DSS Monthly Newsletter
November 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 VOI Newsletters (and other important forms and guides) are archived on the DSS website Industry Tools page.

DSS IN TRANSITION (DiT)

DSS is concluding comprehensive security reviews at select facilities as part of phased implementation of the new DSS in Transition (DiT) methodology. As of November 2018, DSS has completed the first three phases of implementation and recently conducted a comprehensive after action review at the conclusion of phase three. The fourth and final phase of implementation is underway and will be completed in January 2019.

In 2019, DSS will continue to implement the DiT methodology. Select priority technologies have been identified and field personnel are in the process of engaging with cleared industry to validate the presence of these technologies at their locations. Upon validation, DSS personnel will begin planning, scheduling, and conducting comprehensive security reviews throughout 2019 at these facilities.

DSS will continue to make modifications to the new DiT methodology based on the results of phased implementation and the findings developed during after action reviews. These adjustments will support DSS execution of the new methodology on a broader basis to enable to protection of a greater number of critical technologies and programs supported by cleared industry.

For more information on DiT, click here.

SECURITY OVERSIGHT AND REVIEW ACTIVITIES

In 2019, DSS will continue conducting security oversight of cleared contractor facilities using several of the review activities implemented in 2018. Oversight and review activities include a comprehensive security review, enhanced security vulnerability assessment (SVA), and Counterintelligence and Security engagements (previously referred to as meaningful engagements). The comprehensive security review will continue to follow the DiT methodology and result in the development of a tailored security program. These reviews will continue to remain unrated at this time.

In 2018, traditional SVAs were enhanced by introducing 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. DSS will further enhance these SVAs in 2019 by identifying assets at the contractor location, reviewing the facility's business processes used to protect assets, and providing a 12x13 matrix specific to the facility and/or technology the facility is performing on. While these reviews will leverage the new primary concepts of the DiT methodology, they will continue to closely follow the traditional SVA format and be rated under the existing rating model.

Not all facilities will receive an on-site security review. Those receiving one will be dependent upon a number of factors and internal prioritization. DSS personnel will continue to conduct CI and Security engagements with those facilities not receiving an on-site security review. These 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 CI and Security engagements 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.

REQUESTS FOR INFORMATION

From time to time, industry may receive correspondence from their local field office regarding their security program, classified contracts, or other NISP activities. These routine inquiries enable DSS personnel to validate a facility's continued participation in the NISP and helps to ensure DSS records are updated with pertinent, relevant, and current contract information. These interactions can also assist DSS in validating an industry partner's support to critical programs and technologies.

As DSS is unable to conduct a security review at each contractor facility on an annual basis, personnel often leverage these engagements to maintain routine and ongoing interaction with industry partners. Industry is encouraged to cooperate with DSS security officials in support of the protection of critical technologies and strengthened national security partnerships.

FACILITY CLEARANCE INQUIRIES

Industry is reminded to attempt to resolve all facility clearance issues at the local level. This includes general questions and requests for support. In these instances, industry should contact their assigned DSS Industrial Security Representative for assistance. For any issues that cannot be resolved at this level, industry may then seek engagement with their DSS field office and regional leadership to find resolution.

As a reminder, the DSS Knowledge Center is also able to assist industry with facility clearance inquiries. The Knowledge Center can be reached at (888) 282-7682. Please note that the Knowledge Center is closed on weekends and all federal holidays.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) IS NOW THE SYSTEM OF RECORD FOR FCL INFORMATION

NISS is the system of record for FCL information. NISS launched for external users on October 8, 2018. ISFD and e-FCL are no longer available. All official business such as: reporting change conditions, performing facility clearance verifications, and submitting FCL sponsorship requests should be submitted in NISS.

For instructions on how to register, please visit the Registration section on the NISS website: http://www.dss.mil/is/niss.html. If you encounter registration issues, please contact the DSS Knowledge Center at (888) 282-7682 and select Option 1, then Option 2.

After obtaining your NISS account, you may access training resources directly from the NISS Dashboard. Topics include: How to Message your ISR, How to Submit a FCL Sponsorship Request, and How to Change Roles within the NISS.

A full system training course is available on STEPP:
https://www.cdse.edu/catalog/elearning/IS127.html.

NATIONAL INDUTRIAL SECURITY PROGRAM (NISP) AUTHORIZING OFFICE (NAO)

ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (E-MASS)

The eMASS transition is scheduled for March 18, 2019. Until then, NISP Industry partners will continue to 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 (RMF) 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.

E-MASS JOB AID FOR TRAINING REMINDER

NISP Industry partners are reminded to obtain access and complete the required DISA computer based training. The training takes approximately 2 hours and a certificate of completion is granted upon finishing the training. This certificate is one of the required artifacts needed to request an eMASS account. NAO has created and released a Job Aid for NISP Industry partners to obtain sponsorship and access to the DISA eMASS training web site. NISP Industry partners need to be sponsored for access to the training. The job aid and instructions are available now.

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".

SYSTEM SECURITY PLAN (SSP) SUBMISSION RECOMMENDATION

NISP Industry partners are strongly encouraged to follow the SSP submission recommendations listed in the DSS Assessment and Authorization Process Manual (DAAPM). Section 6 of the DAAPM states the following:

"DSS highly recommends SSP submission for RMF packages at least 90 days before required need, whether re-authorization or new IS. This timeframe will allow for complete SSP review and interaction between the ISSM and ISSP on any potential updates or changes to the SSP."

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

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, Defense Security Service (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 10 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 Under Secretary 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.psmo-i@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 Joint Personnel Adjudication System (JPAS).

You can confirm that the National Background Investigations Bureau (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.

PR FINGERPRINT REJECTIONS

Recently, the Vetting Risk Operations Center (VROC) received notifications of Periodic Reinvestigations (PR's) submissions rejected due to missing fingerprints. PR's do not require fingerprints unless requested. When selecting the Periodic Reinvestigation, please ensure your submission is not requesting the fingerprints. Because PR's submitted with fingerprints are coded (I) and are rejected due to the missing prints not received by the system before the suspense date. When the Federal Investigations Processing Center (FIPC) Code "I" is added to

the PR case; the code (I) indicates that fingerprints will be sent electronically and, when present on the Agency Use Box (AUB), it will suspense the fingerprint request for 14 days and then reject the case if it does not arrive. If you have received a message from the Joint Personnel Adjudication System (JPAS)/Defense Information System for Security (DISS), please contact the Knowledge Center (KC) for further guidance.

VERIFY THE IDENTITY OF AN OPM/NBIB INVESTIGATOR

NBIB has a number of contract companies that support the investigative mission. As of November 2018, listed below is a quick summary of the companies that currently support the NBIB mission that may contact the applicant for additional information:

CACI
Perspecta
GDIT- General Dynamics Information Technology
Securitas Critical Infrastructure Services Inc
NTConcepts

Please visit (https://nbib.opm.gov/industry/frequently-asked-questions/) to review sample emails from field investigators.

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 OFFICE IDENTIFIER (SOI) CODE UPDATES FOR INDUSTRY

With the release of JPAS v5.7.5.0 in October 2017, Facility Security Officers (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

DISS DEPLOYMENT GUIDELINES FROM DSS

At this time, DSS will begin provisioning hierarchy managers in DISS for facilities that have not yet been contacted by DMDC; DSS will provision one hierarchy manager per facility, who will then subsequently provision other users for the facility themselves. Please read all of, and carefully follow, the DISS JVS Industry Provisioning Instructions (this should be a link to that attachment); failure to do so may result in the rejection of your provisioning package, which will return your next submission to the end of the queue and needlessly delay your provisioning.

Once you have obtained access to DISS, please review the following DISS Tips & Tricks (http://www.dss.mil/documents/DISS_JVS_Industry_Provisioning_Instructions.docx) for helpful hints and answers to frequently asked questions."

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 records of all employees are recorded accurately in the JPAS.

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 Joint Personnel Adjudication System (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 16020-0168s

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.

SECURITY EDUCATION AND TRAINING
NEW INSIDER THREAT VIGILANCE SERIES VIDEO NOW AVAILABLE

CDSE is pleased to present the Insider Threat Vigilance Video Series: Season One "Turning People Around, Not Turning Them In." Episode Two, “Check Out My New Ride” is available now on CDSE.edu and the CDSE YouTube channel.

The Insider Threat Vigilance Video Series aids the workforce in identifying and reporting insider threat indicators. The series also provides an overview of Insider Threat Programs and their multi-disciplinary approach to gathering and reviewing information indicative of an insider threat, referring that data as appropriate, and developing mitigation response options all while protecting the privacy and civil liberties of the workforce. Each episode in the series is approximately 8-9 minutes long.

The videos are accompanied by a facilitation guide to enhance group discussion. These resources make a great training event, town hall opener, or "lunch and learn" session. Individual students can also access a Micro-Learning Video Lesson on their own to watch the video, answer questions, and access additional resources.

Additional episodes will be released in December and January. Binge watching optional!

YouTube - https://youtu.be/E9w9bDyH1rU
Video Lesson - https://www.cdse.edu/micro/vigilance-episode2/vigilance-episode2.html

RECORDINGS RELEASED FOR 2018 DOD VIRTUAL SECURITY CONFERENCE FOR INDUSTRY

The recordings for the 2018 DoD Virtual Security Conference for Industry held on September 19, 2018 are now available. Please use the following link to register and log into Adobe Connect to view the recordings: http://cdse.adobeconnect.com/dvsci2018-record/event/registration.html.

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 second iteration for the FY19 schedule is currently open for registration. Check out the course below to see if it meets your training needs.

February 5-6, 2019, Linthicum, MD, https://www.cdse.edu/catalog/classroom/IS121-feb2019.html.

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). Registration procedures have changed so request registration for the course as soon as possible. Once approved, submit your visit request no earlier than 60 days prior to the course starting (on or after December 7, 2018).

Come join us in the Nation's Capital!

UPCOMING SPEAKER SERIES

CDSE invites you to participate in our upcoming Speaker Series:

Applied Research on Exfiltration and Security
Thursday, January 17, 2019
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 January 17, 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.

SOCIAL MEDIA

Connect with CDSE on Twitter and on Facebook.