DoD Insider Threat Program

– Best Practice –

5.1 Processes: Getting Started

Rev 1

01/08/2018

The Under Secretary of Defense for Intelligence is the Senior Official for Insider Threat

Do you have any questions, comments, or concerns on this topic or others? Would you like to add your component to this Best Practices Edition?

If so, please contact the DoD Counter Insider Threat team at **osd.pentagon.ousd-intel.mbx.dod-counterinsiderthreat@mail.mil**

NOTE: The Best Practices series will deliberately be anonymized so that responses are not attributed to a participating Component with exception to the DoD Insider Threat Management Analysis Center (DITMAC), the Center for Development of Security Excellence (CDSE), and the National Insider Threat Task Force (NITTF). The information in this booklet is offered as guidance. It does not convey a task or directive. Each Component conforms to multiple and varying authorities. As such, each Component needs to confer with their Office of General Counsel (OGC) to verify their procedures conform to legal pronouncements.

Purpose:

Data and information were compiled from several selected DoD Components that offer field tested procedures that produced credible results. These methods, techniques, and professional procedures are offered to Components to assist in their efforts to improve their respective Insider Threat Programs (InTP). All best practices are informational, and individual programs should ensure any implementation actions are in compliance with their Office of General Counsel (OGC) and organizational policies before implementation.

Description:

This edition will provide Insider Threat Programs with the basic tenets necessary to get their programs started. The participating Component in this Best Practices edition has successfully overcome the challenges of getting their program started and has reached a higher level of maturity than others. The questions posed in this Best Practice edition are basic 101 questions surrounding the functional requirements of an Insider Threat Program and how they were implemented.

If you have additional questions that you would like answered in "Getting Started", please reach out to the DoD Counter Insider Threat team.
We anticipate expanding this edition and updating it as needed

Table of Contents

Q1. Where is your InTP embedded within your Component (e.g. a certain staff section or staff entity)?

Component Response:

Our Insider Threat Program is aligned under the Intelligence Directorate, separate from all other programs. The program manager is a direct report to the Senior Intelligence Officer, and has direct access to Senior Leadership.

Q2. Can you describe how your InTP has broken out the functional requirements? How is your InTP designed?

Component Response:

The Agency's Insider Threat Program, established in March 2014, consists of three core elements. The Insider Threat Hub, the Insider Threat Case Management Council (CMC), and the Insider Threat Council (ITC).

The Insider Threat Hub

The Hub analyzes multiple data sets received daily from Human Resources, Security, Counterintelligence, Cybersecurity, as well as external sources to identify behavior indicative of a potential insider threat.

To accomplish this the Hub utilizes behavioral analysis to establish the "business normal" of all agency employees, and user activity monitoring (UAM) based off of established triggers.

Hub analysts review behavior or events that have been flagged as being anomalous, placing them into one of three (3) categories.

- Category One – Incidents that can be validated by the analyst as being routine, and not requiring further analysis or mitigation
- Category Two – Incidents that involve three (3) or more potential risk indicators (PRI). These incidents are immediately raised to the attention of the Insider Threat Program Manager, who can authorize the analyst additional analytical protocols to determine if the incident needs to be raised to the CMC for response/mitigation.
- Category Three – Incidents that involve five (5) or more PRI or any indicator that is indicative of a potential workplace violence incident.

Incidents transferred to the CMC must be responded to or mitigated in order to reduce the risk to the agency.

Risk is determined by the Hub, while response/mitigation is the responsibility of the CMC. Actions taken by the CMC are taken into account by the Hub when re-evaluating associated risks.

The Hub tracks all CMC actions, and only closes an incident after all potential risk has been reduced or accepted by agency leadership.

The Case Management Council

The Case Management Council is responsible for responding to or mitigating insider threat risk identified by the Hub. These risks are associated with an individual or a process that an insider may attempt to exploit.

The CMC is comprised of subject matter experts (SME) from Human Resources, Security, Counterintelligence, Special Programs, General Council, Cybersecurity, Acquisitions, Internal Review and Equal Opportunity.

Once an incident has been referred, the SMEs of the CMC determine which of the action arms are best suited to address the concern. The CMC then places the incident into one of four mitigation tiers and provides the Hub with continuous updates until the Hub determines that the risk has been reduced or accepted by agency leadership.

Note: Due to the sensitive nature of the mitigation tiers, they have been omitted from this overview. If needed, the Insider Threat Program Manager is available to discuss the tiers if deemed appropriate.

The Insider Threat Council

Chaired by the Director of Technical Intelligence, who serves as the Insider Threat Senior Executive the Insider Threat Council (ITC) provides oversight and guidance to the Insider Threat Program.

The ITC is comprised of Division Chiefs from Human Resources, Security, Counterintelligence, Special Programs, General Council, Cybersecurity, Acquisitions, Internal Review and Equal Opportunity.

In addition to providing oversight, the ITC serves as a forum for collaboration, information sharing, policy review and development, and strategic planning for the protection of proprietary information, personnel and resources; improving mission assurance through intra-agency, cross-disciplinary synchronization.

Q3. What was your initial plan for designating and filling leadership positions for your InTP? How did you identify your InTPs Senior Official? Program Manager?

Component Response:

Our Senior Official is our Senior Intelligence Officer (SIO). This designation was made based on existing functions within the Agency. Our SIO is responsible for Security, Counterintelligence, Special Access Programs and Program Protection.

The SIO selected the Program Manager based on his background and training in law enforcement, counterintelligence and cyber forensics.

Q4. Can you describe your policy development process and who was involved in writing, coordinating, and publishing your InT policy? What made your process successful? What difficulties, if any, did you encounter in getting your InT Policy endorsed and how did you overcome them?

Component Response:

The Program Manager organized and led an Insider Threat Process Development Team comprised of representatives from Security, Special Access Programs, Human Resources, Program Protection, Counterintelligence, General Counsel, Privacy Office, and Equal Opportunity and Diversity Management.

This approach ensured the development of the program was transparent, everyone's ideas were considered, and all concerns were addressed.

Q5. How did your Component establish your InT Implementation Plan, to include the process, who was involved, and what made your process successful? What difficulties, if any, did you encounter in getting your InT Implementation Plan endorsed and how did you overcome them?

Component Response:

The Program Manager organized and led an Insider Threat Process Development Team comprised of representatives from Security, Special Access Programs, Human Resources, Program Protection, Counterintelligence, General Counsel, Privacy Office, and Equal Opportunity and Diversity Management.

This approach ensured the development of the program was transparent, everyone's ideas were considered, and all concerns were addressed.

Q6. What was your process for determining your desired direction for your UAM capability and who was involved? How did you decide what UAM tool to use?

Component Response:

During the development of the program, leadership insisted that all networks, regardless of classification would be monitored for potential insider threats. Based on the cost, and additional resources associated with a commercial UAM tool, the Agency utilized existing toolsets, already deployed on all Agency networks. The combined capabilities of these tools met the requirements established for UAM.

Data collected by the UAM tools is then fed into the Insider Threat Hub where it is analyzed on an isolated network, then correlated and compared with data from Human Resources, Security, Program Protection and Counterintelligence.

Hub analyst are then able to place all anomalies into context, and refer unresolved incidents to our Case Management Council for further mitigation and response.

Q7. If your UAM tool was an unfunded requirement, how did you succeed in getting resources?

Component Response:

Our UAM tools are part of our operating budget. The Agency did fund, through existing program dollars to development and deployment of an isolated network, and the purchase of analytical software.

Q8. How did your Component build an InT analytic and response capability to gather, integrate, and analyze InT information? How are your InT personnel trained in conducting InT response actions?

Component Response:

The Insider Threat Hub, managed by the Program Manager, analyzes multiple data sets received daily from Human Resources, Security, Counterintelligence, Cybersecurity, as well as external sources to identify behavior indicative of a potential insider threat.

To accomplish this, the Hub utilizes behavioral analysis to establish the "business normal" of all agency employees, and user activity monitoring (UAM) based off of established triggers.

Hub analysts review behavior or events that have been flagged as being anomalous, placing them into one of three (3) categories.

- Category One – Incidents that can be validated by the analyst as being routine, and not requiring further analysis or mitigation
- Category Two – Incidents that involve three (3) or more potential risk indicators (PRI). These incidents are immediately raised to the attention of the Insider Threat Program Manager, who can authorize the analyst additional analytical protocols to determine if the incident needs to be raised to the Case Management Council (CMC) for response/mitigation.
- Category Three – Incidents that involve five (5) or more PRI or any indicator that is indicative of a potential workplace violence incident.

Incidents transferred to the CMC must be responded to or mitigated in order to reduce the risk to the agency.

Risk is determined by the Hub, while response/mitigation is the responsibility of the CMC. Actions taken by the CMC are taken into account by the Hub when re-evaluating associated risks.

The Hub tracks all CMC actions and only closes an incident after all potential risk has been reduced or accepted by agency leadership.

The CMC is responsible for responding to or mitigating insider threat risk identified by the Hub. These risks are associated with an individual or a process that an insider may attempt to exploit.

The CMC is comprised of subject matter experts (SME) from Human Resources, Security, Counterintelligence, Special Programs, General Council, Cybersecurity, Acquisitions, Internal Review and Equal Opportunity.

Once an incident has been referred, the SMEs of the CMC determine which of the action arms are best suited to address the concern. The CMC then places the incident into one of four mitigation tiers and provides the Hub with continuous updates until the Hub determines that the risk has been reduced or accepted by agency leadership.

Note: Due to the sensitive nature of the mitigation tiers, they have been omitted from this overview. If needed, the Insider Threat Program Manager is available to discuss the tiers if deemed appropriate.

Q9. Can Components reach out to you directly for assistance in getting their programs started?

Component Response:

Absolutely, I am available upon request. Due to the anonymity bestowed upon these best practices, please reach out to OUSD(I) if you would like to get in touch with us directly.