DSS Monthly Newsletter
August 2017

(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 VOI NEWSLETTER

Missing a few back issues of the 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)

DSS is changing. Where the Agency once concentrated on schedule-driven NISPOM (National Industrial Security Program Operating Manual) compliance, DSS is now moving to an intelligence-led, asset-focused, and threat-driven approach to industrial security oversight.

To achieve this, the Agency is engaging the entire DSS enterprise through a multi-year initiative called, "DSS in Transition." As part of this initiative, DSS has formed a Change Management Office, launched a comprehensive communications strategy, and is developing a new methodology for implementing this change with industry.

To develop the new methodology, DSS is drawing upon the background, experience, and expertise of security professionals from across the Agency to transform each component of this new approach into an efficient, effective, and repeatable process that can be used for all cleared facilities in the National Industrial Security Program (NISP).

Over the past several months, draft Concepts of Operation (CONOPs) for each component in the new methodology have been developed. These component CONOPs have recently been updated, refined, and integrated into a single, unified, and aligned process. Over the remainder of this year and into early 2018, DSS plans to run a series of pilot exercises in the field with cleared industry to validate assumptions, capture lessons learned, and further refine this CONOPs.

For more information on the new methodology and the DSS in Transition initiative, click here.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) DEPLOYMENT UPDATE

The NISS soft launch is on hold pending system updates requested through Industry tester feedback. NISS will replace the Industrial Security Facilities Database (ISFD) and the Electronic Facility Clearance System (e-FCL). NISS will be the system of record for facility clearance information and submitting Change Conditions packages, among additional features. For information regarding this critical information system transition, please visit the NISS Informational Webpage.

REVISED SF 86 QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS

The 2016 SF 86, Questionnaire for National Security Positions, will replace previous versions of the form in e-QIP on Aug. 27, 2017.

Several changes have been made throughout the form to clarify what information is reportable. For example, Section 17, which covers marital/relationship status, has been expanded to more accurately collect information regarding legally recognized relationships, and Section 9, which covers citizenship, now includes the option of stating that the Subject is a derived U.S. citizen. Other changes include:

- **Section 12** - Where You Went to School - added a link to assist in determining school address.
- **Section 21** - Psychological and Emotional Health – revised as a result of a comprehensive review to clarify support for mental health treatment and encourage proactive management of mental health conditions, including wellness and recovery.
- **Section 23** - Illegal Use of Drugs and Drug Activity - clarifies that drug use or activity illegal under Federal laws must be reported, even if that activity is legal under state law.
- **Section 26** - Financial Record - includes collection of information involving Chapter 12 bankruptcy petitions..
- **Certification** – includes an acknowledgement that no classified information has been provided on the form.

More detailed information about the implementation of the revised SF 86 can be found in Office of Personnel Management Notice No. 17-07, issued on Aug. 18, 2017.

PRIORITIZATION OF INVESTIGATION REQUESTS

The Personnel Security Management Office for Industry (PSMO-I) is prioritizing the submission of initial T5 (Top Secret) and T3 (Secret) investigative requests to the National Background Investigations Bureau (NBIB). PSMO-I is continuing to monitor industry periodic reinvestigations to ensure none expire from the system. Industry should continue to submit T3R investigation requests to PSMO-I, in addition to caveat program T5Rs per the Apr 7, 2017 guidance.

REMINDER ON TIMING FOR ELECTRONIC FINGERPRINT TRANSMISSION

Reminder! 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 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. A high level process flow outlining this and other Personal Security Clearance (PCL) activities associated with obtaining a security clearance for Industry is provided here for your ease of reference, and Step #2 outlines the submission activities.

KNOWLEDGE CENTER PCL INQUIRIES CLOSED ON SEPTEMBER 29, 2017

PCL Inquiries (Option #2) including e-QIP Authentication Resets of the DSS Knowledge Center will be closed on Friday, Sept. 29, 2017. This closure is to conduct internal training to deliver the highest quality customer service to Industry and Government callers. Normal operations for PCL and e-QIP inquiries will resume on Monday, Oct. 2, 2017. Also, as a reminder, the PCL portion of the DSS Knowledge Center is typically closed on the last Friday of each month.

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

The NAO hosted a small group of volunteer industry Information Systems Security Managers (ISSMs) at RKB from 22 to 25 August 2017 to participate in a thorough review of changes to the DSS Assessment & Authorization Process Manual (DAAPM). The DAAPM is currently being updated and is tentatively scheduled for release in the Fall 2017. The participating companies included L3 Technologies, Leidos, Lockheed Martin, and Leonardo DRS.

PKI TOKENS NOW REQUIRED FOR SIPRNet CONNECTIONS

In accordance with the DoD Chief Information Officer Memo dated July 14, 2017, all DoD sponsors of contractor-site SIPRNet connections must obtain SIPRNet PKI tokens for their cleared contractors no later than Oct. 1, 2017.

Additionally, no later than Oct. 1, 2017: all DoD sponsors of contractor-site SIPRNet connections using Microsoft Active Directory (AD) must configure these connections to require user network crypto-logon with DoD SIPRNet PKI tokens; and all users of contractor-site SIPRNet connections must use PKI tokens to authenticate to websites and applications.

Finally, beginning Oct. 1, 2017, all Command Cyber Readiness Inspections will check for compliance with these requirements.

For additional information on SIPRNet PKI, please see the Defense Information Systems Agency SIPRNet PKE webpage here.

Please contact your assigned ISSP with any questions or concerns regarding the implementation of this requirement.

SECURITY EDUCATION AND TRAINING

CDSE OPENS FY18 REGISTRATION

The FY18 Center for Development of Security Excellence (CDSE) Training Course Schedule is now available and may be found at FY18 CDSE Training Course Schedule. Review our schedule and get a jump on planning next year's security training. Sign up and reserve your seat today!

UPCOMING INDUSTRIAL SECURITY WEBINAR

Join CDSE on Thursday, Sept. 14, 2017 at 11:30 a.m. or 2:30 p.m. ET for the "Conducting Initial and Refresher Briefings" webinar. This webinar will assist with understanding the initial and refresher briefings required by the NISPOM. The webinar will feature exercises to ensure that participants know exactly what to incorporate in briefings and how to present them to their personnel. Sign up today at CDSE Webinars.

PERSEREC SUPPORT TO INSIDER THREAT PROGRAMS

The Defense Personnel Security Research Center (PERSEREC) is a Department of Defense entity dedicated to improving the effectiveness, efficiency, and fairness of DoD personnel suitability, security, and reliability systems. Join us for a live discussion on their recent active shooter/ kinetic violence studies and research for Insider Threat on Thursday, Oct. 5, 2017, from 1:00 to 2:00 p.m. ET. Sign up today at CDSE Webinars.

NEW SECURITY POSTERS

Trick out your hallways with free printables from CDSE! Download small or large versions of our posters. Here are a few of our newest posters: Every Leak Makes Us Weak, Lady Liberty, and Unauthorized Disclosure Poster, Think Before You Click.

Access all of our security awareness posters at Security Posters.

NEW CI CASE STUDY AVAILABLE

CDSE recently released a new "Counterintelligence Case Study – Dual Use Technology" job aid, which 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 an may be found at Counterintelligence Case Studies.

NEW SAP SECURITY SHORT RELEASED

CDSE has launched a new short, "Special Access Program (SAP) Security Incident Practical Exercise – Industrial Day." This short is designed to give an individual the necessary information to properly safeguard information, gather facts required for an inquiry, and create a Security Incident Report in the SAP environment. It includes feedback on recommended answers and a certificate of attendance at the completion of the short. The audience for the short is DoD civilian, military, and contractors with multidiscipline responsibilities for management, oversight, and support to DoD SAPs. Access the short at SAP Security Shorts.

FSOs CAN HOST A GETTING STARTED SEMINAR FOR NEW FSOs COURSE

Have you ever thought about hosting a CDSE course at your location, but didn't know how to go about doing so? Have you ever wanted to meet other Facility Security Officers (FSOs) and Security professionals that share your concerns? If so, this is your lucky day! The CDSE is formulating its Getting Started Seminar (GSS) for New FSOs course schedule. The GSS is a 2-day course 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). This is an opportunity for FSOs to host a course and have Security Instructors there to answer questions on topics such as National Industrial Security Program (NISP) reporting, the DD 254, and Insider Threat. Courses have been varied geographically to give all regions an opportunity to receive training and in the past have been held in Menlo Park, CA; Largo, FL; Burlington, MA; Savannah, GA; and Chantilly, VA. This year, the course will be offered for Capital/Southern Regions on 17 and 18 April 2018, and for Western/Northern Regions on 14 and 15 August 2018. More information may be found at Getting Started Seminar for New FSOs.

If interested, please reach out to your DSS ISR or send an email to our CDSE Industrial Security Mailbox. Be sure to include your location and the potential dates that interest you.

SOCIAL MEDIA

Connect with CDSE on Twitter (@TheCDSE) and on Facebook.

Thanks,
ISR
Defense Security Service