DSS Monthly Newsletter
**March 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.

## RISK-BASED INDUSTRIAL SECURITY OVERSIGHT

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. Historically referred to as "DSS in Transition" (DiT), this methodology is part of the larger DSS effort in conducting Risk-based Industrial Security Oversight in support of critical technology protection. As DSS moves from transition to transformation, the DiT lexicon will begin to be phased out.

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 (CSRs) at validated locations in 2019. These reviews will be focused at cleared industry locations supporting the following technology categories from the Industrial Base Technology List (IBTL): Armament and Survivability; Command, Control, Communication, and Computers; Energy Systems; Electronics, Positioning, Navigation, and Time; Materials Raw and Processed; Space Systems; and Software.

DSS continues to receive significant feedback from industry partners and DSS participants conducting CSRs. DSS staff analyzed the feedback and has started making adjustments to the 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 will result in greater efficiencies, supporting the broader use of the methodology and protection of a larger number of critical technologies resident in cleared industry.

In the weeks ahead, DSS will be updating the DiT 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 has created 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 Risk-Based Industrial Security Oversight, please visit the DSS website at: https://www.dss.mil/ma/ctp/io/dit/.

## CERTIFICATE PERTAINING TO FOREIGN INTEREST (SF 328)

On November 2018, the certificate pertaining to Foreign Interests was updated. There were revisions made to capture the DoD Enhanced Security Program as well as the DHS Classified Critical Infrastructure Protection Program. Industry can begin to use this form immediately as there were no additional changes made. To access the form, visit the General Services Administration website at https://www.gsa.gov/node/32986. The current SF 328 forms will remain effective additional changes are made. Industry should utilize the new SF 328 form when reporting any changes to their foreign ownership, control, or influence.

## DERIVATIVE CLASSIFICATION TRAINING

As of January 31, a reference was made to the DoD Memorandum, Derivative Classification Training. The memorandum applies to DoD government personnel, unless otherwise directed by a government customer. The National Industrial Security Program Operating Manual requirement for biennial derivative classification training remains the same. 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. An Industrial Security Letter is currently in coordination, which, upon release, will provide industry with detailed guidance and

instruction on evaluating the insider threat program effectiveness. DSS will train its personnel at OTEs in April 2019 in advance of communicating the process to industry.

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 security clearance (FCL) 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 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

As an enhancement to NISS training and ease of use, we have developed a list of NISS frequently asked questions (FAQs). Many of the challenges for NISS users can be successfully addressed through self-help, speeding up access to NISS usability and resources. These FAQs can be found on the NISS website. Topics include: Registration, Navigating the System, Troubleshooting, Facility Profile, FCL Package, and Training.

Please continue to check the Dashboard, Knowledge Base and STEPP training before contacting the NISS Support Team. We are updating these resources with products and information based on most frequently asked questions.

## NISP PSI DATA COLLECTION IS NOW OPEN IN THE NISS

DSS is responsible for projecting PSI requirements each year. The data collection of NISP PSI projections is now open and can be accessed through NISS. Annual projections acquired from Industry through this collection are the key component in DoD program planning and budgeting for NISP security clearances.

To submit your projections, please log into the NISS Application. A PSI Job Aid is available on the NISS Dashboard (after you have logged in) to assist in completing the collection. For more information about logging in or establishing your NISS account, please visit the "Registration" section of the NISS page on the DSS public website. (https://www.dss.mil/is/niss). Additional support for registration and access issues can be provided by the DSS Knowledge Center, 1-888-282-7682, select Option 1 then Option 2.

Please note that submitting your PSI projections is independent of any other NISS package submissions; submitting information related to your facility clearance is not required as part of the PSI data collection. All facilities with an active or interim facility clearance may submit their projections now.

Data collection is available from March 11, 2019 through April 5, 2019. We look forward to your participation. If you have any questions about the PSI data collection, please contact the PSI team at: dss.ncr.dss.mbx.psiprogram@mail.mil. All other NISS questions should be sent to DSS.NISS@mail.mil.

## DSS ASSESSMENT AND AUTHORIZATION PROCESS MANUAL (DAAPM) VERSION 2.0 RELEASE

On April 8, 2019, the NISP Authorization Office (NAO) will release the DAAPM version 2.0 which will be posted on the NAO Risk Management Framework Site: https://www.dss.mil/ma/ctp/io/nao/rmf/) under "Policy and Guidance". Version 2.0 becomes effective on May 6, 2019 and supersedes all previous versions of the DAAPM and ODAA Process Manuals.

Questions or concerns should be referred to your assigned Information System Security Professional (ISSP). Send specific questions about the format, content, or general comments todss.quantico.dss-hq.mbx.odaa@mail.mil.

## NISP ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (E-MASS) UPDATE

The NISP eMASS is scheduled to become operational on May 6, 2019. Industry partners should continue to use the ODAA Business Management System (OBMS) until then. Work with your local ISSP and/or ISSP Team Lead to complete the required training to ensure readiness for the transition.

The NISP Authorizing Office (NAO) posted a job aid located in the NISP Risk Management Framework (RMF) Resource Center link on the DSS website for cleared industry to obtain sponsorship.

The following are the step-by-step procedures to request a NISP eMASS account and complete the training:

1. Complete Defense Information Systems Agency (DISA) eMASS Computer Based Training (CBT)
2. Complete DISA Cyber Awareness Challenge (CAC) training
3. Complete DSS Industrial Security Field Operations (IO) (pre-populated) System Authorization Access Request (SAAR) form
4. Submit the completed artifacts (DD 2875 SAAR, CAC certification, and eMASS training completion certification) to DSS NAO eMASS mailbox: dss.quantico.dss.mbx.emass@mail.mil

Send questions and inquiries to the NAO eMASS mailbox at:
dss.quantico.dss.mbx.emass@mail.mil.

## DEFENSE VETTING DIRECTORATE (DVD)

## ELECTRONIC APPLICATION (EAPP) DELIVERS FIRST USER ACCEPTANCE TEST

The eApp has reached a major milestone and is one step closer to achieving operational capability. The eApp is a web-based tool hosted on the National Background Investigation Service (NBIS) Information Technology System, and will eventually replace the electronic questionnaires for investigations processing (e-QIP) system. Built with a user-centric focus in mind, the eApp delivers a user-friendly questionnaire that is intuitive and easier to complete. The eApp is also postured to reduce data inconsistencies and increase throughput by delivering a security questionnaire with a modern, seamless navigation flow.

In November, the Enterprise Business Systems Office (EBSO) spearheaded the first User Acceptance Test (UAT) with the U.S. Army Personnel Security Investigation Center of Excellence (PSI-CoE). What did we learn from it? It produced what tests are designed to produce – challenges and opportunities to improve the tool for a better user experience.

As we continue to gather lessons learned and feedback from our customers, we strive to continuously refine eApp. The UAT enabled us to validate the functional business requirements and focus on eApp's important purpose: improving the quality of investigative questionnaires to support a responsive, risk-based vetting enterprise. We anticipate user testing will continue into spring with product delivery early summer.

## POSITION DESIGNATION TOOL (PDT) UNDERGOES IMPROVEMENT TRAINING

Another application, the Position Designation Tool (PDT), is also undergoing an operational UAT. The PDT provides agencies with a methodical, uniform system to accurately evaluate and assess the appropriate investigative requirement for a national security or public trust position. It is currently available to agencies through the Office of Personnel Management website, and a new application has been developed within the NBIS domain. The new application will offer greater flexibility and allow easier technical modifications to support Trusted Workforce 2.0 enhancements in the future.

Users will experience a seamless migration and have more transparency into what has changed, with a better overall user experience. The application is currently undergoing UAT and will be released to the Suitability and Security Executive Agents (SuitEA and SecEA) for content validation. These activities will provide feedback to the NBIS developers to further refine the tool. The application will be rolled out in phases to all users this spring.

## WHAT IS THE APPLICANT KNOWLEDGE CENTER?

The DSS/DVD, in partnership with the National Background Investigations Bureau (NBIB), is working to expand the current help desk to include an applicant support capability. The Knowledge Center is designed to further educate and assist applicants in the forms completion process. This will improve the quality of the investigative request while simultaneously supporting NBIS development, testing, implementation, and coordination with federal customer agencies. Initially, the sole contact method will be by phone. As the Knowledge Center matures, the strategic plan is to leverage NBIS and incorporate the necessary tools to enhance customer service support, such as help desk instant messaging, a robust website, and eApp resource tool kits. By streamlining and delivering this capability, the Knowledge Center will help mitigate operational impacts and support transformation vetting efforts.

For additional information or for questions regarding the Enterprise Business Support Office, please email us at dss.ebso@mail.mil.

## PROCESSING PRE-EMPLOYMENT CLEARANCE ACTIONS

Per the NISPOM, DoD5220.22M, 2-205, Pre-employment Clearance Action, if access to classified information is required by a potential employee immediately upon commencement of their employment, a Personnel Security Clearance (PCL) application may be submitted to the Cognizant Security Agency by the contractor prior to the date of employment provided a written commitment for employment has been made by the contractor, and the candidate has accepted the offer in writing. The commitment for employment will indicate that employment shall commence within 30 days of the granting of eligibility for a PCL. When filling out the Standard Form 86, Employment History, section 13, it requires individuals to provide ONLY current and previous work location addresses and supervisor names, addresses, and contact information, -- 'NOT Future Employment'.

NBIB provides six tips to filling out the SF86, Employment section 13:
1. List ALL employment beginning with the present and back 10 full years with no breaks. No job is too short or insignificant to list.
2. Do NOT list tentative or future employments.
3. Do not stretch employment dates to fill gaps when you were really unemployed for a month or more.
4. Provide the physical work location.
5. Whether or not you agree, if the employer would say that you were fired, terminated, or left under unfavorable circumstances, list and explain.
6. Discipline, warnings, reprimands, etc. - If you received one, list it (Verbal, written, formal, and informal, etc.)

## IMPLEMENTATION OF INTERIM BACKLOG MITIGATION MEASURES FOR ENTITIES CLEARED BY DOD UNDER THE NISP

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 Agent (Executive Agents), jointly issued a memorandum directing the implementation of interim measures intended to mitigate the existing backlog of personnel security investigations at 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 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 that 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 e-QUIP 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.

## DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) 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 Defense Information System for Security (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 JPAS.

## CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE) TRAINING

### DiT WEBINAR SERIES

Please join CDSE in its fourth installment of the DiT webinar series, "What's different about my Security Review now?" This is the fourth of seven webinars in a series designed to increase industry partner awareness and understanding of the DiT methodology and their role in it. This webinar will be a panel interview of DSS field representatives and will include a discussion of the Counterintelligence Tool being used to deliver threat information to a cleared facility. Business process, supply chain, and asset lifecycle concerns and how they will be assessed will be discussed, as will the Plan of Action & Milestones Framework and how it will be used by industry.

What's different about my Security Review now?
Wednesday, April 24, 2019
12:00 – 1:00 p.m. ET
Register here!

If you missed our first, second, and third DiT webinars, "Overview of the DSS in Transition Methodology," "Evolution of the FSO Role," and "Asset Identification and Your Security Baseline," you can find them all here, along with many other previously recorded webinars.

Don't forget to mark your calendars 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 18, 2019 (New Date)
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 4-18th at noon Eastern Time. 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.

## REGISTER NOW FOR UPCOMING CDSE INDUSTRIAL SECURITY TRAINING

## GETTING STARTED SEMINAR (GSS) FOR NEW FSOS

Seats are available for the "Getting Started Seminar (GSS) for New FSOs," being held in San Diego, California on May 14-15, 2019 - https://www.cdse.edu/catalog/classroom/IS121-feb2019.html.

This course is open to Facility Security Officers (FSOs) and Assistant Facility Security Officers (AFSOs), Security Specialists, and anyone employed in the security environment (such as Human Resources, Administrative Assistants, Program Managers, and Military Members exiting the various Armed Services). A prerequisite course titled "FSO Role in the NISP" is required for all seminar registrations and must have been completed after November 23, 2015. No previous completion of the prerequisite will be accepted.

With our new STEPP system, registration has changed. Please ensure that you have completed both the prerequisite course and associated exam prior to attempting to register for the seminar. Once prerequisite has been completed, register for the course of your choosing. After registration verification has been received from our Registrar's Office, submit a Visit Request through the STEPP system. You will be able to submit a Visit Request 30 days from the start of the course. Please contact the Help Desk if you have any problems with the process, https://cdse.usalearning.gov/blocks/help_desk/newticket.php. Please contact the Course Manager if you have registration questions, dss.cdsetraining@mail.mil.

## NEWLY ARCHIVED SPEAKER SERIES

Did you miss our February and March Speaker Series? No problem! Check out all of our Speaker Series and webinars in the On Demand Webinars (includes CDSE Certificate of Training) and the Previously Recorded Webinars (does not include certificate).

## CDSE 2019 CI VIGILANCE CAMPAIGN – APRIL | SUPPLY CHAIN RISK MANAGEMENT

A Counterintelligence (CI) Vigilance Campaign is an ongoing, continual communication program, using 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. Here are the products being showcased for April 2019:

Video: Know the Risk – Raise Your Shield: Supply Chain Risk Management

Brochure: Exploitation of Global Supply Chain

Toolkit Tab: CI Awareness – Supply Chain Risk Management

## CDSE 2019 INSIDER THREAT VIGILANCE CAMPAIGN – APRIL |

An Insider Threat Vigilance campaign is an ongoing, continual communication program, using 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. Here are the products being showcased for April 2019:

Case Study: SP4 Ivan A. Lopez | Active Shooter

Toolkit: Kinetic Violence Toolkit

Video: Vigilance Video – Season One, Episode Three

## SUPPLY CHAIN INTEGRITY MONTH RELATED COUNTERINTELLIGENCE TOOLKIT

CDSE maintains a robust Supply Chain Risk Management (SCRM) toolkit that contains job aids, policy, training videos, threat awareness products, and best practices as they relate to SCRM. To find these useful products, click here.

## SUPPLY CHAIN INTEGRITY MONTH RELATED COUNTERINTELLIGENCE PRODUCTS

As part of our Deliver Uncompromised Campaign, check out these additional products:

Job Aid: Supply Chain Risk Management

Video**:** Supply Chain Risk Management

Video: Response to Military Technology Transfer

Poster: Supply Chain Resilience

## SOCIAL MEDIA

Connect with CDSE on Twitter and Facebook.