DSS Monthly Newsletter
January 2019

(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.

SECURITY RATING SCORE

DSS is developing a new Industry rating model, called the "Security Rating Score" (SRS), to further the DSS, DoD, and National Security goal of Delivering Uncompromised and support DSS' focus on Critical Technology Protection. The SRS is also a critical component of DSS' effort to move toward a more risk-focused assessment of Industry. DSS aims to elevate security as the fourth pillar in the acquisition process to prioritize and cultivate a culture of security in Industry organizations.

Though we are still in the beginning phases of development, in the spirit of transparency, I wanted to provide you all an update on our progress. The SRS model has been in the works for over a year. Through our studies, analysis, and internal discussions, we have refined the model to its current iteration. In the month of February, we will be conducting four dry run sessions with select industry partners to learn and gain feedback from Industry before conducting a limited pilot this spring. The learnings from these dry runs will inform our next phase of model development.

DSS considered many factors in selecting the dry run partners to ensure representation from all four geographic regions, a mix of small, medium, and large organizations, and FOCI and non-FOCI companies, among other factors.

As we solidify the content of the model and details for implementation, we will keep you all updated. DSS is committed to delivering a model that is defendable, objective, and repeatable and, most importantly, supports the goals of Deliver Uncompromised.

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 January 30, 2019, DSS has completed comprehensive security reviews at the majority of facilities identified for phased implementation of DiT. The fourth and final phase of implementation is now concluding and DSS will continue using the new methodology throughout 2019, expanding its use at a larger number of cleared facilities supporting select priority technologies.

Since November 2018, DSS field personnel have been in the process of engaging with cleared industry to validate the presence of these technologies at their locations and are continuing to schedule comprehensive security reviews at validated locations in 2019.

DSS received a significant amount of feedback from both DSS participants conducting comprehensive security reviews as well as industry partners participating in these reviews. This feedback has been analyzed and the DSS staff has started to make adjustments to the DiT process to support its execution on a broader scale. This will support the protection of a larger number of critical technologies.

DSS will soon be updating the "DSS in Transition" page on the DSS website to include additional resources and tools to educate industry and enable the proactive development of tailored security programs. The Center for Development of Security Excellence has made available several resources for cleared industry to begin utilizing in support of the new DiT methodology. This includes the publishing of an Asset Identification Guide, PIEFAO-S Job Aid, Industrial Base Technology List, and Supply Management Risk Management resources. These resources and many more can be found here: https://www.cdse.edu/toolkits/fsos/asset-id.html.

For more information on DiT, please visit the DSS website at: https://www.dss.mil/ma/ctp/io/dit/

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 meaningful security engagement. 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 meaningful 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 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 NISP oversight, industry is encouraged to work directly with local field office representatives on any questions or concerns they have.

INSIDER THREAT PROGRAM EFFECTIVENESS

DSS is finalizing procedures to evaluate the effectiveness of cleared industry insider threat programs. These procedures will review 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 will be evaluated by reviewing program requirements, assessing program implementation, and determining effectiveness of the programs. DSS anticipates finalizing its process for evaluating insider threat effectiveness in early 2019 and will train DSS personnel and communicate the process to industry prior to implementation.

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.

DSS RELEASES ISL 2019-01 "FOREIGN PASSPORTS – SEAD 4"

ISL 2019-01 replaces the September 2018 notice on Security Executive Agent Directive (SEAD) 4 posted to the DSS web site. The ISL provides additional guidance to industry on the implementation of SEAD 4 Adjudicative Guidelines related to the disposition of foreign passports belonging to cleared employees that have been previously retained by contractors in accordance with DoD directions and the former Adjudicative Guidelines. The ISL can be accessed at: https://www.dss.mil/Portals/69/documents/io/nisp_lib/ISL2019-01_ForeignPassports_SEAD4.pdf.

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) 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. DSS encourages Industry members to establish their NISS account, especially in preparation for the Personnel Security Investigation Projections survey in March 2019.

For instructions on how to register, please visit the Registration section on the NISS website: https://www.dss.mil/is/niss/. 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.

We appreciate your patience as we work through a large volume of questions and inquiries sent to the NISS team. We apologize for the delay in response as we are working diligently to provide a quality reply as soon as possible.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) FOR PERSONNEL SECURITY INVESTIGATIONS DATA COLLECTION TO INDUSTRY

The Defense Security Service (DSS) is responsible for projecting Personnel Security Investigations (PSI) requirements each year. The data collection for PSI projection requirements will be conducted and available in March 2019 through the National Industrial Security System (NISS) Submission Site. Annual projections acquired from Industry through this collection are the key component in Department of Defense program planning and budgeting for NISP security clearances.

In preparation for this upcoming data collection, please ensure that you register for your NISS account prior to March 2019 in order to participate in the survey. Registration instructions are found on the NISS website under the Registration section (https://www.dss.mil/is/niss/).

Additional instructions and information regarding the PSI data collection will be forthcoming prior to deployment. We look forward to your participation. If you have any questions, please contact: dss.ncr.dss.mbx.psiprogram@mail.mil.

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

ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (E-MASS) UPDATE

The eMASS transition is tentatively scheduled to begin March 25, 2019. Until then, NISP industry partners should continue to submit all System Security Plans and supporting artifacts via the ODAA Business Management System (OBMS). Work with your local ISSP and/or ISSP Team Lead to complete the required eMASS training to ensure readiness for the transition.

NAO has created and released a Job Aid for cleared industry partners to obtain sponsorship and access to the DISA training web site in order to prepare for the transition to eMASS. The Job Aid is located in the NISP RMF Resource Center link on the DSS website home page.

The following is the procedure to request a NISP-eMASS account:
1. Complete DISA eMASS Computer Based Training (CBT)
2. Complete DISA Cyber Awareness Challenge (CAC) training
3. Complete DSS IO (pre-populated) System Authorization Access Request (SAAR) form
4. Submit completed artifacts to DSS NAO eMASS mailbox
dss.quantico.dss.mbx.emass@mail.mil

Questions and inquiries are handled through the NAO eMASS mailbox at dss.quantico.dss.mbx.emass@mail.mil.

OUR GPO TOOL HAS A NEW NAME

The NAO Windows Configuration Toolkit Group Policy Object (GPO) has been updated and released as the NISP Classified Configuration (NCC), effective January 5, 2019. The updated NCC will bring an out-of-box Windows 7/10 – 32 or 64 bit and Windows Server 2012/2016 installations within 95 percent compliance with automated security checks. The updated NCC is available in the Headquarters bulletin Board within OBMS and will be made available on the NISP eMASS instance once the transition begins. NAO may in the future leverage the use of the NCC to facilitate submission of proposal system plans under the Risk Management Framework in order to provide an efficient and responsible means of quickly hardening standalone proposal system submissions for authorization.

NAO ATTENDANCE AT NCMS 2019

NAO has been invited to NCMS 2019 to host the NAO Helpdesk and to provide presentations on the following: NAO Update; NAO Enterprise Wide Area Network Initiative; NISP Enterprise Mission Assurance Support Service (eMASS), our new authorization application. We are looking forward to attending and interacting with our NISP industry partners. See you there!

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 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.

FILLING IN THE PRIME CONTRACT NUMBER FIELD IN JPAS WHEN SUMITTING PERSONNEL SECURITY CLEARANCE INVESTIGATIONS

Beginning February 1, 2019, DSS may reject investigation submissions that don't include the prime contract number, as shown on the associated industry guidance. The prime contract number is a required field in the Joint Personnel Adjudication System for personnel security clearance investigations. Please contact the VROC Knowledge Center for questions (888) 282-7682, select option #2.

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

At this time, DSS is now provisioning users for any facilities that have not yet been provisioned; 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 that can be found on both the recent news section of the DSS and VROC DISS webpages; 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 continue to perform a Data Quality Initiatives (DQIs). Please ensure the records of all employees are recorded accurately in the Joint Personnel Adjudication System (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, Defense Central Index of Investigation, Secure Web Fingerprint Transmission, 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: https://www.dss.mil/contact/foia/foia_privacy/.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE) TRAINING

DSS IN TRANSITION (DiT) WEBINAR SERIES

Please join CDSE in its second installment of the DiT webinar Series, "The Evolution of the FSO Role." This is the second of seven webinars in a series designed to increase industry partner awareness and understanding of the DSS in Transition methodology and their role in it. This webinar will be a panel interview of a Facility Security Officer (FSO) and a DSS Industrial Security Representative as they discuss how the role of the FSO changes to address an intelligence-led, threat-driven, and asset-focused methodology.

The Evolution of the FSO Role
Thursday, February 14, 2019
12:00 - 1:00 p.m. ET

If you missed our first DiT webinar, "Overview of the DSS in Transition Methodology," you can find it here, along with many other previously recorded webinars. This webinar discussed an overview of the DiT methodology and DSS' 2019 lines of effort.

Don't forget to mark your calendars for these upcoming DiT webinars. Registration opens 30 days in advance of each webinar.

NEW INSIDER THREAT VIGILANCE SERIES VIDEO NOW AVAILABLE

CDSE is pleased to present the Insider Threat Vigilance Video Series: Turning People Around, Not Turning Them In, Season One / Episode Four: “Meeting of the Minds” is now available now at CDSE.edu.

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 are located in on our Insider Threat Vigilance page.

UPCOMING SPEAKER SERIES

CDSE invites you to participate in our upcoming Speaker Series:

Maximizing Organizational Trust
Thursday, February 7, 2019
12:00 – 1:00 p.m. ET

The Defense Personnel and Security Research Center (PERSEREC) has published a new eLearning course and associated guide on the importance of organizational trust in creating a safe work environment. This 1-hour webinar will address the importance of organizational trust, highlight important lessons from the course, and discuss use of the guide. The webinar is free for all participants. Register here.

Critical Technology Protection | Foreign Visits and Academic Solicitation
Thursday, February 21, 2019
11:00 a.m. – 12:00 p.m.

This webinar will feature a conversation with Defense Security Service (DSS) Special Agent (counterintelligence) Justin Shanken discussing the threat environment, techniques adversaries may use to target our critical assets, and what industry can do to be prepared to counter this threat. DSS Counterintelligence Directorate and Regional Field Offices provide support for Foreign Visits and Academic Solicitation for the Defense Industrial Base. The webinar if free for all participants. Register here.

NEW INSIDER THREAT COURSE RELEASED

To further build off our February 7 webinar regarding Maximizing Organizational Trust, we just released a course on the same topic. As you know, employees are an organization’s first line of

defense against threats to the mission or to the safety of the workforce. In order to motivate employees to actively participate in security and safety initiatives, organizational leaders must create an environment in which personnel trust leadership to be fair, honest, and transparent. In response to a tasking from the Office of the Under Secretary of Defense for Intelligence (OUSD[I]), the Defense Personnel and Security Research Center (PERSEREC) reviewed business, psychology, and communication literature to identify best practices for building and maintaining organizational trust. Sign up to take the free, 60 minute class today.

SOCIAL MEDIA

Connect with CDSE on Twitter and on Facebook.