DSS Monthly Newsletter
April 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.

EXECUTIVE ORDER DIRECTING TRANSFER OF INVESTIGATIVE MISSION SIGNED BY PRESIDENT

Consistent with Executive Order 13869, signed on April 24, 2019, the Department of Defense (DoD) will begin a phased transition of the investigations conducted by the National Background Investigations Bureau (NBIB) to DoD. This action will include the transfer of personnel and resources from NBIB to DSS, as authorized by the president of the United States. The transfer of NBIB's operations, personnel, and resources to DoD will commence not later than June 24, 2019, with the transfer completed by Oct. 1, 2019. DSS will be renamed the Defense Counterintelligence and Security Agency (DCSA) and serve as the primary Federal entity for conducting background investigations for the Federal Government. DCSA will also serve as the primary DoD component for the National Industrial Security Program (NISP) and shall execute responsibilities relating to continuous vetting, insider threat programs, and any other responsibilities assigned to it by the Secretary of Defense. NBIB and DSS have and will continue to work in an integrated manner to minimize disruptions to existing missions while beginning the transfer process.

RISK-BASED INDUSTRIAL SECURITY OVERSIGHT (RISO)

DSS continues to use its new comprehensive security review (CSR) 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 to conduct RISO in support of critical technology protection. As DSS moves from transition to transformation, the DiT lexicon will be phased out.

Over the last several months, DSS field personnel have engaged with cleared industry to validate the presence of these technologies at their locations and schedule CSRs. These reviews are currently underway and while 60 of these reviews were conducted in 2018, DSS estimates approximately 150 reviews to be conducted in 2019. These reviews will be focused at cleared industry locations supporting the following Industrial Base Technology List (IBTL) categories: Armament and Survivability; Command, Control, Communication, and Computers; Energy Systems; Electronics; Positioning, Navigation, and Time; Materials: Raw and Processed; Space Systems; and Software.

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 (CDSE) has several resources created for cleared industry to utilize in support of the DiT methodology. This includes an Asset Identification Guide, a Job Aid for People Information Equipment Facilities Activities Operations Suppliers (PIEFAOS); the Industrial Base Technology List, and Supply Chain Risk Management Resources. These resources and many more can be found here.

For more information on RISO, please visit the DSS website.

2019 OPERATIONAL TRAINING EVENTS (OTEs)

DSS recently conducted the first of two OTEs in early April with DSS Western and Southern Region personnel. The second event is currently underway with Capital and Northern Region personnel. The theme of this year's events was "Protecting Critical Technology," where DSS personnel are trained on the new RISO methodology, asset identification, CSRs, the Methods of Contact/Methods of Operation (MCMO) matrix, and many other topics. Personnel also receive briefings on Industrial Security Operations, Defense Vetting, and Counterintelligence. The events also highlight organizational changes and prepared DSS personnel to execute RISO.

IMPLEMENTATION OF SECTION 842 OF FY19 NATIONAL DEFENSE AUTHORIZATION ACT (NDAA)

On April 10, 2019, the Under Secretary of Defense for Intelligence (USD(I)) directed DSS to accelerate the implementation of Section 842 of the NDAA for Fiscal Year 2019. Section 842 allows the Secretary of Defense, in consultation with the Director of the Information Security Oversight Office (ISOO), to waive the National Interest Determination (NID) requirement for a U.S. company operating under a special security agreement (SSA) if the company has:

- an "ultimate parent" located in a country that is part of the National Technology and Industrial Base (NTIB), as defined in section 2500 of Title 10, U.S. Code (Canada, Australia, or the United Kingdom);
- previously been approved for access to proscribed information; and
- a "demonstrated successful record of compliance" with the NISP.

DSS has identified the legal entities that appear to meet the preliminary requirements of that statute and is in the process of reviewing those companies for a demonstrated successful record of compliance with the NISP. Within 30 days, DSS will provide USD(I) with recommendations

for waivers of the requirement to obtain an NID prior to accessing proscribed information under the control and authority of the Secretary, which is limited to Special Access Program Information, Top Secret Information, and, with the approval of the Director, National Security Agency communications security information.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) INFORMATION

Effective immediately, user questions and issues should no longer be sent to dss.niss@mail.mil. If you send a question or issue to the NISS email address, you will receive an automated reply with instructions for who to contact. Users should not expect a reply for routine questions or issues when emailing the NISS box, as these items should be reported by calling the DSS Knowledge Center. When necessary, the Knowledge Center will open IT Service Request Tickets on behalf of external users.

In an effort to improve customer service, all NISS questions and issues should be reported to DSS by calling the DSS Knowledge Center at 888-282-7682 and selecting Option 1, then Option 2. The DSS Knowledge Center hours of operation are Monday through Friday from 8:00AM to 6:00PM EST.

NISP AUTHORIZATION OFFICE (NAO)

DSS will be transitioning cleared industry to the Enterprise Mission Assurance Support Service (eMASS) to provide automated workflows for the execution of Risk Management Framework (RMF). The eMASS is a web-based tool developed by DISA and used by all the military components for executing RMF. On May 6, industry will cease using the ODAA Business Management System (OBMS) and eMASS will become the system of record for assessment and authorization decisions. Questions and inquiries regarding eMASS are handled through the NAO eMASS Mailbox at dss.quantico.dss.mbx.emass@mail.mil.

Several job aids have been created and published for use by cleared industry partners to facilitate the transition. RMF Knowledge Service and eMASS access to the job aids are on the NISP eMASS Information and Resource Center.

The DSS Assessment and Authorization Process Manual (DAAPM) Version 2.0 was released on April 8, 2019, with an effective date of May 6, 2019. The early release provided industry 30 days to review the updated policy prior to the effective date. Questions and inquiries regarding the DAAPM are handled through the NAO Mailbox at dss.quantico.dss-hq.mbx.odaa@mail.mil.

DEFENSE VETTING DIRECTORATE (DVD)
PROCESSING PRE-EMPLOYMENT CLEARANCE ACTIONS

Per the NISPOM, DoD 5220.22M, Subsection 2-205, Pre-employment Clearance Action, if access to classified information is required by a potential employee immediately upon commencement of their employment, a PCL application may be submitted to the CSA 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 (SF) 86, Section 13, Employment Activities, individuals are to provide ONLY current and previous work location addresses and supervisor names, addresses, and contact information, and NOT Future Employment'.

The National Background Investigations Bureau provides six tips to filling out the SF86, Section 13, Employment Activities:

1. List ALL jobs 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 a completed SF86 with the reinvestigation request, 6 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 Dec. 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 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.

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) GUIDANCE FROM DSS

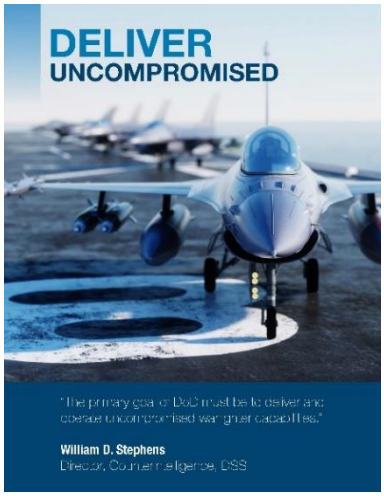
At this time, DSS is now provisioning users for any facilities that have not yet been provisioned; DSS will provision one hierarchy manager per facility, who will then subsequently provision other users for the facility themselves. Please read all of, and carefully follow, the DISS JVS Industry Provisioning Instructions found on both the recent DSS News and the VROC DISS News 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 DISS Tips and Tricks 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 Data Quality Initiatives (DQIs). Please ensure the records of all employees are recorded accurately in JPAS.

CDSE NEW COUNTERINTELLIGENCE AWARENESS TRAINING MATERIALS

Poster: Deliver Uncompromised – Download now.



Job Aid: Counterintelligence Awareness Integration Plan – Outlines how to incorporate counterintelligence (CI) and threat awareness into an existing program and to obtain leadership's approval of planned actions.

eLearning: CI117 Protecting Assets in the NISP – This course provides a detailed explanation of the importance of CI awareness to effective industry security programs.

Toolkit: Deliver Uncompromised: Critical Technology Protection – A more capable, resilient, and innovative defense requires capabilities developed and produced by the defense industrial base be delivered to the warfighter uncompromised. Utilize this toolkit for access to training, awareness materials, best practices, and other resources to help deliver uncompromised.

CDSE NEW INSIDER THREAT TRAINING MATERIALS

Poster: Insider Threat/Unauthorized Disclosure – Download and promote awareness in the workplace.

Game: Concentration – An "Oldie But Goodie," with an Innovative Insider Threat Twist.

Video: Insider Threat in Critical Infrastructure – Breakdowns in critical infrastructure can have devastating effects on national security and national public health and safety. Watch, Think, and Dig Deeper on how an insider's access can pose a unique threat to these sectors.

Job Aid: Tales from the Inside – This job aid provides a brief account of a real world event. It highlights a positive outcome of insider threat program risk mitigation. The name of the subject and organization have been anonymized to protect privacy.

DSS IN TRANSITION (DIT) WEBINAR SERIES

Please join CDSE in its fifth installment of the DiT webinar series, "Creating a Tailored Security Plan." This is the fifth of six planned webinars in a series designed to increase industry partner awareness and understanding of the DSS in Transition methodology and their role in it.

Creating a Tailored Security Plan
Thursday, May 9, 2019
Register here!

If you missed our first, second, third, or fourth DiT webinars, "Overview of the DSS in Transition Methodology," "Evolution of the FSO Role," "Asset Identification and Your Security Baseline," and "What's Different About My Security Review Now?," you can find them all here under *Previously Recorded Webinars*.

Also, don't forget to mark your calendars for the upcoming sixth DiT webinar, "Active Monitoring," scheduled for Thursday, June 6, 2019. Registration opens 30 days in advance of each webinar.

UPCOMING SPEAKER SERIES

CDSE invites you to participate in our upcoming Speaker Series:

Insider Threat and the DoD CAF
Thursday, May 23, 2019
12:00 – 1:00 p.m. ET

CDSE is hosting a discussion with Special Agent Cindy Beard on Insider Threat and the DoD CAF. This webinar will address the DoD CAF's conceptual approach to Insider Threat, key players and partners, processes, and the DoD CAF's future role in Insider Threat. Join us and be part of the conversation. Register here!

Counterintelligence Support to Personnel Security
Thursday, May 30, 2019
12:00 – 1:00 p.m. ET

Counterintelligence supports the Personnel Security (PERSEC) mission by identifying foreign intelligence entity (FIE) threats to personnel and enacting efforts to detect, deter, and neutralize the threat. Our guest, Special Agent Craig Beck from DSS, will discuss FIE targeting of U.S.

persons, how to identify indicators of the recruitment cycle, and how the PERSEC professional can recognize and report elicitation attempts and other suspicious activity. Register here.

REGISTER NOW FOR UPCOMING CDSE INDUSTRIAL SECURITY TRAINING

"Threats in the NISP" - Seats are available for this course being presented in conjunction with the NCMS Annual Seminar in St. Louis, MO, on June 10, 2019. Register here.

Take advantage of this opportunity to save training costs by completing both the CDSE training course and the NCMS Annual Seminar at the same time. This course is open to FSOs, Assistant FSOs (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).

To accommodate the 2019 NCMS Annual Seminar schedule, this iteration of the "Threats in the NISP" will be presented as a 1-day session. A special certificate will be uploaded to each participant's official student account.

Please note a separate registration is required in order to attend the NCMS Annual Seminar from June 11-13, 2019.

"Getting Started Seminar for New FSOs" - You have 90 days remaining to join us for this course in the Southern Region from July 24-25, 2019 in Orlando, FL. Register here.

This course is open to FSOs and Assistant FSOs (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). Due to the expansion of the counterintelligence block, this course is 2 full days. A prerequisite course titled "FSO Role in the NISP" is required for seminar registration and must have been completed after Nov. 23, 2015. A visit request must be submitted at least 30 days prior to the start of the class.

Come join us, we look forward to seeing you there!

SOCIAL MEDIA

Connect with CDSE on Twitter and Facebook.