DSS Monthly Newsletter
July 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 DiT methodology, which is an unrated review that results in the development of a Tailored Security Plan (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 National Industrial Security Program (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 concluding reviews at eight facilities identified for the second phase. Upon completion of the second phase reviews, DSS will conduct a comprehensive after action review in August and begin the third phase of implementation in September. The DSS website was recently updated with new information and resources regarding DiT. For more information, click here.

INSIDER THREAT EFFECTIVENESS

DSS is currently evaluating the effectiveness of insider threat programs at the eight facilities selected for the second phase of DiT implementation. This evaluation reviews five aspects of a contractor's insider threat program:

- Insider Threat Program Management
- Insider Threat Awareness Training
- Information Systems Protections
- Collection and Integration
- Analysis and Response

These five principles are evaluated by reviewing program requirements, assessing program implementation, and determining effectiveness of the program. Lessons learned from this pilot will be captured in a comprehensive after action review and shared with Industry representatives during a scheduled DSS-Industry engagement in August. DSS anticipates finalizing its process for evaluating insider threat effectiveness in early 2019.

The Center for Development of Security Excellence offers insider threat training, eLearning courses, and job aids at: https://www.cdse.edu/catalog/insider-threat.html.

FACILITY CLEARANCE BRANCH (FCB) UPDATE

The DSS FCB processes over 2,500 facility clearance (FCL) requests each year. Many are rejected or discontinued for various reasons.

What can you do to help expedite an FCL request?

- Ensure there is a valid need or requirement to access classified information.
- Provide complete and accurate information on the sponsorship letter and DD-254.
- Obtain Government Contracting Activity (GCA) authorization.
- Contact the DSS Knowledge Center, Option 3, at 888-282-7682 regarding questions.

Once an FCL request is accepted, the sponsored facility must:

- Meet all timelines and deadlines for FCL and Key Management Personnel (KMP) processes.

- Review the FCL Process Orientation Video and Handbook at dss.mil.
- Gather and upload all required business documents and forms.
- Submit e-QIPs and fingerprints for KMP on time.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) UPDATE

DSS continues to resolve critical application and data migration issues in preparation for NISS becoming the system of record for FCL information. DSS plans to deliver additional communications in August for the transition period when ISFD and e-FCL are replaced by NISS. This guidance will provide procedures for operations conducted by sponsors, facility clearance verifiers, and industry security staff during the transition period.

In order to facilitate a successful data migration and application deployment, there will be a brief period of time when ISFD and e-FCL are unavailable before NISS launches. We will announce the exact timelines and key dates for sponsorship requests and other functions in the coming weeks. We will provide the user community with 30 days' notice prior to transitioning to NISS.

As a reminder, ISFD and e-FCL continue to remain the systems of record.

Thank you for your patience during this transition as we bring NISS to the user community. Please refer to the NISS website for status updates: http://www.dss.mil/is/niss.html.

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

As a reminder, DSS is working with DISA to transition industry to the National Industrial Security Program enterprise Mission Assurance Support Service (NISP eMASS) system replacing OBMS. October 1, 2018 is the tentative target date for all new authorization packages to begin processing through NISP eMASS. Please refer to the job aid below to receive guidance on how to obtain training. The training is a requirement to get an account once NISP eMASS is operational.

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 that began 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"

2018 IMPLEMENTATION OF INTERIM BACKLOG MITIGATION MEASURES FOR ENTITIES CLEARED BY DOD UNDER THE NATIONAL INDUSTRISL SECURITY PROGRAM

In early June 2018, the Director of National Intelligence, in his capacity as the Security Executive Agent, and the Director of the Office of Personnel Management, in his capacity as the Suitability & Credentialing Executive Agent (Executive Agents), jointly issued a memorandum directing the implementation of interim measures intended to mitigate the existing backlog of personnel security investigations at the National Background Investigations Bureau (NBIB). These measures include the deferment of reinvestigations when screening results are favorable and mitigation activities are in place, as directed.

In accordance with the guidance and direction received from the Executive Agents, DSS will adopt procedures to defer the submission of Tier 3 Reinvestigations (T3Rs) and Tier 5 Reinvestigations (T5Rs) for entities cleared under the National Industrial Security Program. Facility Security Officers should continue to submit completed Standard Form 86 and the reinvestigation request, six years from the date of last investigation for the T5Rs and ten years from the date of the last reinvestigation for the T3Rs. New reinvestigation requests will be screened by DSS using a risk management approach that permits deferment of reinvestigations according to policy. If the determination is made to defer reinvestigations, individuals will be immediately enrolled into the DoD Continuous Evaluation (CE)/Continuous Vetting (CV) capabilities, as required.

The Executive Agents have directed all Federal departments and agencies to reciprocally accept the prior favorable adjudication for deferred reinvestigations that are out of scope (overdue). Existing eligibility remains valid until the individual is removed from CE, no longer has any DoD affiliation, or has their eligibility revoked or suspended.

The Office of the Undersecretary of Defense for Intelligence signed a memorandum on December 7, 2016, reminding DoD Components that personnel security clearances do not expire. Individuals with current eligibility in the Joint Personnel Adjudication System (JPAS), or its successor, should not be denied access based on an out-of-scope investigation. That memorandum is posted on the DSS website for ease of reference. If you encounter any challenges with this process, please email dss.ncr.dss-isfo.mbx.psmoi@mail.mil for assistance.

These procedures will remain in effect until further notice.

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 Joint Personnel Adjudication System (JPAS).

You can confirm that the National Background Investigations Bureau (NBIB) has processed the fingerprints by checking 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

Defense Information System for Security (DISS) deployment to Industry remains an ongoing effort with Defense Manpower Data Center (DMDC) continuing to provision additional hierarchy managers. If you have been contacted by DMDC via email with a username and instructions for logging in to DISS, please follow the directions provided and log in to DISS at your earliest opportunity. Once you are able to log in, please verify that your SMO hierarchy is accurate; if not, please follow the instructions to request modifications to your hierarchy found at http://www.dss.mil/psmo-i/indus_diss.html (6/6/2018 Update and 7/17/2018 HCR Form).

Given ongoing DISS provisioning efforts, the following guidance remains in effect: 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 Joint Personnel Adjudication System (JPAS) RRUs and fax/mail SF-312s while awaiting the provisioning of their DISS account. For communication originating from PSMO-I or the DoD Central 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."

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 Investigation 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/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

STEPP IS MOVING OCTOBER 1

Our current learning management system, STEPP, will be migrated to a new location on October 1st. To prepare for this move, please plan to complete all training by Friday, 14 September 2018, 6:00 p.m. ET. Participants in the SPeD Certification program, additional information regarding the deadline for SPeD account creations/edits can be found at https://www.cdse.edu/certification/index.html.

2018 DOD VIRTUAL SECURITY CONFERENCE FOR INDUSTRY – SAVE THE DATE!

Mark your calendars for the 2018 DoD Virtual Security Conference for Industry on September 19! This conference will focus on “security in motion” and is open to industry. This includes, but not limited to the NISP Risk Management Framework Process, DSS’s Changing Approach to Industrial Security, and Information Sharing with the Insider Threat Community. Stay tuned for more details closer to the conference date.

NEW UPDATED SUBSCRIBER EMAIL SERVICE

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 were previously subscribed to the CDSE Flash, your subscription was discontinued on July 20, 2018. Sign up today at https://www.cdse.edu/news/index.html!

UPCOMING WEBINAR

Join CDSE for our next webinar:

- **DD254: What has Changed?**
  Thursday, 9 August 2018
  11:30 a.m. ET
  2:30 p.m. ET

This webinar is designed to ensure a government and industry-wide uniform understanding and application of the new DD Form 254. Each of the 17 items contained on the form will be discussed with emphasis on the new portions of the form.

- **Securing the Internet of Things**
  Thursday, 20 September 2018
  12:00 p.m. ET

More and more devices are joining our home networks. Today, it's not unusual to have internet-enabled cameras, thermostats, or appliances in our home. This webinar discusses what we need to do to secure our devices and protect ourselves at home.

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:

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

The Defense Personnel and Security Research Center's 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.

- **CI Support to Research, Development and Acquisition**
  Thursday, 23 August 2018
  12:00 p.m. ET

The Defense Security Service Counterintelligence (CI) Directorate provides support to Research Development and Acquisition programs resident in defense industry. Our guest, DSS CI Special Agent Michelle Yoworski, will discuss the threat environment for our industry partners and CI support to RDA.

- **Applied Research on Exfiltration and Security**
  Thursday, September 13, 2018
  12:00 p.m. ET

The Defense Personnel & Security Research Center (PERSEREC) has published four comprehensive reports on espionage in America. In recognition of the shifting threat landscape, PERSEREC has expanded its Espionage Project to include all known incidents in which government personnel were convicted of exfiltration of protected resources without authorization. This expanded effort, titled The Exfiltration Project, will identify actionable intervention points and the corresponding behavioral indicators along individuals' critical pathways to exfiltration, which in turn can be incorporated into data science monitoring/evaluation tools, workforce training, and organizational risk management plans. On September 13, Ms. Stephanie Jaros, PERSEREC Project Director, will present the results published in the first report from this expanded project.

Join the discussion! Sign up today at CDSE Webinars.

GETTING STARTED SEMINAR FOR NEW FSOS FY19 SCHEDULE

The Center for Development of Security Excellence (CDSE) is a nationally accredited, award-winning directorate within the Defense Security Service (DSS). CDSE provides security education, training, and certification products and services to a broad audience, supporting the protection of National Security and professionalization of the Department of Defense (DoD) security enterprise. With that said, consider hosting a course at your facility with CDSE's certified instructor staff this upcoming fiscal year (FY). The Getting Started Seminar (GSS) for New Facility Security Officers (FSOs) Course Manager is beginning the solicitation process and welcome your requests. If you are interested, 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. Below is a tentative schedule of our upcoming iterations.

Nov. 6-7, Capital Region

May 14-15, Western Region

July 23-24, Southern Region

Aug. 13-14, Northern Region

SOCIAL MEDIA

Connect with CDSE on Twitter and on Facebook.