DSS Monthly Newsletter
February 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, other important forms, and guides are archived on the Defense Security Service (DSS) website, Industry Tools page.

DSS IN TRANSITION (DiT)

DSS continues to use its new comprehensive security review methodology in 2019, expanding its use at a larger number of cleared facilities and 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 significant feedback from industry partners and DSS participants conducting comprehensive security reviews. DSS staff analyzed the feedback and has started making adjustments to the DSS in Transition (DiT) process to support the execution on a broader scale. The DSS workforce will receive training on these adjustments at the Operational Training Events (OTEs) in April 2019. Continued adjustments and refinements to the DiT process support the protection of a larger number of critical technologies resident in cleared industry.

In March, DSS plans to update the "DSS in Transition" webpage to include additional resources and tools to educate and enable the proactive industry development of tailored security programs. The Center for Development of Security Excellence (CDSE) has several resources created for cleared industry to utilize in support of the DiT methodology. This includes the following: an Asset Identification Guide; People Information Equipment Facilities Activities Operations Suppliers (PIEFAOS) Job Aid; Industrial Base Technology List; and Supply Chain 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/.

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 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 program effectiveness. The draft DSS Industrial Security Letter (ISL) provides industry with detailed guidance and instruction on evaluating the insider threat program effectiveness. DSS anticipates finalizing the insider threat evaluation process effectiveness in early 2019. DSS will train personnel at the OTE in April 2019 in advance of communicating the process to industry. Implementation plans will be released at a later date.

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 facility clearance issue resolution at the local level. This includes general questions and requests for support. In these instances, industry should contact the assigned DSS Industrial Security Representative (ISR) for assistance. For any issues that cannot be resolved at this level, industry may engage the DSS field office and regional leadership for issue resolution.

As a reminder, the DSS Knowledge Center is also able to assist industry with facility clearance questions regarding the FCL process and status updates. The Knowledge Center can be reached at (888) 282-7682, Option #3. Please note the Knowledge Center is closed on weekends and on all federal holidays.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) INFORMATION

The National Industrial Security System (NISS) is the current system of record for facility clearance (FCL) information. NISS launched for external users on October 8, 2018. The ISFD and e-FCL applications are no longer available. All official business such as: reporting change conditions, performing FCL verifications, and submitting FCL sponsorship requests, are to be submitted via the NISS. DSS encourages industry members to establish the NISS accounts in preparation for the Personnel Security Investigation Projections survey in March 2019.

For account registration instructions, please visit the Registration Section on the NISS support website at: https://www.dss.mil/is/niss/. If you encounter registration issues: 1) Contact the DSS Knowledge Center at (888) 282-7682, Select Option 1, and then 3) Select Option 2.

After obtaining your NISS account, NISS Dashboard provides direct access to training resources. Training 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.

The NISS team appreciates your patience as as a volume of questions and inquiries are under action. The team is working diligently to provide a quality responses as soon as possible.

PSI REQUIREMENTS FOR INDUSTRY DATA COLLECTION THROUGH NISS

DSS is responsible for projecting Personnel Security Investigations (PSI) requirements each year. The PSI projection data requirements will be collected March 11 through April 5, 2019 via the National Industrial Security System (NISS) Submission Site. Annual industry projections acquired are the key component in DoD program planning and budgeting for National Industrial Security Program (NISP) security clearances.

In preparation, the industry partners' registration is encouraged for NISS accounts prior to March 11. Registration is required to participate in the survey. Registration instructions are found on the NISS website under the Registration Section at: https://www.dss.mil/is/niss/. For NISS Registration or survey questions, please contact: https: dss.ncr.dss.mbx.psiprogram@mail.mil.

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

NAO DELAYED RELEASE OF THE ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (eMASS)

The Enterprise Mission Assurance Support Service (eMASS) transition is postponed until May 6, 2019. Cleared industry partners should continue to work with the assigned Information Systems Security Professional (ISSPs) and team leads to complete the required training to request a NISP eMASS account. User registration and accounts ensure transition readiness. NISP eMASS job aids are posted on at: https://www.dss.mil/ma/ctp/io/nao/rmf/.

The DSS Assessment and Authorization Process Manual (DAAPM) Version 2.0 release will be delayed as a result of the eMASS transition postponement. Industry will have 30 days to review the updated policy prior to the effective date. The revised release date is April 8, 2019 and with a projected effective date of May 6, 2019.

Industry partners will continue to submit all System Security Plans (SSP) and supporting artifacts via the ODAA Business Management System (OBMS).

Questions and inquiries regarding eMASS are handled through the NISP Authorizing Office (NAO) eMASS Mailbox at: dss.quantico.dss.mbx.emass@mail.mil.

Submit questions and inquiries regarding the DAAPM to the NAO Mailbox at: dss.quantico.dss-hq.mbx.odaa@mail.mil.

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

In early June 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 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 a 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 provided here for ease of reference. If you encounter any challenges with this process, please email dss.ncr.dss-dvd.mbx.askvroc@mail.mil for assistance.

These procedures will remain in effect until further notice

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 the NBIB has processed the fingerprints by checking SII in JPAS that 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. When submitting personnel security clearance investigations, fill in the 'Prime Contract Number' field in JPAS.

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 JPAS for personnel security clearance investigations. Please contact the Vetting Risk Operations Center (VROC) for questions at (888) 282-7682, and select option #2.

SECURITY OFFICE IDENTIFIER (SOI) CODE UPDATES FOR 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

DISS DEPLOYMENT GUIDANCE FROM DSS

At this time, DSS is now provisioning users for 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 Defense Information System for Security (DISS) Joint Verification System (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 DISS Tips & Tricks for helpful hints and answers to frequently asked questions.

As JPAS continues to transition to DISS in an ongoing effort to enhance data quality, JPAS will continue to perform Data Quality Initiatives (DQIs). Please ensure the records of all employees are recorded accurately in the JPAS.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE) TRAINING

NEW INSIDER THREAT COURSES RELEASED

INT240 Basic Insider Threat Hub Operations. The Insider Threat Basic Hub Operations course provides Insider Threat Program Managers and operations personnel with an overview of Insider Threat Hub operations and proactive approaches to deter, detect, mitigate and report the threats associated with trusted insiders. The course explains the roles and purpose of an Insider Threat Hub and Insider Threat Hub management process details. Designed for insider threat program personnel in industry, DoD, and federal agencies.

INT250 Critical Thinking for Insider Threat Analysts. The Insider Threat Critical Thinking for Analyst course provides a high-level explanation of analytical and critical thinking as related to producing comprehensive analytic products for insider threat programs. Users learn how critical thinking tools visually structure, facilitate, and empower thinking to help explain uncertainties, conclusions and judgments. This course will give users the skills to help support their insider threat program in the deterrence, detection, and mitigation of insider risks while protecting the privacy and civil liberties of the workforce.

INT260 Privacy and Civil Liberties for Insider Threat. The Insider Threat Privacy and Civil Liberties course provides a high-level explanation of the importance that civil liberties, privacy laws, regulations, and policies have on conducting insider threat program actions. This course identifies the information protected by law and how to safeguard information. The user is introduced to insider threat challenges that impacting socially charged matters regarding civil liberty laws and policies, unauthorized disclosure, whistleblowing, protected speech, and threats of violence.

These courses are designed for insider threat program personnel in industry, DoD, and federal agencies. Enroll today.

NEW INSIDER THREAT AWARENESS POSTER

Download our new "Effective Mitigation" poster to encourage reporting and awareness by highlighting the Insider Threat Program role in effective Risk Mitigation. Access all of CDSE's Insider Threat posters https://www.cdse.edu/resources/posters-insider-threat.html.

DSS IN TRANSITION (DiT) WEBINAR SERIES

Please join CDSE in its third installment of the seven DiT webinar series, *Asset Identification and Your Security Baseline*. The series is designed to increase industry partner awareness and understanding of the DSS in Transition methodology and their role. This webinar presents a panel interview of DSS field representatives discussing best practices in asset identification and in completing a Security Baseline. The panel addresses the definition of a national security asset, approaches to asset identification, and available resources to assist in the completion of a Security Baseline

Asset Identification and Your Security Baseline
Thursday, March 28, 2019
12:00 - 1:00 p.m. ET

If you missed our first and second DiT webinars, *Overview of the DSS in Transition Methodology*, and *Evolution of the FSO Role*. The webinars are located https://www.cdse.edu/catalog/webinars/webinar-archives.html, along with many others.

Don't forget to mark your calendars: https://www.cdse.edu/catalog/webinars/index.html for these upcoming DiT webinars. Registration opens 30 days in advance of each webinar.

UPCOMING SPEAKER SERIES

CDSE invites you to participate in our upcoming Speaker Series:

Positive Outcomes in Insider Threat Programs
Thursday, April 4, 2019
12:00 – 1:00 p.m. ET

Join CDSE and special guests from U.S. Special Operations Command as we highlight positive outcomes from the Insider Threat community. Counter insider threat programs (ITPs) emphasize awareness and reporting, early intervention, and effective risk mitigation. As ITPs have matured from an initial stand up to a more sophisticated operating capability, the benefits to individuals, organizations, and national security has manifested in a variety of positive outcomes. Learn more at the live webinar on April 4 at noon Eastern. Join us and be part of the conversation! The webinar is free for all participants. Register here.

Supply Chain Resilience
Thursday, April 25, 2019
12:00 – 1:00 p.m. ET

CDSE hosts the National Counterintelligence and Security Center for a discussion on foreign intelligence entity (FIE) supply chain exploitation. FIE uses this method to target U.S. equipment, systems, and information used every day by government, businesses, and individual citizens. Learn more about the risk and your role in recognizing and reporting suspicious activity. Supply chain resilience is everyone's responsibility. Join us and be part of the conversation. Register here.

NEWLY ARCHIVED SPEAKER SERIES

Did you miss our January and February Speaker Series? No problem! Access the following archived Speaker Series:

Applied Research on Exfiltration and Security
Maximizing Organizational Trust
Critical Technology Protection | Foreign Visits and Academic Solicitation

Check out all of our Speaker Series and webinars in the On Demand Webinars to include CDSE Certificate of Training and the Previously Recorded Webinars
These do not include a certificate.

CDSE FY18 YEAR END REPORT NOW AVAILABLE

The CDSE had a busy fiscal year (FY18). Activities included: hosting the DoD Security Conference, and DoD Virtual Security Conference for Industry; new learning management system (LMS) implementation; Industrial Security Oversight Certification (ISOC) and Adjudicator Professional Certification (APC) accreditations; connecting security expertise with the community; and much more. Check out the FY18 Year End Report to see the complete accomplishments.

CDSE 2019 CI VIGILANCE CAMPAIGN – MARCH | FOREIGN COLLECTION METHODS

A Counterintelligence (CI) Vigilance Campaign is an ongoing, continual communication program that uses a variety of communication platforms such as posters, videos, briefings, and internet sites to keep CI Awareness and reporting requirements in the forefront for personnel. CDSE provides a toolkit each month with products that help outline specific CI topics. The products being showcased for the month of March 2019 are:

Poster: Foreign Collection Methods

Job Aid: Foreign Collection Methods: Indicators and Countermeasures

Learning Awareness Game: Counterintelligence Trivia Twirl

CDSE 2019 INSIDER THREAT VIGILANCE CAMPAIGN – MARCH | FOREIGN INTELLIGENCE ENTITY

An Insider Threat Vigilance campaign is an ongoing, continual communication program that uses a variety of communication platforms such as posters, videos, briefings, and internet sites to keep Insider Threat Awareness and Reporting Requirements in the forefront for personnel. The products being showcased for the month of March 2019 are:

Job Aid: Foreign Intelligence Entity Targeting Recruitment Methodology

Case Study: Walter Liew

Video: Insider Threat Training Scenarios

SOCIAL MEDIA

Connect with CDSE on Twitter and Facebook.