DSS Monthly Newsletter
May 2017

(Sent on behalf of your ISR.)

Dear FSO,

This is the monthly newsletter containing recent information, policy guidance, security education and training updates. If you have any questions or recommendations for information to be included, please feel free to let us know.

DSS IN TRANSITION (DiT)

The world is rapidly changing and the Defense Security Service (DSS) is changing, too. Where the agency once concentrated on schedule-driven National Industrial Security Program Operating Manual (NISPOM) compliance, DSS is now moving to an intelligence-led, asset-focused, and threat-driven approach to industrial security oversight.

The need for change is clear. The United States is now facing the most significant foreign intelligence threat it has ever encountered. Adversaries are successfully attacking cleared industry at an unprecedented rate. They are using multiple avenues of attack, varying their methods, and adjusting their priorities based on the targeted information they need. As a result, they are upgrading their military capabilities and competing against our economy using the very same information they have stolen from cleared industry.

DSS has recognized this fact and is now moving forward in partnership with industry to design, develop, and pilot a multi-dimensional approach to industrial security oversight. Our goal is to help cleared industry ensure that contracted capabilities, technologies, and services are delivered uncompromised.

To learn more about DiT, watch our April 10, 2017 DiT webinar with industry on Adobe Connect.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

Coming soon! NISS will replace the Industrial Security Facilities Database (ISFD) and the Electronic Facility Clearance System (e-FCL) in the Fall of 2017. NISS will be the system of record for facility clearance information and for submitting Change Conditions packages, among additional features. For information regarding this critical information system transition, please visit the NISS informational webpage.

RISK MANAGEMENT FRAMEWORK (RMF)
FREQUENTLY ASKED QUESTIONS (FAQs)

The NISP Authorization Office (NAO) has posted RMF FAQs on the DSS Website to answer the most commonly asked RMF questions received from Industry over the past months. Specific questions not covered in the FAQs should be addressed to your assigned Information Systems Security Professional (ISSP).

If you have specific questions about the format or content of the FAQs, please provide comments and questions to dss.quantico.dss-hq.mbx.odaa@mail.mil.

ODAA BUSINESS MANAGEMENT SYSTEM (OBMS) ARCHIVE FEATURE

OBMS provides the Contractor Submitter role the ability to archive older versions of Unique Identifiers (UIDs) so that the contractor can effectively manage their records. To archive an UID, perform the following:

1. Log into OBMS, the Contractor Submitter Module, and the Certification and Accreditation Module.
2. Select "Edit an Accreditation."
3. Click the radio button next to the selected UID.
4. Click "Archive Accreditation Package."
5. A pop-up will appear asking "Are you sure you want to archive the selected accreditation?" Click "Submit." The UID will be permanently archived and removed from the queue.

If the UID is in a draft status, it cannot be archived. The contractor will need to contact the DSS Knowledge Center and submit a request to have the draft UID(s) archived. The DSS Knowledge Center can be reached at (888) 282-7682 or via email at dss.quantico.dss-hq.mbx.knowledge-center@mail.mil

For questions or concerns, contact your assigned Information Systems Security Professional (ISSP). For specific OBMS questions, email dss.quantico.dss-hq.mbx.odaa@mail.mil.

UPDATED RISK MANAGEMENT FRAMEWORK
SYSTEM SECURITY PLAN (SSP)

NAO has released an updated SSP Word template for RMF plan submissions. The updated SSP incorporates the feedback received from Industry, and is posted on the DSS RMF Website.

For questions or concerns, contact your assigned ISSP. For specific questions about the format or content of the SSP, contact dss.quantico.dss-hq.mbx.odaa@mail.mil.

UPDATE ON INDUSTRY T5R EXPIRATIONS AND REJECTIONS

The Personnel Security Management Office for Industry (PSMO-I) is currently managing the investigation request inventory in order to stay within our budget authority, with priority being given to requests for initial clearances. This may result in Tier 5 Reinvestigations either terminating from the system or being rejected if a Special Access Program (SAP) Caveat is not identified as described in the February 10, 2017 guidance (available here).

Note: a SAP Caveat applies only where DoD Policy explicitly states an investigation must be conducted at five year intervals for personnel within a certain program. The SAP Caveat does not apply to every person on a SAP, but only specific programs designated in writing by the DoD.

At this time, please do not submit/resubmit for Top Secret reinvestigation unless the requisite SAP Caveat criteria is met and clearly identified. PSMO-I will provide additional guidance on submission of requests for Non-SAP Caveat Tier 5 Reinvestigations through public communications and a system of record messaging. To facilitate the change in periodicity of Top Secret Reinvestigations and clearance timeliness issues, the Office of the Undersecretary of Defense for Intelligence (OUSD(I)) signed a memorandum (dated December 7, 2016) reminding DoD Components that personnel security clearances do not expire. Individuals with current eligibility in the Joint Personnel Adjudication System (JPAS) should not be denied access based on an out-of-scope investigation. This memorandum is available on the DSS website and was disseminated to non-DoD NISP signatories on March 28, 2017.

KNOWLEDGE CENTER PCL INQUIRIES EXTENDED CLOSURE

PCL inquiries (option #2) to include e-QIP authentication resets of the DSS Knowledge Center will be closed from Monday, June 19, 2017 through Tuesday, July 4, 2017. DSS regularly assesses its execution strategy against available resources. In order to reduce processing timelines of initial investigation requests, Knowledge Center services will be temporarily suspended. The extended closure enables PSMO-I to focus on processing the inventory of investigation requests, with an anticipated substantial improvement to timelines for processing initial investigation requests and relative improvement to requests for periodic reinvestigation. Normal operations for PCL and e-QIP inquiries will resume on Wednesday, July 5, 2017. As a reminder, answers to common PCL inquiries are available on the DSS website.

PERSONNEL SECURTY INFORMATION ON DSS WEBSITE

Looking for that OUSD(I) memorandum reminding DoD Components that personnel security clearances do not expire? Or the Common PCL Knowledge Center Inquiries web posting? We realize that it can be difficult to locate PCL information on the main DSS website due to the volume of updates and frequency in which items go into archive. For that reason, we recommend looking for PCL-specific items on the PSMO-I website. PCL-specific news items will remain available for a much longer period of time. Relevant items are updated within the left menu, like the common PCL Knowledge Center Inquiries. Be sure to create a bookmark and check back frequently for the most recent information.

MEMO ISSUED REGARDING PERSONAL SECURITY CLEARANCE EXPIRATION

On December 7, 2016, the USD(I) signed a memorandum reminding DoD Components that personnel security clearances do not expire. Individuals with current eligibility in JPAS should not be denied access based on an out-of-scope investigation. When the system of record shows current adverse information, but eligibility is still valid, access may continue. The memorandum is provided here for your ease of reference.

FROM COUNTERINTELLIGENCE:
THE CYBER THREAT IS INTENSIFYING.

> "The breadth of cyber threats posed to U.S. national and economic security has become increasingly diverse, sophisticated, and serious, leading to physical, security, economic, and psychological consequences.
>
> Despite ever-improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years to come from remote hacking to establish persistent covert access, supply chain operations that insert compromised hardware or software, malicious actions by trusted insiders, and mistakes by system users."
>
> *-The Honorable James R. Clapper, former Director of National Intelligence, from "Foreign Cyber Threats to the United States" (January 5, 2017)*

Contractors should remain vigilant for suspect cyber actions against their unclassified and classified information systems, system users, and system functions (e.g., 3-D printing). The cyber threat actors will attempt to gain access to these systems to target and capture information on classified contracts, systems, associated personnel, facilities, and technologies. These actors may also impair system functions or output and gain classified material in the aggregate. They will diversify their coverage through human sources, including insiders. Contractors should have prudent measures in place to recognize and report these suspicious actions in accordance with NISPOM paragraphs 1-301 and 1-302, as well as Industrial Security Letter 2013-05, dated July 2, 2013.

The threat actors normally first profile the targeted organization through open sources, and build knowledge of key information on the business, such as products, employees, business locations, practices, management, customers, network activity and addresses, and core technologies. The suspect actions may appear for example, as unusual network performance issues, unauthorized external mapping of the network, emails strangely worded or unexpected, efforts to elicit passwords and access credentials, unexplained changes in data file size or structure or movement, links to suspicious sites, and unauthorized changes in system privileges. The scope of concern should extend to whatever information systems the contractor owns, operates, uses, controls, or connects with, that hold this information or would allow compromising actions. Contractors should expect these nation-state threat actors will identify and include the contractors' subsidiaries, partners, suppliers, service providers, and other company or corporate elements among the actors' cyber targets.

When you detect suspicious actions that require reporting under NISPOM paragraphs 1-301, 1-302 or Industrial Security Letter 2013-05, dated July 2, 2013, you should file an initial report quickly, and provide more specific details in follow-on reporting.

REMEMBER: Our united ability to counter these cyber threats improves directly with the timeliness of your detection and reporting, and strengthens our collective National Security.

SECURITY EDUCATION AND TRAINING

2016 HORIZON AWARDS

The Center for Development of Security Excellence (CDSE) won nine Horizon Interactive Awards in the 2016 competition. CDSE won its first silver medal for a promotional video and eight CDSE products won bronze medals.

Training/eLearning:

- DSS Annual Security Awareness Training (Bronze)
- Introduction to RMF Course (Bronze)
- ISM Course SF 700 Practical Exercise (Bronze)
- SAP Security Incident Virtual Exercise (Bronze)
- Clearances in Industrial Security: Putting it All Together (Bronze)
- Acquisitions and Contracting Basics in the NISP (Bronze)

Videos:

- Counterintelligence (CI) Awareness Video (Silver)
- Special Access Program (SAP) Security Incident Videos (Bronze)
- Defense Insider Threat Management Analysis Center (DITMAC) Short (Bronze)

The 2016 Horizon Interactive Awards Competition saw over 1,200 entries from around the world including 40 out of 50 U.S. States and 20 countries. In its 15th season, the Horizon Interactive Awards recognize the best web sites, videos, online advertising, print media, and mobile applications.

In 2015, the Horizon Interactive Awards added a "Distinguished Agency" award for agencies attaining four or more awards. CDSE was included on this list for a second year in 2016. Since 2009, CDSE has won a total of 49 Horizon Interactive Awards.

UPCOMING INDUSTRIAL SECURITY AND INSIDER THREAT WEBINARS

CDSE invites you to participate in the following live webinars:

DD 254
Thursday, June 8, 2017
11:30 a.m. or 2:30 p.m. Eastern Time

This webinar is designed to ensure government and industry-wide uniform application of the DD Form 254. Each of the 17 items contained on the form will be explored through a series of practical exercises. It is recommended that you bring or download a copy of A Guide for the Preparation of a DD Form 254 Job Aid to this webinar.

User Activity Monitoring in Insider Threat Programs
Thursday, July 13, 2017
12:00 p.m. Eastern Time

This webinar will discuss the requirement of User Activity Monitoring in Insider Threat Programs. Our live session will focus on elements of successful User Activity Monitoring to support insider threat detection and mitigation.

NEW INSIDER THREAT AWARENESS GAME

Looking for a fun way to encourage Insider Threat awareness at your organization? Share CDSE's Vigilance Word Search with your personnel. This popular game is a quick and easy way to remind the workforce of messaging associated with Insider Threat.

COMING SOON: INSIDER THREAT "SHORT" FOR SENIOR EXECUTIVES

Thanks to the community for providing subject matter expertise in the development of our latest learning product. This "Short" is designed for the Insider Threat Senior Executive who does not have day-to-day oversight of the Insider Threat Program. The product provides a policy and standard overview in less than 12 minutes. Find the short and all of our learning products in the CDSE Insider Threat Training Catalog.

NEW INSIDER THREAT VIDEO LESSON

Watch, Think, and Dig Deeper into Potential Risk Indicators in less than five minutes.

NEW POSTERS

Trick out your hallways with free printables from CDSE:

Insider Threat
Vigilance
Everyone struggles sometimes…

INSIDER THREAT DEFINITIONS

Access this dynamic job aid for frequently used terms and phrases.

REGISTER NOW FOR UPCOMING INDUSTRIAL SECURITY TRAINING

Seats are still available for the "Getting Started Seminar (GSS) for New FSOs," which will be presented in conjunction with the National Classification Management Society (NCMS) Annual Seminar in Anaheim, CA on June 19, 2017.

Take advantage of this opportunity to save training costs by completing both the CDSE training course and the NCMS Annual Seminar at the same time. This course is open to Facility Security Officers and Assistant Facility Security Officers, Security Specialists, and anyone employed in the security environment (such as Human Resources, Administrative Assistants, Program Managers, and Military Members exiting the various Armed Services). A prerequisite course titled "FSO Role in the NISP" is required for seminar registration and must have completed after November 23, 2015.

To accommodate the 2017 NCMS Annual Seminar schedule, this iteration of the "Getting Started Seminar for New FSOs" has been condensed and will be presented as a one day session. Please note that a separate registration is required to attend the NCMS Annual Seminar on June 20-22, 2017. CDSE also offers this seminar at no cost via the Security Training, Education and Professionalization Portal (STEPP).

SECURITY AWARENESS HUB MOVING

The Security Awareness Hub is moving to a new location. Stay tuned for updated links and other important information about our new learning platform by following us on Twitter (@TheCDSE), Facebook, or on the current Hub webpage.

SOCIAL MEDIA

Connect with CDSE on Twitter (@TheCDSE) and on Facebook.

Thanks,
ISR
Defense Security Service