Webinar Questions and Answers

Insider Threat for DoD Security Professionals

Webinar guests submitted several questions before and during the **23 April 2015, Insider Threat for DoD Security Professionals** session. The following responses are provided by Mr. Hopkins and the Center for Development of Security Excellence (CDSE):

Question: What will motivate other agencies to participate in information sharing?

Answer: Please note that my response is focused on actions taken by a component; that said, components will conform to the requirement to establish an insider threat program, and the effectiveness of that program will be contingent on the degree of information shared to facilitate the collection and analysis of information relevant to insider threat behavior or activity. Also note that policies at the DoD and component level are to be reviewed and revised to mandate appropriate information sharing. This is not a negotiable task; everyone has to do it.

Question: Will thresholds for triggering insider threat concerns/attention be developed across the Interagency or agency-by-agency?

Answer: Unable to answer this question at this time; still being worked. I believe that each department & agency will develop their own triggering thresholds but that's to be determined.

Question: How to identify a Sensitive Information breach effectively?

Answer: Please refer this question to your information security expert.

Question: Will the presentation and slides be available on the DSS site as I'm not able to log in to see them?

Answer: The presentation slides, webinar recording, and Q&A will be posted on the CDSE Counterintelligence Webinar Archive page.

Question: What if your command does not have the resources-mental health/Chaplain?

Answer: I am not able to respond to situations that exist at the command or activity-level. The DoD policy I addressed is focused on the requirements for DoD components. The components will be establishing policy and procedures for sub-elements/commands/etc.

Question: What do you mean by TMU/hub?

Answer: DoD Components must establish an integrated capability (or activity or team) to monitor and audit information for insider threat detection and mitigation. This entity will gather, integrate, review, assess, and respond to information derived from CI, security, cybersecurity, civilian and military personnel management, workplace violence, law enforcement, network monitoring, and other sources to identify, mitigate, and counter insider threats.

Webinar Questions and Answers

Question: Does DoD intend to establish a System of Record for Insider Threat?

Answer: Refer to DSS POC for complete answer.

Question: How do the components do the self-assessments?

Answer: The forthcoming DoD Insider Threat Implementation Plan will provide guidance to DoD Components on what entails a self-assessment.

Question: Will employment opportunities be opening up for management of this program at different levels?

Answer: This matter rests solely with the Component Head, not a staff office, in OSD.

Question: Is there a good model to follow in the development of such a program?

Answer: There are several Components that have excellent insider threat programs in operation. We will attempt to highlight them on the DoD Security Policy and Oversight Division (SPOD) webpage. To reach this site you must have access to "Intelink" on NIPRnet (and you must use a CAC/PIV for access). Once on Intelink, enter this URL to get to the SPOD webpage: https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/default.aspx

Once you are on the webpage, look for the "Insider Threat" TAB at the top of the page (far right); click on it, and you will be directed to the Insider Threat page, which we are populating with program information and guidance.

Question: The Insider Threat Program Personnel are required to have a lot of knowledge on different topics, with support from (potentially unavailable) SMEs (not everyone is in a national intelligence agency). The training and knowledge requirements were extremely vague, and the schoolhouses that currently provide that knowledge is limited to national intelligence agencies (e.g. CISAC, JCITA CIAC, etc.). Where can we look for policy on standardized training and professional development for Insider Threat personnel?

Answer: The baseline training topics that need to be brought to the general workforce, and the staff who will work within the insider threat program, will be addressed in the DoD Insider Threat Implementation Plan. This information will guide the development of required instruction within the Components.

Question: What is the lowest echelon in which an insider threat program must be established? As far as the Army goes, does annual Threat Awareness and Reporting Program training requirement suffice?

Answer: I am not able to answer an Army-unique question, and ask that you contact the HQDA Insider Threat POC, in G-3/5/7.

Question: Is there any more funding to offset the additional manpower that it will take to fulfill these new actions?

Webinar Questions and Answers

Answer: At the present time, no funding has been earmarked for additional manpower. The manpower to administer and oversee the component's insider threat program must be re-directed from current organizational assets.

Question: With all of the information given, I am assuming that it will take until least Q4 to have an insider threat program established and possibly Q1 of 2016 for implementation?

Answer: Your assessment or projection must be unique to your situation; as many DoD Components currently have an insider threat program; and others are making progress that will achieve full operations capability before the end of CY 2016.

Question: I know this might sound silly... But would the insider threat program inherently fall to the Special Security Office (i.e. SCI world)? Or can this program be managed by a collateral only office?

Answer: Management of the Component insider threat program will likely not be performed from the SSO community or the SCI community. We anticipate that the program would be best run from the activity's security section. That said, the actual placement for an insider threat program is left to the discretion of the Component Head or Senior Official.

Question: How does the new DoD Insider Threat Policy apply to host nation regarding overseas DoD Installations? Will this drive bilateral agreements and international law changes to facilitate implementation of this new policy?

Answer: This DoD policy has no requirements or impact on a Host Nation. That said, U.S. activities supported by a host nation need to heed the directions they get from the DoD Component in their chain of command concerning an insider threat program.

Question: How will this be used in the future with retention in the Military? Recruiting?

Answer: As far as I can tell, this program will have no impact on recruiting or retention parameters.

Question: Please provide the cost estimator to webcast participants when sending attendance confirmation. Thank you.

Answer: The program cost estimator will be available to all on the DoD insider threat webpage. To reach this site you must have access to "Intelink" on NIPRnet (and you must use a CAC/PIV for access). Once on Intelink, enter this URL to get to the SPOD webpage:

https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/default.aspx

Once you are on the webpage, look for the "Insider Threat" TAB at the top of the page (far right); hit it, and you will be directed to the Insider Threat page, which we are populating with program information and guidance.

Webinar Questions and Answers

Question: How do you suggest the Components apply knowledge management IT aspects to the Insider Threat program? If we need data, it all needs to interact and "speak" for aggregation purposes.

Answer: Please contact your respective CIO staff official regarding this item.

Question: For those Defense Agencies with subcomponents located on military installations (CONUS and OCONUS), does the HUB at the HQ level cover its subcomponents? Or, can the subcomponents feed into the HUB at the military installations level?

Answer: This matter must be address by the Component; OSD does not set implementing standards for subcomponents.

Question: Is the senior official accrediting or who?

Answer: Please provide more information; I cannot answer it as worded.

Question: I understand this forum is more for DoD policy, but the recent DITMAC CONOPS sent out was misleading as far as what was initially briefed on their intent. Do you have any input on this?

Answer: Refer to DSS POC for complete answer.

Question: These programs discussed to this point appear to be heavily focused on "Information" protection - but little information regarding the "physical" element of insider violence. Will additional information be forthcoming from the DoD regarding the physical element of violence?

Answer: Unable to answer; out of my topical area.

Question: Is it also going to eventually draw from the terrorist watch list?

Answer: This remains a possibility; however, authority for DoD components to connect to that database, and the means of connecting to it remain unresolved at this time.

Question: Will OUSDI be pushing out standardized training for Insider Threat similar to what exists for AT/FP? So there is a minimum standard?

Answer: Yes; this does not impact the minimum standard for training; but it will establish a standard training package.

Question: Is IMESA available to the Defense Agencies? Is IMESA limited to Law Enforcement agencies or can Uniformed Security Service personnel utilize it?

Webinar Questions and Answers

Answer: Yes, IMESA is available to Defense Agencies; contact the Defense Manpower Data Center. General obstacles include Components not having Physical Access Control Systems (PACS) that are compatible with IMESA.

Question: The Defense Science Board Task Force on - Predicting Violent Behavior provided some excellent recommendations regarding threat management with regard to physical violence. Is the DoD planning on implementing any of those recommendations?

Answer: Unable to answer; out of my topical area.

Question: Just to revalidate ... Did we hear correct that the OUSDI Implementer to 5205.16 should be out in 2 weeks?

Answer: The final, signed, document will not be out in two weeks. Our goal remains to get the "draft" of the implementation plan to DoD Components for review and comment NLT 15 May 2015.

Question: Where are the specific training requirements for hub personnel identified?

Answer: Baseline topics/subjects will be identified in the DoD insider threat implementation plan.

Question: What training is available in the civil liberties area?

Answer: Unable to answer; out of my topical area.

Question: Will CDSE be developing a training curriculum for Insider Threat Program Managers?

Answer: CDSE has developed a course "Establishing an Insider Threat Program" which covers many of the basic elements required for Insider Threat Program Management personnel. At this time, there are no plans to develop a training curriculum. However – what a great suggestion. We will take it under advisement. Please note that the National Insider Threat Task Force currently hosts Establishing an Insider Threat Detection Program seminar that is an excellent resource for program management personnel.

Question: Who keeps Insider Threat Personnel training records?

Answer: Training records will be retained in accordance with DoD Component guidance/procedures.

Question: I'm sorry; I forgot what is NITTF stands for?

Answer: National Insider Threat Task Force

Webinar Questions and Answers

Question: Good Afternoon, what is the Insider Threat course called that individuals would need to take that access classified. Thank you.

Answer: CDSE provides general Insider Threat Awareness course that has been recommended under Directive One issued by the National Insider Threat Task Force.

Question: In order to test ITPs (and overall security) where are the red teams/threat emulating teams that you can provide points of contacts for?

Answer: For this issue, please coordinate with your servicing intelligence official.

Question: When did this requirement go into effect?

Answer: Officially, it will go into effect when the Implementation Plan is signed. This plan, though, is based on DoD policy issued in September 2014.

Question: Much of this overlaps with Work Place violence? Yet I don't hear anything about that correlation.

Answer: Collaboration is occurring at OSD and needs to occur at activity level amongst staff personnel.

Question: Is the Insider Threat Awareness Training available elsewhere besides the toolkit to provide to command personnel in meeting the initial and annual refresher training requirement?

Answer: Although there are several Insider Threat Awareness courses in the community, CDSE provides the only general Insider Threat Awareness course that has been recommended under Directive One issued by the National Insider Threat Task Force.

Question: Have you seen the MARADMIN on Insider Threat program it has the Security Manager be appointed as the Program manager.

Answer: Unable to answer this question; MARADMIN – what is that?

Question: Will there be a centralized DoD Hub/TMU for Components to feed their information into for consolidated Analyses?

Answer: Yes.

Question: Will the DoD CAF be required to share information with insider threat programs?

Answer: Conversely, the TMUs/hubs and DITMAC will forward their “flags” to the DoD CAF.

Webinar Questions and Answers

Question: Does the .16 policy take a pro-active posture to prevent insider threats or is primarily reactive in nature?

Answer: It provides guidance that employs both proactive and reactive measures.

Question: Will we see funding to support this program sometime in the future?

Answer: To Be Determined based on the identification of needs/requirements and program posture versus other Component priorities.

Question: Is DBIDS the same as IMESA?

Answer: No. DBIDS is an all-inclusive, expandable force protection access control system (i.e., PACS) utilizing biometrics and automatic identification technology. It is designed to verify DoD-produced identification credentials and access authorization of personnel entering military installations or government-controlled areas using machine-based authentication technologies in conjunction with photograph and fingerprint biometric identification.

Question: Is there a train the trainer for this program?

Answer: Not planned at this time.

Question: When can we expect to see the Implementation Plan?

Answer: This draft plan should be in your hands NLT 15 May for you to review and comment. If this timeline is met, the plan should be published NLT 15 July.

Question: Will this program be required to be integrated within ATFP programs?

Answer: This is not a stated requirement, but it makes sense to do so.

Question: Are there any plans to look at the CAF's loss of capability to conduct a full Insider Threat review of adjudication files that was loss upon its consolation? Or additional policy to tie the DOD CAF into an Insider Threat program?

Answer: The DoD CAF will receive funding to hire additional staff to service the anticipated increase in case workload.

Question: Will this be an inspectable program and what inspection will it fall under 107

Answer: At a minimum, the programs will be assessed by: the local insider threat program manager, overseen by the Component Senior Official, monitored by OUSD(I), and subject to NITTF assessment.

Webinar Questions and Answers

Question: What if there are joint programs. How is the requirement initiated and would the requirement fall to all involved, or only DoD personnel?

Answer: Cannot answer this until "joint" is clarified here (multiple Services; or multiple countries).

Question: What is your relationship to components regarding implementation?

Answer: OSD is obligated to provide implementing guidance to the Components; assist as needed; and receive quarterly and annual program status reports.

Question: It does not apply to classified information?

Answer: Yes the insider threat program does apply to classified information, and much more. Insider threat is not exclusive to classified information though.

Question: In the real world as we continue to downsize employees in the security department. Identifying an individual with the title security administrative as the insider threat officer if they are given the authority to make the decisions. Is this feasible?

Answer: This scenario sounds to be dependent on decisions being made at a sub-component level, and OSD is not positioned to comment on this. It's a component level or organizational decision.

Question: In regards to SO management and oversight. Do these responsibilities need to be direct management/oversight?

Answer: Senior Official duties can be delegated; however, the Senior Official will be held accountable that management and oversight is conducted and corrective actions are taken when necessary.

Question: When is IMASA online? And does it do live NCIC checks or are they batched checks?

Answer: IMESA is operational now. PACS must be compatible with and connect to IMESA. IMESA vets identity (using biographic information) authorized to access a DoD installation against authoritative data sources (DEERS, FBI/NCIC wants/warrants, installation data, local population data, and (pending) terrorist screening center data, in real time, not batched.

Question: Is the initial/annual training for cleared personnel the same as training as the counterintelligence that NCIS gives?

Answer: Unable to answer; must defer question to CDSE CI staff.

Question: Since this is an unfunded mandate, who does it and what do they stop doing to make this happen?

Webinar Questions and Answers

Answer: The response to this question must come from the respective Component Head.

Question: How are recurring Risk Assessments conducted within the program?

Answer: In accordance with the DoD Insider Threat Implementation Plan.

Question: What is the expected date of implementation to have an insider threat required?

Answer: National program standards require Departments and Agencies to have fully operational programs NLT December 31, 2016. Accordingly, DoD Components must meet this same timeline.

Question: Is there a recommendation on a budget request for this new program?

Answer: No standardized recommendation can be offered; however, you can utilize the program cost estimator tool found at the SPOD website: https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/default.aspx.

Please note: there were numerous questions from our industry partners regarding the pending update to the NISPOM under Conforming Change 2 (CC2) and attendant Insider Threat Program requirements. Until such time as the update is released, we are unable to comment on program specifics. In the interim, DSS has provided an External Website Notice to provide Information on Pending Insider Threat Program Requirements for Industry. CC2 and/or related Industrial Security Letters are expected to be published within the calendar year and full compliance with the program will be mandated six months from the date of publication.