DSS Monthly Newsletter
May 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 (RISO)

DSS continues the comprehensive security review (CSR) methodology in 2019 at a larger number of cleared facilities and to support select priority technologies. Historically referred to as "DSS in Transition" (DiT), the methodology is part of the larger effort to conduct risk-based industrial security oversight to support critical technology protection. As DSS moves from transition to transformation, the DiT lexicon will be phased out and replaced with RISO**.**

DSS field personnel have engaged with and conducted CSRs or enhanced security vulnerability assessments at cleared facilities supporting priority technologies. While only 60 CSRs were conducted in 2018, DSS estimates 150 of these reviews will be conducted in 2019. The reviews target cleared industry locations supporting specific technologies from the following technology categories within the Industrial Base Technology List: Armament and survivability; command, control, communication, and computers; energy systems, electronics, positioning, navigation, and time; materials raw and processed, space systems; and software.

INDUSTRY TOOLKIT & METHODOLOGY RESOURCES

The DiT webpage includes additional resources and tools to enable the industry development of tailored security programs. The toolkit is composed of six tabs. The first tab provides a process overview. The subsequent tabs focus on the five process steps and contain step specific resources to assist industry with the new methodology.

Prioritization: While DSS allocates and prioritizes resources based on national security information, industry partners can commence activities that will lead to a Tailored Security Plan (TSP). Industry partners should start the process by identifying critical assets and developing

awareness of threats related to those assets. The prioritization tasks require real-time knowledge of the participant's specific classified contracts and programs for process step completion.

Security Baseline: The Security Baseline requires industry to identify critical assets and analyze the threat analysis. The baseline supports the information required to execute the protection compilation and execution.

Security Review: Industry self-assessments, or security reviews of the security programs, ensures comprehensive compliance. In addition to the standard self-inspection, industry incorporates a supply-chain risk management (SCRM) analysis and review for other potential vulnerabilities.

Tailored Security Plan: After identifying vulnerabilities based on threats related to assets, industry partners should develop appropriate countermeasures. The security controls listed on the Security Baseline should be updated to reflect any new or enhanced countermeasures. This updated Security Baseline constitutes an initial TSP.

Active Monitoring: While the TSP is a living document, industry partners must actively continue to conduct the actions related to the new methodology and update TSPs as necessary.

To access the tools and resources available, please visit the DSS website at: https://www.dss.mil/ma/ctp/io/dit/.

Additionally, the Center for Development of Security Excellence 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 SCRM resources. These resources and many more can be found here: https://www.cdse.edu/toolkits/fsos/asset-id.html.

THE ROLE OF SECURITY SERVICE PROVIDERS AND SECURITY CONSULTANTS IN THE NISP

In 2018, DSS received several requests for guidance on issues currently affecting many security consultants, security service providers, remote facility security officers (FSOs), and the contractors they support. DSS will soon publish frequently asked questions to support these concerns.

DD Form 254 Validation

A contract is considered to be a "classified contract" when classified information access is required in performance of the contract and the requirement is documented on a form DD 254. DSS justifies the facility clearance (FCL) need by validating the DD 254. The supporting documentation may include some or all of the following: DD Form 254, security aspects letter, statement of work, requests for proposal, quote and/or information, Cooperative Research and Development Agreement, Government Contracting Activity (GCA) sponsored Independent Research & Development, etc.

Review of this documentation by DSS personnel assists in validating the requirement of an FCL and the need for a contractor to access classified information.

Maintaining a Facility Clearance

An FCL requires cleared industry to maintain one classified contract for justification. The sole purpose of accessing classified systems does not constitute a classified contract. If a facility has no classified contracts, DSS will reject the FCL sponsorship or initiate FCL termination. DSS personnel may request additional documentation to validate classified contracts and a FCL is required.

Sponsorship Validation

DSS is responsible for validating FCL sponsorships in addition to classified information access. Normally sponsorship is accomplished through DD 254 review, but sometimes the language within the form does not sufficiently explain the required classified work. In those instances, DSS may coordinate with the relevant GCA to better understand requirements, or review additional documentation. The Performance Work Statement often provides a clearer description of the classified work and can assist with validating the need for the FCL.

FCL Termination

In accordance with DD Form 441, DSS provides contractors with a 30 day written notice of the intent to terminate the FCL. This occurs when there is no need for access to classified information. A contractor must provide a justification for an FCL within the 30 day timeframe in order to maintain an FCL. DSS will validate any justification requests or the FCL termination will be initiated.

Facility Security Officer (FSO) effectiveness

While no policy requirement exists for an FSO to have a specific work schedule or work location, FSOs must effectively supervise and direct security measures consistent with the requirements of the National Industrial Security Program Operating Manual. Generally, DSS evaluates the effectiveness of the FSO during the Security Vulnerability Assessment (SVA). DSS personnel may also gather and record information about the FSO and their security program management effectiveness.

Security Vulnerability Assessment participation

Security consultants and other security service providers may participate in SVAs. The FSO is responsible for supervising and directing the security program and interfacing with DSS. The consultant and/or service provider role is not program oversight, but supplement and assist the FSO with the management of the security program. Consultants by their very nature work with multiple companies and may provide consulting services to more than one company at a time.

DEPARTMENT OF VETERANS AFFAIRS JOINS NISP

On May 8, 2019, DSS released Industrial Security Letter (ISL 2019-02), which amends the list of non-Department of Defense (DoD) agencies that have agreements for industrial security services with DoD. The list is now amended to include the Department of Veterans Affairs, which entered into an agreement with the DoD on May 8, 2019. The addition makes the Department of Veterans Affairs the 33rd non-DoD agency for which the department will provide industrial security services. The ISL can be accessed here: https://www.dss.mil/About-Us/News/News-Display/Article/1844370/dss-releases-isl-2019-02-to-add-department-of-veterans-affairs-to-nisp/

Previously issued ISLs can also be accessed from the National Industrial Security Program Library on the DSS website at: https://www.dss.mil/ma/ctp/io/fcb/nisp/

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) INFORMATION

In an effort to continue improving the customer service experience and developing efficiencies for NISS users, users will be limited to only have one change condition package in process at a time per facility. Users can still report multiple changes within the same package, but they will be limited to only one package in process at a time. This update was implemented to prevent users from creating multiple unnecessary change condition packages (in turn, creating duplications of the key management personnel list) which caused performance issues.

There has been an update to automated selections when using the DSS Knowledge Center when submitting user questions and issues for NISS. Effective May 7, 2019, NISS questions and issues can be reported by calling the DSS Knowledge Center at 888-282-7682 and selecting Option 2, then Option 2 a second time. The DSS Knowledge Center hours of operation are Monday through Friday from 8 a.m. to 6 p.m. EST.

NISP ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (EMASS) TRAINING GUIDANCE & REMINDERS

On May 6, 2019, the NISP eMASS became operational and mandatory for all cleared industry partners. This is a cybersecurity business management system used to maintain the Risk Management Framework (RMF) documentation needed to authorize information systems. New and existing re-authorizing systems must be entered into eMASS to support system authorization. eMASS can be accessed from this link: https://emass-nisp.csd.disa.mil/

The following is the step-by-step procedures to request a NISP eMASS account:

1. Complete the Defense Information Systems Agency (DISA) eMASS computer-based training (training takes two hours and a certificate of completion is granted. Work with your local information systems security professional (ISSP) and/or ISSP team lead for sponsorship to the training)
2. Complete DISA Cyber Awareness Challenge training
3. Complete DSS NISP eMASS (pre-populated) System Authorization Access Request (SAAR)

4. Submit all the completed artifacts (DD 2875 SAAR, CAC certificate, and eMASS training completion certificate) to DSS NAO eMASS mailbox: dss.quantico.dss.mbx.emass@mail.mil
5. Access the NISP eMASS link and register user profile

Accounts take three-to-five business days to be established. Job aids are available on the NISP RMF Resource Center link on the DSS website (https://www.dss.mil/ma/ctp/io/nao/rmf/).

On September 30, 2019, ODAA Business Management System (OBMS) will no longer be available to industry. Industry participants are strongly encouraged to ensure that the system artifacts and documents supporting current authorizations are locally available before the OBMS is discontinued.

NISP industry partners are strongly encouraged to follow the system security plan submission timeline recommendations listed in the DSS Assessment and Authorization Process Manual (DAAPM). Section 7 of the DAAPM states the following:

"DSS highly recommends submitting system security authorization packages at least 90 days before required need, whether reauthorization or new system. This timeframe will allow for complete package review to include the on-site assessment, interaction between the information system security manager and ISSP, and addressing any potential updates or changes to the authorization package."

Questions regarding eMASS should be referred to the NAO eMASS mailbox at: dss.quantico.dss.mbx.emass@mail.mil

VETTING RISK OPERATIONS CENTER (VROC)

Deferment FAQs
VROC provides frequently asked questions regarding the deferment process. Click the following link: https://www.dss.mil/Portals/69/documents/dvd/vroc/Deferment_FAQ.pdf

Implementation of Interim Backlog Mitigation Measures
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 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.

FSOs should continue to submit completed Standard Form (SF) 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 for assistance: dss.ncr.dss-dvd.mbx.askvroc@mail.mil

These procedures will remain in effect until further notice.

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 SF86, 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 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.)

ELECTRONIC FINGERPRINT TRANSMISSION TIMING REMINDER

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 the NBIB has processed the fingerprints by checking SII in JPAS which indicates a "Special Agreement Check (SAC)" closed.

Fingerprint results are valid for 120 days, which is the same amount of time for which Electronic Questionnaires for Investigations Processing (e-QIP) signature pages are valid. 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

On August 1, 2019, the Vetting Risk Operations Center (VROC) will no longer accept Research, Recertify, and Upgrade (RRU) requests in JPAS or Non-Disclosure Agreements (NDAs)/SF312s via fax, email, or mail. These actions previously requested via RRU should be submitted as CSRs in DISS. Similarly, NDAs should be submitted for approval via DISS. For specific instructions on how to complete CSR/NDA actions, please reference the DISS User Manual. The manual is accessible by: Clicking the Help link in the application. For additional assistance with how to complete the most common actions in DISS, please refer to DISS Tips and Tricks.

In order to prepare your security management office for this transition, it is imperative that you obtain a DISS account prior to August 1, 2019. To obtain an account, please read and follow the DISS JVS Provisioning Instructions.

DSS is now provisioning users for any facilities that have not created an account; DSS will create one hierarchy manager access account per facility, who will then subsequently create and manage other user accounts for the facility. Please read and follow the DISS Joint Verification System (JVS) Industry Provisioning Instructions found on the recent DSS webpage, News Section and the VROC DISS webpage. Failure to follow the procedures may result in the rejection of your request which will be returned. The last request submission goes to the end of the queue and may delay your access.

Once you have obtained access to DISS, please review the following DISS Tips & Tricks at:

http://www.dss.mil/documents/DISS_JVS_Industry_Provisioning_Instructions.docx) for helpful hints and answers to frequently asked questions

As JPAS transitions to DISS, JPAS will continue to perform a Data Quality Initiatives (DQIs). Please ensure the all employee’s records are accurate.

Knowledge Center Menu Options

The menu options for the DSS Knowledge Center (888) 282-7682 has changed. The customers will hear the following menu options:

Option 1 - PCL inquiries to include e-QIP
Office Hours: 8 a.m. to 5 p.m. Eastern Time

Option 2 - Account Lockouts and Passwords
Office Hours: 8 a.m. to 6 p.m. Eastern Time

Option 3 - FCL inquiries
Office Hours: 8 a.m. to 5 p.m. Eastern Time

Option 4 - OBMS

Option 5 - CDSE
Office Hours: 8 a.m. - 4 p.m. Eastern Time

Option 6 - Industrial Policy -
Please send an email for after-hours information:
dss.quantico.dss-hq.mbx.policyhq@mail.mil

DSS COUNTERINTELLIGENCE

DSS Counterintelligence identifies threats to U.S. technology and programs resident in cleared industry and articulates that threat to stakeholders. The information below is for awareness.

FOREIGN COUNTRY BACKGROUND INVESTIGATION SERVICE PROVIDERS

Cleared contractors often utilize private companies to conduct due diligence background investigations on potential employees. Those using this type of service should be mindful of the heightened risks posed if the service provider is foreign. In many foreign countries, citizens and private companies are required to support the intelligence and security services of their home country; failure to do so can result in fines and/or imprisonment. Foreign intelligence services have considerable interest in the personally identifiable information (PII) of cleared industry because it can be used to target individuals for solicitation, exploitation, elicitation, coercion, or monitoring. In some countries, foreign intelligence services may seek information on cleared industry, and conceal this effort by collecting information through a legitimate foreign background investigation service provider as part of its normal business operations. This presents a considerable conflict of interest between the foreign business' legal requirements to their own government, and privacy expectations of cleared U.S. contractor clients. In addition to being mindful of using foreign background investigation service providers, cleared contractors should not identify specific U.S. government customers or classified projects on any related work orders or service requests.

CLEARED JOB FAIRS

Job fairs for cleared personnel can be an excellent opportunity to grow careers to support highly sensitive U.S. government critical programs and technologies. Foreign intelligence may use recruiting venues as a means to identify and target cleared personnel. Cleared personnel are strongly encouraged to only attend recruiting events sponsored by the U.S. government or reputable organizations. Further, cleared personnel should avoid sharing personal information in person or online if the identity or creditability of the recipient is questionable. For additional

information about conferences, conventions and tradeshows, please see: https://www.dss.mil/Portals/69/documents/ci/Conferences_Conventions_Tradeshows.pdf

ADVERTISING FACILITY CLEARANCE

NISPOM 2-100c states: "a contractor shall not use its facility clearance for advertising or promotional purposes." To avoid being targeted by foreign intelligence, contractors should avoid identifying their facility clearance on job postings or company webpages.

SUSPICIOUS CONTACTS

The NISPOM defines suspicious contacts as:

- "Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee" or
- Contacts by cleared employees with known or suspected intelligence officers from any country
- Any contact which suggests a cleared employee may be the target of an attempted exploitation by the intelligence services of another country

FSOs can report suspicious contacts to their local DSS Industrial Security Representative (ISR) or Counterintelligence Special Agent (CISA) using the DSS submission form.

NEW COUNTERINTELLIGENCE AWARENESS TRAINING MATERIALS

DSS IN TRANSITION (DIT) WEBINAR SERIES

Please the sixth and final installment of the DiT Webinar Series: Active Monitoring.

Active Monitoring
Thursday, June 6, 2019
Register here!

If you missed any of the previous webinars they are located under Previously Recorded Webinars.

JULY SPEAKER SERIES

CDSE invites you to participate in our upcoming Speaker Series:

Human Resources and Insider Threat
Thursday, July 11, 2019
12 p.m. to 1 p.m. ET

CDSE is hosting a discussion with the Insider Threat Lead for the Human Capital Management Office (HCMO) of the Defense Security Service.

Register Now!

NEW CERTIFICATION RENEWAL FORM COMING SOON!

The Security Professional Education Development (SPēD) Certification Program is in the process of updating the Certification Renewal Form to provide easy access and user-friendly platform.

GETTING STARTED SEMINAR FOR NEW FSOS

Join us in the Southern Region from July 24-25, 2019 in Orlando, Fla. 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 service members exiting the various armed forces).

Due to the expansion of the counterintelligence content, this course is two full days. The prerequisite seminar registration is a course titled: FSO Role in the NISP. The prerequisite 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.

SOCIAL MEDIA

Connect with CDSE on Twitter and Facebook.