DSS Monthly Newsletter
June 2018

(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.

WHERE TO FIND BACK ISSUES OF THE VOICE OF INDUSTRY (VOI) NEWSLETTER

Missing a few back issues of the VOI Newsletter? The Defense Security Service (DSS) Public Affairs Office maintains a library of the VOI Newsletter (and other important forms and guides) on its Industry Tools page.

DSS IN TRANSITION (DiT)

In early 2018, DSS leadership briefed Government and Industry Stakeholder groups at a number of meetings, conferences, and seminars on the security review types that would be used by DSS field personnel during the year. Review types include a comprehensive security review, targeted security review, and enhanced security vulnerability assessment (SVA).

The comprehensive security review will follow the new DSS in Transition (DiT) methodology which is an unrated review that results in the development of a TSP. The second review type is a targeted security review. This review type follows the new DiT methodology but stops short of developing a TSP. Targeted security reviews are rated under our traditional rating model.

The third review type is the enhanced SVA, which introduces facility personnel to the concepts of asset identification, business processes associated with the protection of assets, and the new threat tool known as the “12x13” matrix. Enhanced SVAs follow the traditional SVA format and are rated. While not all facilities will receive one of these three reviews, the review type a facility receives will be dependent on a number of factors and internal prioritization.

DSS personnel will conduct meaningful engagements with those facilities not receiving one of the three review types. Meaningful engagements are activities designed to get a sense of the security posture at a cleared facility. DSS field offices have multiple activities they can leverage to conduct a meaningful engagement with a facility and these determinations will be made at the field office level based on resources and priorities. While each of these activities will adhere to

DSS authorities and NISP oversight, Industry is encouraged to work directly with local field office representatives on any questions or concerns they have.

DSS continues to implement DiT using a phased approach. After completing the first phase of implementation in April 2018, DSS is now conducting reviews at eight facilities identified for the second phase. DSS anticipates these reviews will be completed in late July 2018 and will conduct a comprehensive after action review upon completion. The DSS website was recently updated with new information and resources regarding DiT. For more information, click here.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) UPDATE

NISS is currently unavailable as we prepare for full deployment. Please do not attempt to create new accounts or log into the system as you will be unable to do so until full deployment.

Over the past several months, DSS has been finalizing the NISS application for deployment. We appreciate your patience throughout this period as we continue to resolve unforeseen critical issues with the NISS Application. At this time, the Industrial Security Facilities Database (ISFD) and Electronic Facility Clearance System (e-FCL) remain the systems of record for facility clearance information until further notice. Once DSS has validated that the critical issues are resolved, DSS will inform the user community of the NISS transition dates and guidance. At this time, DSS is not ready to announce firm transition dates and we apologize for any inconvenience this may cause. Please refer to the NISS website for status updates:

http://www.dss.mil/is/niss.html.

Thank you again,
The NISS Team

NISP ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (E-MASS) JOB AID FOR TRAINING GUIDANCE AND SYSTEM ACCESS

The NISP Authorization Office (NAO) has created and released a Job Aid for Cleared Industry to obtain sponsorship and access to the NISP eMASS training web site. This site is hosted by DISA and requires Cleared Industry to be sponsored for access. The Job Aid and instructions will allow NISP partners to access and complete the required DISA computer based training beginning on July 2, 2018.

The Industry Job Aid can be found at:

http://www.dss.mil/rmf/index.html, under the header "Resources", or on the website: http://www.dss.mil/isp/nao/news.html, under the header "NAO News"

NAO RELEASE OF DSS ASSESSMENTS AND AUTHORIZATION PROCESS MANUAL (DAAPM) 1.3

The NAO is pleased to announce the release of the DAAPM Version 1.3 in our continuing effort to provide users with the most up-to-date requirements of the Risk Management Framework (RMF) process. Version 1.3 supersedes all previous versions of the DAAPM and went into effect on June 4, 2018.

This version updates two specific areas of interest.

First, it includes a recommended submission period for RMF packages of at least 90 days. This change is located at the beginning of Section 6, which has been renamed to "Assessment and Authorization Implementation Guidance". The rational for the change is to ensure that both industry and DSS allow sufficient time to work the packages before and after submission.

Next, it identifies who (Cleared Industry or DSS) has the responsibility for each step of the process. Section 6 contains a walk-through of each RMF step and identifies the responsible party for each task within each step. In summary, Industry is responsible for Step 1, Step 2, Step 3, the first part of Step 4, and the first part of Step 6. DSS is responsible for the second part of Step 4, Step 5, and the second part of Step 6. Additionally, the flowchart in Section 5 is updated to reflect the ownership of each step. Finally, the Concurrence Form has been eliminated. The intent of this change is to eliminate confusion.

You may access the DAAPM 1.3 from the DSS RMF Resource Center site here.
We welcome comments and suggestions as they help us improve our products and processes.

REMINDER ON TIMING FOR ELECTRONIC FINGERPRINT TRANSMISSION

Electronic fingerprints should be submitted at the same time or just before an investigation request is released to DSS in the Joint Personnel Adjudication System (JPAS).

You can confirm that the National Background Investigations Bureau (NBIB) has processed the fingerprints by checking the Security/Suitability Investigations Index (SII) in JPAS which indicates a "SAC" closed.

Fingerprint results are valid for 120 days, the same amount of time for which Electronic Questionnaires for Investigations Processing (e-QIP) signature pages are valid. Therefore, submitting electronic fingerprint at the same time or just before you complete your review for adequacy and completeness, should prevent an investigation request from being rejected for missing fingerprints.

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) DEPLOYMENT GUIDANCE FROM DSS

On June 25, 2018, DISS will deploy to Industry, but given ongoing DISS provisioning efforts, the following guidance is being provided to define what deployment means. Industry users that have been provisioned in DISS should begin using DISS to submit Customer Service Requests (CSRs) and SF-312s. Industry users not yet provisioned in DISS may continue to submit JPAS RRUs and fax/mail SF-312s while awaiting the provisioning of their DISS account. For communication originating from PSMO-I or the DoD Consolidated Adjudications Facility (CAF), and being sent to facility security officers, PSMO-I/DoD CAF will transmit all communication via both DISS and JPAS; this is a temporary measure during the interim time period where user provisioning is an ongoing effort, which will be re-evaluated every 30 days.

FOR THOSE REQUESTING INVESTIGATION/ADJUDICATIVE RECORDS FROM DSS

Freedom of Information Act/Privacy Act (FOIA/PA) requests for investigative or adjudicative records maintained in the Investigative Records Repository (IRR), Defense Central Index of Investigation (DCII), Secure Web Fingerprint Transmission (SWFT), or JPAS IT systems should be submitted to the DMDC Office of Privacy at:

Defense Manpower Data Center
ATTN: Privacy Act Branch
P.O. Box 168
Boyers, PA 16020-0168

DSS no longer maintains any personnel security investigative records, to include clearance adjudicative records, JPAS, and SF-86s (e-QIP) on DoD employees or DoD contractor personnel. For further information, please visit the DSS FOIA website here.

INVESTIGATION STATUS UPDATES

You can obtain an investigation status update by performing a search of the SII in JPAS. This link is available at the bottom of the Person Summary Screen in JPAS (Perform SII Search). The following statuses are available to let you know what is happening with the investigation:

- Received - The Investigation Service Provider has acknowledged receipt of the investigation request and will be reviewing for acceptability.

- Unacceptable - The Investigation Service Provider determined the investigation request to be deficient. PSMO-I will transmit a JPAS message with the reason the request was rejected. If your employee still requires a clearance, a new investigation request will need to be initiated and submitted with the corrected information.

- Scheduled - The Investigative Service Provider has determined the investigation request to be acceptable and the investigation is current ongoing/open.

- Closed - The Investigative Service Provider has completed the investigation and the investigation has been sent for adjudication.

- Case Action (CA) Considered - The "CA Considered" in SII indicates that the case is closed pending leads at Office of Personnel Management (OPM). Once the investigation is closed it will be sent to the DoD CAF for adjudication. DISS /Joint Verification System (JVS) will be updated once the adjudication process is complete.

Please do not call the DSS Knowledge Center to request the status of an investigation showing in one of the statuses provided above. The Knowledge Center will no longer provide lead count and does not have the ability to estimate nor impact investigation timelines

SECURITY EDUCATION AND TRAINING

NEW UPDATED SUBSCRIBER EMAIL SERVICE

Center of Development of Security Excellence (CDSE) is pleased to announce that we have implemented a new email subscription service to make it easier for you to learn about updates on the topics which interest you. We hope that you will find it useful to have the ability to customize your emails based upon your particular areas of interests.

With this new service you can password protect your subscriptions and preferences, change your email address, or remove yourself at any time by accessing your Manage Subscriptions (https://public.govdelivery.com/accounts/USDSSCDSE/subscriber/edit?preferences=true#tab1) page.

You'll find convenient links to your Subscriber Preferences in the footer of every message. You'll need to log in with your email address. Be sure to save your changes, and look for a confirmation via email verifying the updates you make. In addition to the functions listed above, you can also:

- Add new subscription Topics, such as Twitter Digest or the CDSE News Flash
- Choose a frequency preference for how often you'd like to receive email

If you currently subscribe to the CDSE Flash, your subscription will be discontinued on July 20, 2018. Sign up today at https://www.cdse.edu/news/index.html!

NEW INSIDER THREAT CASE STUDIES AVAILABLE

Your awareness is key to protecting our National Security from insider threats like Ivan Lopez and Jiaqiang Xu. See these latest case studies and others here: https://www.cdse.edu/resources/case-studies/insider-threat.html

Did you know you can subscribe to the CDSE Rich Site Summary (RSS) feed for case studies? It's an easy way to have the latest case studies sent right to you! Subscribe here: https://www.cdse.edu/news/casestudy.xml

UPCOMING WEBINAR

Join CDSE for our next webinar:

- **Business Structures**
  Thursday, 19 July 2018
  11:30 a.m. ET & 2:30 p.m. ET

In this live webinar, we will analyze business structures, determine ownership or control and clearance or exclusion, and identify vulnerabilities associated with improper analysis of business structures.

Register and be part of the conversation! Sign up today at CDSE Webinars.

UPCOMING SPEAKER SERIES

CDSE invites you to participate in our upcoming Speaker Series:

- **Defense Insider Threat Management and Analysis Center Update 2018**
  Thursday, July 19, 2018
  12:00 p.m. ET

In this webinar, CDSE will host a status discussion with leadership of the Defense Insider Threat Management and Analysis Center (DITMAC). DITMAC was established in the wake of the Washington Navy Yard shooting and other recent insider threat incidents to serve as a catalyst for information sharing and collaborative insider defense. DITMAC offers an enterprise capability that leverages relevant data; a multidisciplinary team of analysts and experts to assist in research, analysis, and risk assessment; and enabling tools and technologies to build an enterprise view of insider threat issues across DoD in support of DoD Components.

- **NATO at the Defense Security Service (DSS)**
  Thursday, July 26, 2018
  12:00 p.m. ET

In this webinar, CDSE will host a status discussion with the Program Manager for the North Atlantic Treaty Organization (NATO) in the Technical Oversight Programs and Services (TOPS) division of DSS. We will discuss how DSS got involved with the NATO Program, how it intergrates within the overall mission of DSS, and some positive aspects and challenges with this misson.

- **Applied Research on Mental Health Conditions & Security**
  Thursday, August 2, 2018
  12:00 p.m. ET

The Defense Personnel and Security Research Center’s (PERSEREC) mission is to improve the effectiveness, efficiency, and fairness of DoD Personnel Security and Suitability Programs. Current efforts include research on assessing and managing mental health issues related to personnel security, suitability, and insider threat. The goals of the project are to improve clinicians and adjudicators’ handling of cases with suspected personality disorders and to ensure that individuals with risky personality disorders are identified correctly and handled appropriately by selection, HR and personnel security staff. CDSE hosts a discussion with Dr. Eric Lang and Dr. Rene Dickerhoof of PERSEREC.

Join the discussion! Sign up today at CDSE Webinars.

ARCHIVED WEBINARS AND SPEAKER SERIES NOW AVAILABLE

Did you miss June's Speaker Series, "Supervisor Reporting and Security with PERSEREC" webinar? If the answer is "yes," you can access both and other past webinars in our archives.

Access all archived webinars (no certificate provided) at CDSE Previously Recorded Webinars or register for the on-demand webinars (certificate provided) at CDSE On Demand Webinars.

GETTING STARTED SEMINAR FOR NEW FSOs

Getting Started Seminar for New FSOs (GSS) gives new FSOs the opportunity to discuss, practice, and apply fundamental NISP requirements in a collaborative classroom environment and develop a network of professional associates. This course is appropriate for any FSO, new or old, who is looking to enhance their security program.

Our final iteration for the FY18 schedule is currently open for registration. Check out the course below to see if it meets your training needs.

- August 14-15, 2018, Pasadena, CA, go here.

Seats are limited, so make sure you have successfully completed the current version of the prerequisite course, "Facility Security Officer (FSO) Role in the NISP" (IS023.16) and exam (IS023.06). We look forward to seeing you soon!

Are you interested in hosting a Getting Started Seminar at your location in FY19? If so, please send an email to our Industrial Security mailbox (dss.ncr.dss-cdse.mbx.industrial-security-training@mail.mil), letting us know your interest and what region you would like us to consider your request under. We are beginning our solicitation process and welcome your requests. Below is a tentative schedule of our upcoming iterations.

- November 6-7, 2018, Capital Region
- May 14-15, 2019, Western Region
- July 23-24, Southern Region
- August 13-14, Northern Region

SOCIAL MEDIA

Connect with CDSE on Twitter and on Facebook.

Thanks,
ISR
Defense Security Service