DSS Monthly Newsletter
October 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 September 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 completing 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 (CDSE) offers insider threat training, eLearning courses, and job aids at: https://www.cdse.edu/catalog/insider-threat.html.

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 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.

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 anticipated to begin 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 (OBMS). 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 two 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:

“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.”

RISK MANAGEMENT FRAMEWORK RESOURCE CENTER

Visit the Risk Management Framework Information and Resources page at www.dss.mil/rmf for the latest information and resources.

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 has adopted 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.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.

VERIFY THE IDENTITIY 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 Critical Infrastructure Services Inc
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 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 GUIDANCE FROM DSS

Additional DISS Tips & Tricks to assist users with provisioning subordinate users, hierarchy set-up/management, and the submission of 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.

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 16020-0168

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.

SECURITY EDUCATION AND TRAINING

STEPP HAS MOVED

Visit https://cdse.usalearning.gov to view the new location. Any questions regarding your username or login help please contact (202) 753-0845 within the Washington, DC area or toll free at (833) 200-0035 (Weekdays 8:30AM to 6:00 PM Eastern Time).

NEW SECURITY PRINCIPLES VIDEO RELEASED

The recently launched “DoD Security Principles” video describes CDSE support to the Defense Security Enterprise (DSE). This video explains how the Department of Defense’s security disciplines and associated programs (Personnel Security, Physical Security, Information Security, Cybersecurity, Special Access Programs, Counterintelligence, Insider Threat, Operations Security, and Industrial Security) serve as the pillars of the DSE. View the video at https://www.cdse.edu/micro/security-principles/security-principles.html

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 One 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 November, December, and January. Binge watching optional!

YouTube - https://www.youtube.com/watch?v=Kr2QAdHBMB4&feature=youtu.be
Video Lesson - https://www.cdse.edu/micro/vigilance-episode1/vigilance-episode1.html

FSO TOOLKIT UPDATED

The FSO TOOLKIT has been updated! The Toolkit now includes the Asset Identification/Security Baseline, Supply Chain Risk Management (SCRM), and Insider Threat categories. The Asset Identification/Security Baseline category contains resources that will assist your facility in identifying assets and completing a security baseline. The SCRM category of the toolkit provides additional key resources that will assist a contractor during a Comprehensive Security Review or an Enhanced Security Vulnerability Assessment.

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

November 13-14, 2018, Washington, DC, https://www.cdse.edu/catalog/classroom/IS121-nov2018.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).

Come join us in the Nation’s Capital!

NEW CYBERSECURITY eLEARNING GAME

In support of National Cyber Security Awareness Month, a collaborative effort between government and industry to raise awareness about the importance of cybersecurity, CDSE has released a new eLearning Game “Cybersecurity Trivia Twirl.” Access this game at https://www.cdse.edu/toolkits/cybersecurity/training.html.

DOD VIRTUAL SECURITY CONFERENCE FOR INDUSTRY

On September 19, the Defense Security Service (DSS) hosted the inaugural DoD Virtual Security Conference for Industry for over 1,300 Industry partners, including participants in Europe, South America, and Asia. The goal of the virtual conference was to continue to bolster the DSS partnership with industry and encourage greater collaboration and trust. The virtual environment facilitated this collaboration and participants were able to submit questions in real time. A total of 480 questions were submitted over the course of the eight hours.

Topics included the Undersecretary of Defense for Intelligence perspective on the changes to DSS and the importance of thwarting the insider threat, the evolution of industrial security oversight, a panel discussion on information sharing in insider threat programs, the NISP RMF process, updates on the Defense Vetting Directorate and the NISS and DISS systems, and Controlled Unclassified Information.

These briefings and panel discussions come at an important time in our history. We hope this will be the first of many industry conferences to come.

SOCIAL MEDIA

Connect with CDSE on Twitter and on Facebook.