DSS Monthly Newsletter
May 2018

(Sent on behalf of your ISR.)

Dear FSO,

This is the monthly newsletter containing recent information, policy guidance, and 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 VOI NEWSLETTER

Missing a few back issues of the Voice of Industry (VOI) Newsletter? The Defense Security Service (DSS) Public Affairs Office maintains a library of the VOI Newsletter (and other important forms and guides) on its Industry Tools page.

DSS IN TRANSITION (DiT)

In 2017, DSS launched an enterprise-wide change initiative called, "DSS in Transition". The goal of DiT is to move the Agency from being focused strictly on schedule-driven NISPOM (National Industrial Security Program Operating Manual) compliance to an intelligence-led, asset-focused, and threat-driven approach to industrial security oversight.

The new DiT methodology is based on knowing the relevant assets at each facility, establishing tailored security plans, and applying appropriate countermeasures based on threat. DSS is implementing the new process in an incremental way that educates both DSS personnel and participating industry partners as the process is continuously evaluated and improved. DSS field personnel were provided with comprehensive training of the new DiT methodology at DSS Operational Training Events in April.

Also in April, the DSS Industrial Security Field Operations Program Management Office established the Implementation Program Review Board (IPRB). The IPRB is responsible for overseeing DiT project areas to ensure new processes are clearly documented, supported by technology, trained, and implemented while ensuring stakeholders are proactively informed and engaged. DSS is also in the process of conducting a training needs analysis that will help inform the long-term training developed for industry, Government partners, and DSS personnel.

As part of a phased implementation, four facilities were selected by DSS to participate in the first phase of implementation of DiT. These four industry partners were the first to be reviewed under the entire DiT process outside of the direct supervision of the Change Management Office. The assessments concluded in early April and DSS completed several after action reviews, the final of which was conducted on April 18. DSS is now in the process of incorporating lessons learned from the first phase into future phases and will continue to use expertise and insights gained to improve the process throughout the year.

In April, DSS Field Offices validated the list of cleared facilities associated with the Department's top priority technology and determined eight facilities to be reviewed during the second phase of implementation. These facilities have been contacted and pre-review activities are currently underway. DSS anticipates the reviews and post-review activities to be completed in the June/July timeframe. Upon completion, DSS will once again stop to evaluate the process, incorporate lessons learned, and make further changes as appropriate.

By the end of the year, DSS anticipates a majority of personnel will be trained on the new approach, facilities assessed will have developed a tailored security plan, and the process will be refined along the way. DSS will continue to assess and rate facilities not involved in DiT implementation in 2018 under the traditional security vulnerability assessment model. During these assessments, DSS will introduce facility security personnel to the concepts of asset identification and documenting business processes for the protection of assets. DSS will also introduce facility security officials to a new threat assessment tool known as the "12x13" matrix.

For more information on the DiT methodology, click here.

SECURITY OVERSIGHT AND REVIEW ACTIVITIES

In early 2018, DSS leadership briefed Government and Industry Stakeholder groups at a number of meetings, conferences, and seminars on the security review types that would be used by DSS field personnel during the year. Review types include a comprehensive security review, targeted security review, and enhanced security vulnerability assessment (SVA).

- The comprehensive security review will follow the new DiT methodology. It is an unrated review that results in the development of a tailored security program.
- The targeted security review follows the new DiT methodology but stops short of developing a tailored security program. Targeted security reviews are rated under our traditional rating model.
- The enhanced SVA introduces facility personnel to the concept of asset identification, the concept of mapping business processes associated with protecting assets, and the the new threat tool known as the 12x13 matrix. Enhanced SVAs follow the traditional SVA format and are rated.

While not all facilities will receive one of these three reviews, the review type that a facility will receive will depend on a number of factors and internal DSS prioritization.

DSS personnel will conduct meaningful engagements with those facilities not receiving one of the three review types. Meaningful 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.

REQUESTS FOR INFORMATION

From time to time, industry may receive correspondence from their local field office regarding their security program, classified contracts, or other NISP activities. These routine inquiries enable DSS personnel to validate a facility's continued participation in the NISP and helps to ensure DSS records are updated with pertinent, relevant, and current contract information.

These interactions can often provide DSS personnel with a sense of the current security posture and program at a contractor facility. As DSS is unable to conduct a security review at each contractor facility on an annual basis, personnel often leverage these engagements to maintain routine and ongoing interaction with industry partners. Industry is encouraged to cooperate with DSS security officials in support of a strengthened national security partnership.

NON-NISP INVESTIGATIONS

As referenced in NISPOM 2-200d, contractors are required to limit requests for personnel security clearances to the minimal number of employees necessary for operational efficiency, consistent with contractual obligations and other requirements of the NISPOM. Requests for personnel security clearances shall not be made to establish pools of cleared employees.

Government agencies should not request contractors initiate personnel security clearance requests for personnel not requiring access to classified information. As a reminder and per the DoD Manual 5200.02, Procedures for the DoD Personnel Security Program (April 3, 2017), DoD Component heads are required to submit and resource investigation requests for contractor personnel outside the NISP (i.e. investigations required for other than access to classified information).

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) UPDATE

NISS is currently unavailable and will be offline until it becomes the system of record this summer. Additional communications and guidance on the deployment will be provided soon.

For now, please ignore any account "lockout" messages that you may receive. Users may allow their accounts to expire as the system is unavailable. As a result of fixing several registration issues, all users will re-register upon full launch.

If you participated in NISS access and provided feedback during this past "soft launch" period, thank you! DSS received significant constructive feedback which we have addressed over the past months to include in the initial deployment.

Thank you again,
The NISS Team

NAO RELEASE OF DAAPM 1.3

The NISP Authorizing Office (NAO) is pleased to announce the release of the DSS Assessments and Authorization Process Manual (DAAPM) Version 1.3 in our continuing effort to provide users with the most up-to-date requirements of the Risk Management Framework (RMF) process. Version 1.3 supersedes all previous versions of the DAAPM and goes into effect on June 4, 2018.

This version updates two specific areas of interest.

First, it includes a recommended submission period for RMF packages of at least 90 days. This change is located at the beginning of Section 6, which has been renamed to "Assessment and Authorization Implementation Guidance". The rational for the change is to ensure that both industry and DSS allow sufficient time to work the packages before and after submission.

Next, it identifies who (Cleared Industry or DSS) has the responsibility for each step of the process. Section 6 contains a walk-through of each RMF step and identifies the responsible party for each task within each step. In summary, Industry is responsible for Step 1, Step 2, Step 3, the first part of Step 4, and the first part of Step 6. DSS is responsible for the second part of Step 4, Step 5, and the second part of Step 6. Additionally, the flowchart in Section 5 is updated to reflect the ownership of each step. Finally, the Concurrence Form has been eliminated. The intent of this change is to eliminate confusion.

You may access the DAAPM 1.3 from the DSS RMF Resource Center site here after June 4.

We welcome comments and suggestions as they help us improve our products and processes.

Thank you for your continued support of DSS.

APPROVED MFA OPTIONS AND IFS CAPABILITIES FOR CLASSIFIED INFORMATION SYSTEMS

The DoD Chief Information Officer (CIO) memo dated April 12, 2018 addresses “Approved Multi-Factor Authentication and Identity Federation Service Capabilities.” System owners (SOs) are reminded that per DoD CIO policy, PKI authentication is required for all DoD systems. Industry information systems (ISs) connected to government networks, such as SIPRNet, must meet this requirement. In situations or environments where the ISs cannot support PKI or users cannot obtain DoD-issued or approved PKI credentials, the Deputy CIO for Cybersecurity (DCIO-CS) has approved alternatives. The alternatives apply to classified ISs at the SECRET level using Multi Factor Authentication (MFA) credentials and are as follows:

1. RSA SecurID token
2. YubiKey Universal Two Factor token.

In situations or environments where the IS cannot fully support the alternative credentials using direct authentication with DoD-approved PKI or MFA, the DCIO-CS has approved the Identity Federation Services (IFS) for classified systems at the SECRET level as follows:

1. Enterprise Privileged User Authentication Service
2. Secure Administration Authentication Gateway
3. Centrify Server Suite and Centrify Privileged Service.

The actual MFA and IFS approval memos and respective implementation guidance can be found here. See the “DoD CIO Documentation” heading to download the file(s).

EVALUATING INSIDER THREAT PROGRAM EFFECTIVENESS

Since the release of NISPOM Change 2 and Industrial Security Letter 2016-02 Revised (06/29/17), industry has done a great job implementing insider threat program requirements.

As of April, 99% of facilities have appointed an Insider Threat Program Senior Official and 95% of facilities have certified that an insider threat program plan is in place and current.

Additionally, industry course completions continue to rise. As of April, 14,246 industry personnel have completed INT122.16, "Establishing an Insider Threat Program for Your Organization," and 242,831 industry personnel have completed INT101.16, "Insider Threat Awareness."

As industry establishes and maintains their programs, DSS continues to verify that minimum insider threat program requirements are in place including:

- An Insider Threat Program Senior Official is appointed
- An insider threat program plan is in place which meets minimum requirements
- Insider threat awareness training has been provided to cleared employees
- Necessary controls are in place on classified information systems.

However, in the future, DSS will evaluate the effectiveness of industry's insider threat programs.

In February, DSS held a tabletop exercise with representatives from several industry partners and expects to sponsor a follow-on engagement to discuss the proposed process.

Under our current plan, insider threat program requirements will be broken into five principles:

- Insider threat program management
- Insider threat awareness training
- Information systems protections
- Collection and integration of insider threat indicators
- Analysis of those indicators and response actions.

DSS will pinpoint items to consider when evaluating a facility's implementation of each principle. DSS will use these items to determine whether an insider threat program is effective.

As the process is finalized, industry will be kept informed. While the specific date for DSS to begin evaluating the effectiveness of insider threat programs has not been identified, the evaluation is not set to take effect until sometime in calendar year 2019.

Although DSS has not begun to evaluate the effectiveness of industry's insider threat programs, we strongly encourage you to set aside some time to test your own insider threat program for effectiveness. The Center for Development of Security Excellence (CDSE) has developed several tools to help you build your insider threat program, including the insider threat toolkit. If you have any questions about how to improve your insider threat program, please contact your local field office.

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 Security/Suitability Investigations Index (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.

PREPARING FOR DISS

The Defense Information System for Security (DISS) is deploying to Industry on June 25, 2018. In preparation for accessing DISS, additional guidance on account provisioning has been added to the DSS DISS website here.

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 (IRR), Defense Central Index of Investigation (DCII), Secure Web Fingerprint Transmission (SWFT), or Joint Personnel Adjudication System (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 here.

CREDIT FREEZE DURING INVESTIGATIONS

The credit report is to remain unfrozen until the investigation is closed because there are situations where a second report is required. If the subject opts to refreeze their credit report before the investigation closes, we can provide the following guidelines. Normally, the credit is checked at the time the case schedules in our system. If we have to ask the agency to unfreeze the credit, it could take up to 30 days to rerun the credit report. This timeframe is our best estimate and there could be circumstances that don't fit this time scenario.

INVESTIGATION STATUS UPDATES

You can obtain an investigation status update by performing a search of the SII in JPAS. This link is available at the bottom of the Person Summary Screen in JPAS (Perform SII Search). The following statuses are available to let you know what is happening with the investigation:

- **Received** - The Investigation Service Provider has acknowledged receipt of the investigation request and will be reviewing for acceptability.

- **Unacceptable** - The Investigation Service Provider determined the investigation request to be deficient. PSMO-I will transmit a JPAS message with the reason the request was rejected. If your employee still requires a clearance, a new investigation request will need to be initiated and submitted with the corrected information.

- **Scheduled** - The Investigation Service Provider has determined the investigation request to be acceptable and the investigation is current ongoing/open.

- **Closed** - The Investigative Service Provider has completed the investigation and the investigation has been sent for adjudication.

Please do not call the DSS Knowledge Center to request the status of an investigation showing in one of the statuses provided above. The Knowledge Center will no longer provide lead count and does not have the ability to estimate nor impact investigation timelines.

CORRECTION TO DMDC DQI 945 NOTICE

On May 1, 2018, the Defense Manpower Data Center (DMDC) posted Data Quality Initiative (DQI) 945. The DQI included item 6) Favorable Eligibility Date is > 16 years old, and item 7) Interim Eligibility Date is > 3 years old, which do not align with the Department of Defense guidance that clearances do not expire. DMDC is not automatically taking away anyone's eligibility for aging interims or overdue PRs. DMDC has confirmed there were no downgrade actions initiated based on the DQI notice. However, actions are still required on items 1-5 (see below).

THIS PERSONS DATA MUST BE CORRECTED WITHIN 30 DAYS FOR ITEMS 1-5. The subject identified in this notification currently has one or more of the following issues:

1. Eligibility Date prior to the Birth Date

2. Eligibility Date equal to the Birth Date

3. Eligibility Date < 16 years after Birth Date

4. Future Birth Date

5. Future Death Date.

SECURITY EDUCATION AND TRAINING

NEW CI CASE STUDY AVAILABLE

The Center for Development of Security Excellence (CDSE) recently released a new Counterintelligence Case Study:

- Counterintelligence Case Study – Attempted Acquisition of Technology – Illegal Export

This case study can easily be included in an organization's security education, training, and awareness programs. The case study is suitable for printing or easy placement in a company or command newsletter, email, or training bulletin. Access the new case study today!

CI VIGILANCE CAMPAIGN GUIDANCE

Not sure how to manage a counterintelligence awareness campaign? CDSE offers a handy job aid to assist your planning. Access the Counterintelligence Job Aid here.

CHECK OUT OUR INSIDER THREAT TOOLKIT

CDSE's Insider Threat Toolkit keeps growing. The Insider Threat Vigilance tab to the toolkit has several new helpful tools to assist with promoting insider threat awareness. Tools include:

- Vigilance Campaign Materials
  - Guidance Document
  - Job Aid for DoD and Industry
  - Insider Threat Posters
  - Access Request for Additional Resources
- Case Studies
- Videos and Interactive Shorts
- eLearning Games.

Access the Insider Threat Toolkit here.

UPCOMING WEBINAR

Join CDSE for our next webinar:

- Business Structures
  Thursday, July 19, 2018
  11:30 a.m. ET & 2:30 p.m. ET

In this live webinar, we will analyze business structures, determine ownership or control and clearance or exclusion, and identify vulnerabilities associated with improper analysis of business structures.

Register and be part of the conversation! Sign up today at CDSE Webinars.

UPCOMING SPEAKER SERIES

CDSE invites you to participate in our upcoming Speaker Series:

- **Supervisor Reporting and Security with PERSEREC**
  Thursday, June 14, 2018
  12:00 p.m. ET

  In this webinar, CDSE will host a discussion with Dr. Leissa Nelson of the Defense Personnel and Security Research Center. We will review known reporting obstacles and identify methods for increasing responsibility and motivation of supervisors for reporting behaviors related to security concerns. Join us and be part of the conversation.

- **Defense Insider Threat Management and Analysis Center Update 2018**
  Thursday, July 19, 2018
  12:00 p.m. ET

  In this webinar, CDSE will host a status discussion with leadership of the Defense Insider Threat Management and Analysis Center (DITMAC). DITMAC was established in the wake of the Washington Navy Yard shooting and other recent insider threat incidents to serve as a catalyst for information sharing and collaborative insider defense. DITMAC offers an enterprise capability that leverages relevant data; a multidisciplinary team of analysts and experts to assist in research, analysis, and risk assessment; and enabling tools and technologies to build an enterprise view of insider threat issues across DoD in support of DoD Components.

Join the discussion! Sign up today at CDSE Webinars.

ARCHIVED WEBINARS AND SPEAKER SERIES NOW AVAILABLE

Did you miss May’s Speaker Series, “Kicking off an Insider Threat Vigilance Campaign” or the “Transmitting or Transporting of Classified Material by Industry” webinar? If the answer is “yes,” you can access both and other past webinars in our archives.

Access all archived webinars (no certificate provided) at CDSE Previously Recorded Webinars or register for the on-demand webinars (certificate provided) at CDSE On Demand Webinars.

GETTING STARTED SEMINAR FOR NEW FSOs

Getting Started Seminar for New FSOs (GSS) gives new FSOs the opportunity to discuss, practice, and apply fundamental NISP requirements in a collaborative classroom environment and develop a network of professional associates. This course is appropriate for any FSO, new or old, who is looking to enhance their security program.

Our final iteration for the FY18 schedule is currently open for registration. Check out the course below to see if it meets your training needs.

August 14-15, 2018, Pasadena, CA, go here.

Seats are limited, so make sure you have successfully completed the current version of the prerequisite course, “Facility Security Officer (FSO) Role in the NISP” (IS023.16) and exam (IS023.06). We look forward to seeing you soon!

Are you interested in hosting a Getting Started Seminar at your location in FY19? If so, please send an email to our Industrial Security mailbox (dss.ncr.dss-cdse.mbx.industrial-security-training@mail.mil) and let us know what region you would like us to consider. We are beginning our solicitation process and welcome your requests. Below is a tentative schedule of our upcoming iterations.

November 6-7, 2018, Capital Region

May 14-15, 2019, Western Region

July 23-24, Southern Region

August 13-14, Northern Region

SOCIAL MEDIA

Connect with CDSE on Twitter and on Facebook.

Thanks,
ISR
Defense Security Service