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

GUIDANCE FOR SECURITY EXECUTIVE AGENT DIRECTIVE 4 (SEAD 4)

On December 10, 2016, the Director of National Intelligence signed SEAD 4, "National Security Adjudicative Guidelines," which became effective on June 8, 2017. SEAD 4 establishes the single common adjudicative criteria for all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position. The guidelines reflected in the SEAD 4 supersede all previously issued national security adjudicative criteria or guidelines. The SEAD 4 guidelines may be found here.

This guidance provides for Industry implementation of the SEAD 4 Adjudicative Guidelines related to the disposition of foreign passports belonging to cleared employees that have been retained by contractors in accordance with prior DoD directions or decisions under the former Adjudicative Guidelines. In accordance with SEAD 4, cleared contractors will not be asked by the DoD Consolidated Adjudications Facility (CAF) to routinely retain or destroy foreign passports and/or identity cards as a means of mitigating security concerns for individuals who maintain dual citizenship with other countries.

In order to implement SEAD 4, cleared contractors who have retained a cleared employee's foreign passport or identity card based on prior DoD directions or personnel security adjudicative decisions should return the foreign passport or identity card to the cleared employee.

Upon returning the foreign passport or identity card to the cleared employee, the facility security officer, or designated JPAS user acting on behalf of the contractor, will remind the cleared employee of their legal responsibility to enter and exit the United States bearing a U.S. passport.

The cleared contractor will submit incident reports if any cleared employees report use of a foreign passport to enter or exit the United States.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) DEPLOYS OCTOBER 8, 2018!

The transition from e-FCL and ISFD to NISS is fast approaching! NISS will be available for Industry and Government partners on October 8, 2018. Do not attempt to register for your NISS account prior to this date.

*** Please visit the NISS webpage for important guidance during the transition period: http://www.dss.mil/is/niss.html. ***

CLASSIFIED INFORMATION SYSTEM (IS) SUBMISSION GUIDANCE REMINDER

The DSS Assessment and Authorization Process Manual (DAAPM) guidelines highly recommend submitting requests for classified IS packages 90 days before system operational need. This includes both re-authorization IS packages and new IS packages. Following this guidance will make sure there is enough time for appropriate DSS review, ISSP/ISSM interaction and DSS validation of the IS. The intent is to ensure NISP Industry partners can support their government customers. Last minute submissions impact other NISP Industry partners.

DELAYED: ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (E-MASS)

The transition to eMASS as the DSS system of record for NISP information system 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 new accounts and become familiar with the 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 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 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. NISP partners are reminded to get access and complete the required DISA computer based training. 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 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".

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 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 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.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 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 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 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 OFFICER 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

JPAS Records Management

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.

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 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.

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.

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 8/27/18, 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

STEPP will be unavailable through September 30, as we prepare for the migration to the new platform:

- Records and transcripts will migrate to the new system
- Courses currently in progress won't carry over
- Current users with updated profiles will receive an email the week of 24 September to access the new site

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 perspective from Office of the Under Secretary of Defense for Intelligence on the changes to DSS and the importance of thwarting the insider threat, the evolution of industrial security oversight, 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.

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 Facility Security Officers (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. Registration is NOW OPEN for the first iteration of FY19 held on November 13-14, 2018, in the Washington, D.C., area. REGISTER NOW!

If you cannot make this iteration, please check out alternative dates and locations that may work for you.

If your facility is located in the Northern Region and you are interested in hosting this course with CDSE's certified instructor staff on August 13-14, 2019, please send an email to our CDSE mailbox (dss.cdsetraining@mail.mil).

COUNTERINTELLIGENCE AWARENESS

Our national defense and strategic advantage are largely dependent upon technologies and capabilities developed and manufactured by our defense industrial base. Industry manufactures the capabilities that are placed in the hands of warfighters to defend our country. Warfighters must have the confidence that those capabilities will do what they are supposed to do when they are employed. Today, the defense industrial base is under attack. Our adversaries are stealing vast amounts of critical technology that jeopardize our mission readiness, the safety and security of our warfighters, and the security of our citizenry. The volume of these losses is both unprecedented and unsustainable. In some areas, our adversaries have stolen technologies, improved them, and moved past us, giving them a technological edge.

Ensuring a more capable, resilient, and innovative defense requires that capabilities developed and produced by the defense industrial base are delivered to the warfighter uncompromised. CDSE delivers training and awareness products that can help protect the technology at your facility and throughout the supply chain. See our latest releases below:

New Video - Deliver Uncompromised: OUSD(I) Response to Military Technology Transfer
https://www.cdse.edu/micro/uncompromised-military-tech/uncompromised-military-tech.html

New Video – Deliver Uncompromised: DSS CI discusses Supply Chain Risk Management
https://www.cdse.edu/micro/uncompromised-supply-chain/uncompromised-supply-chain.html

New Job Aid – Deliver Uncompromised: Supply Chain Risk Management
https://www.cdse.edu/micro/uncompromised-supply-chain/uncompromised-supply-chain.html

SOCIAL MEDIA

Connect with CDSE on Twitter and on Facebook.