedback because we want to make this presentation better and better every year!