DSS Monthly Newsletter
August 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)

DSS continues to conduct comprehensive security reviews and implement the new DSS in Transition (DiT) methodology using a phased approach. These reviews are unrated and result in the development of tailored security plans (TSPs). As of August 2018, DSS has completed the first two phases of implementation and recently conducted a comprehensive after action review at the conclusion of phase two. DSS has started to conduct activities associated with the third phase of implementation, which is expected to conclude in October. The fourth and final phase of implementation will begin shortly after the conclusion of phase three.

DSS is also in the process of conducting a training needs analysis that will inform the development of training for internal and external stakeholders. The DSS website was recently updated with new information and resources regarding DiT and additional content will be added in the weeks ahead. For more information, click here.

INSIDER THREAT EFFECTIVENESS

DSS recently evaluated the effectiveness of insider threat programs at eight facilities reviewed during the second phase of DiT implementation. This evaluation reviewed five aspects of the 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 were evaluated by reviewing program requirements, assessing program implementation, and determining effectiveness of the programs. Lessons learned from this pilot were shared with Industry representatives at a DSS-Industry engagement in August and DSS will continue its evaluation of industry insider threat programs at 16 facilities scheduled to be reviewed in the third phase of DiT implementation. 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.

DOD Manual 5220.22, VOLUME 2 ISSUANCE

On August 1, 2018, DoD issued DoD Manual 5220.22, Volume 2, "National Industrial Security Program: Industrial Security Procedures for Government Activities" which incorporates and cancels DoD Regulation 5220.22-R, "Industrial Security Regulation." DoD Manual 5220.22. Volume 2 prescribes industrial security procedures and practices applicable to DoD components and those non-DoD agencies for which DoD provides industrial security services to ensure uniformity and effectiveness in DoD's implementation of the National Industrial Security Program.

DoDM 5220.22, Volume 2 can be found at:
http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022_vol2.pdf?ver=2018-08-01-114445-000.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) UPDATE

The National Industrial Security System (NISS) is approaching full deployment as the system of record. Once testing has identified the system is ready for deployment, the transition process will begin. This process includes transitioning from ISFD and e-FCL to NISS with the following process implications. Specific dates will be provided for the below once final testing has yielded expected results.

System Downtime:

- ISFD and e-FCL will be taken offline with a three week timeframe of data migration and system deployment activities until NISS is operational for Government and Industry users.

Facility Clearance Sponsorship Impacts:

- During the transition period to NISS, the DSS Facility Clearance Branch (FCB) will not be able to process facility clearances and thus will not accept new sponsorship packages. During this downtime, the FCB encourages sponsors to gather the required information for a complete sponsorship, as outlined in information available at https://www.dss.mil/isp/fac_clear/fac_clear.html

- Additionally, until FCB activities are migrated from legacy manual processes to the automated NISS process, the FCB is predicting a period with additional delays in processing all requests for facility clearances.

Facility Clearance Verification Impacts:

- During ISFD downtime, external Government and Industry users will call the DSS Knowledge Center (888) 282-7682, Option 3, for any facility clearance verifications as NISS will not be live for external users and ISFD will be taken offline.

Change Condition and Self-Inspection Certification Impacts:

- During e-FCL downtime, FSOs will contact their ISR if they have a Change Condition to report. Based on guidance from your ISR, if you need to submit relevant information via email or AMRDEC, please use the following link https://safe.amrdec.army.mil/safe/
- Any self-inspection certifications should be submitted in NISS when live.

NISS Training in STEPP:

- STEPP training is available now for Industry and Government NISS users. (STEPP ID IS127.16, "National Industrial Security System (NISS) External User Training Course")

Thank you for your patience during this transition. As always the latest updates can be found at http://www.dss.mil/is/niss.html

NATIONL INDUTRIAL SECURITY PROGRAM (NISP) AUTHORIZING OFFICE (NAO) ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (E-MASS) UPDATE

The transition to eMASS as the DSS system of record for NISP Information Systems authorizations was scheduled to begin on October 1, 2018. NAO has taken into careful consideration the concerns of our NISP Industry partners regarding this transition. Therefore, in order to allow time for Industry to obtain the required eMASS training, apply and receive their eMASS accounts and become familiar with the eMASS application.user guides, NAO has decided to postpone the transition.

The eMASS transition is anticipated to begin March 18, 2019. Until then, NISP Industry partners will submit all System Security Plans and supporting artifacts via the ODAA Business Management System. NISP Industry partners should continue to work with your designated Information Systems Security Professional (ISSP) and/or ISSP Team Lead to complete the required eMASS training to ensure readiness for the transition.

NAO will continue to keep NISP Industry partners apprised of the transition timelines and actions via the VOI, the Risk Management Framework Information and Resources page (www.dss.mil/rmf) and other Industry forums. If you have any questions regarding eMASS, please reach out through the NAO eMASS mailbox at dss.quantico.dss.mbx.emass@mail.mil.

2018 IMPLEMENTATION OF INTERIM BACKLOG MITIGATION MEASURES FOR ENTITIES CLEARED BY DOD UNDER THE NISP

In early June of 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 NISP. Facility Security Officers (FSOs) 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.

More information is available in the linked frequently asked questions
http://www.dss.mil/documents/psmo-i/Interim_Backlog_Measures_FAQs_Aug2018.pdf

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 JPAS.

You can confirm that the NBIB has processed the fingerprints by checking 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.

VERIFY THE IDENTITY OF AN OPM/NBIB INVESTIGATOR

NBIB has a number of contract companies that support the investigative mission. Two companies are in the midst of changing their company names. Below is a quick summary of the companies that currently support the NBIB mission that may contact the applicant for additional information:

CACI
Keypoint (Changing name to Perspecta)
CSRA (Changing name to GDIT)
Securitas
NTConcepts

Contact the Investigator Verification/Complaint Hotline at 1-888-795-5673 or RMFSIMSST@nbib.gov to verify the identity of NBIB field staff or if you have questions or concerns about the line of questioning or actions of a field investigator.

SECURITY OFFICER IDENTIFIER (SOI) CODE UPDATES OFR INDUSTRY

With the release of JPAS v5.7.5.0 in October 2017, FSOs will need to select the SOIs from the dropdown menu when submitting new investigations.

FSOs must now manually select "DD03" as the SOI Code from the dropdown menu; whereas this code used to be automatically applied. Industry should not be using any other SOI Code when submitting investigation requests.

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

Additional DISS Tips & Tricks to assist users with provisioning subordinate users, hierarchy set-up/management, and the submission of Comprehensive Security Reports (CSRs) has been posted at http://www.dss.mil/psmo-i/indus_diss.html.

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 JPAS RRUs (must be submitted to the DoD IND bucket) and fax/mail SF-312s while awaiting the provisioning of their DISS account. For communication originating from PSMO-I or the DoD 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.

As JPAS continues to transition to DISS and in an ongoing effort to enhance data quality, JPAS will perform a Data Quality Initiative (DQI). Please ensure the citizenship and records of all employees have been updated in the PSMnet.

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.

INTERIM TOP SECRET DETERMINATIONS

At this time, PSMO-I is unable to receive and/or track the Advanced NAC product electronically from NBIB for T5 investigations. It is requested that Industry submit a CSR via DISS or JPAS Research RRU to request the Interim Top Secret determination 30 days after the investigation request was released by PSMO-I. Once the CSR/RRU is received, PSMO-I will review the available information and update JPAS with the appropriate eligibility determination.

This process is temporary. DSS and DMDC are actively working on correcting the issue. Once resolved, PSMO-I will provide an update.

As of August 27, 2018, PSMO-I has started to utilize the following message in JPAS for Interim Top Secret determination for T5 investigations:

Message from PSMO-I: The T5 investigation for this Subject was released to NBIB. If Subject requires an Interim Top Secret eligibility, please notify PSMO-I 30 days after the date of this message by submitting a Customer Service Request (CSR) if you have a DISS account or if you only have a JPAS account, please submit a Research RRU. For further reference information concerning Investigation Requests, Incident Reports, CSR/RRU actions, and Personnel Security Investigations, please refer to the official DSS website at http://www.dss.mil. If you require additional assistance, please contact the DSS Knowledge Center at 1-888-282-7682.

SECURITY EDUCATION AND TRAINING

STEPP IS MOVING OCTOBER 1

As previously mentioned, our current learning management system, STEPP, will be migrated to a new location on October 1. To prepare for this move, please plan to complete all training by Friday, September 14, 2018, 6:00 p.m. EDT, since STEPP will be unavailable two weeks prior to the new location launch.

Participants in the SPēD Certification program:

Additional information regarding the deadline for SPēD account creations/edits can be found at https://www.cdse.edu/certification/index.html.

Current users who have updated their profiles will receive an email the week of 24 September to access the new site. To get ahead of the game, please see the attached "user checklist" for all the information you'll need to login! https://youtu.be/rZCHt_TyOJI

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.

FY19 COURSE REGISTRATION NOW OPEN

The FY19 CDSE Training Course Schedule is now available. Plan your security training for the coming year. Sign up today at https://www.cdse.edu/catalog/classroom/print.html

SEPTEMBER SPEAKER SERIES AND WEBINARS

CDSE invites you to participate in our upcoming Speaker Series:

Personnel Security for Industry - Today and Tomorrow
Thursday, September 6, 2018
12:00 p.m. ET

This is the third and final topic from the Industrial Security discipline that will focus on various missions within the Defense Security Service (DSS). Our guest will be speaking with us about the changes in DSS with regards to Personnel Security and Clearances and will discuss what the Continuous Evaluation Program is and provide an update on the Defense Industrial System for Security (DISS) deployment. We will also talk about FY18 Personnel Security Investigations (PSI) for Industry updates, innovative initiatives, and the way ahead for the program.

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 us and be part of the conversation!

Join CDSE for our next webinar:

Your fridge may be spying on you: Securing the Internet of Things
Thursday, September 20, 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.

GETTING STARTED SEMINAR FOR NEW FSO FY19 SCHEDULE

The Center for Development of Security Excellence (CDSE) is proud to present the instructor-led course, Getting Started Seminar for New FSOs IS121.01. This course allows new FSOs and security personnel the opportunity to discuss, practice and apply fundamental National Industrial Security Program (NISP) requirements in a collaborative classroom environment and develop a network of professional associates. If you are interested in hosting this course at your facility with CDSE's certified instructor staff this upcoming fiscal year (FY), please send an email to our Industrial Security mailbox (dss.ncr.dss-cdse.mbx.industrial-security-training@mail.mil), letting us know which 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

NEW UPDATED SUBSCRIBER EMAIL SERVICE

CDSE has 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 to start or continue receiving updates at https://www.cdse.edu/news/index.html!

SOCIAL MEDIA

Connect with CDSE on Twitter and on Facebook.