DSS Monthly Newsletter
September 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." DiT represents a monumental change for DSS internally, but for many in industry it's not entirely new. DSS is still going to conduct its core functions like performing Security Reviews, providing advice and assistance, and responding to security events. However, the Agency is changing the focus of its core functions from strictly evaluating facility compliance to protection of assets.

As part of this change in focus, DSS has identified several initial partnership opportunities that the Agency will soon begin exploring with a core group of volunteers from industry. These partnership opportunities include: identifying assets; developing tailored security programs; and designing a future measurement system that accurately depicts a facility's true security posture.

For more information on the new methodology and the DiT initiative, click here.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) DEPLOYMENT UPDATE

The NISS Soft Launch is underway beginning on Sept. 28 for Government users and Oct. 5 for Industry. NISS will replace the Industrial Security Facilities Database (ISFD) and the Electronic Facility Clearance System (e-FCL) in October. NISS will be the System of Record for facility clearance information and submitting Change Condition packages, among additional functions. For updates regarding this critical information system transition, please visit the NISS Site.

ISFD AND E-FCL SYSTEM SHUTDOWN APPROACHING

Attention ISFD and e-FCL Users: ISFD and e-FCL will be permanently shut down on Oct. 14 as part of the transition to NISS. These system will be replaced by NISS on Oct. 30. For more information, please visit the NISS Site.

SECURITY OFFICE IDENTIFIER (SOI) CODE UPDATES FOR INDUSTRY

With the recent release of JPAS v5.7.5.0, Facility Security Officers (FSOs) will need to select the SOIs from the dropdown menu when submitting new investigations. FSOs must now manually select "DD03" as the SOI Code from the dropdown menu, whereas, this code used to be automatically applied. Industry should not be using any other SOI Code when submitting investigation requests. Investigations will be discontinued if any other code for DoD contractors is used.

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) DEPLOYMENT

Comprised of two components, the Case Adjudication Tracking System (CATS) and the Joint Verification System (JVS), DISS will serve as the System of Record for comprehensive personnel security, suitability, and credential management for all DoD military, civilian, and contractor personnel.

DISS is undergoing a phased deployment:

- Phase 1 is the Migration to Single Adjudicative System, which is scheduled to launch on Nov. 13, 2017 in support of MILDEPS.
- Phase 2 is DISS Enterprise Subject Management, which is scheduled to launch in May 2018 in support of the Industry population.
- Phase 3 is the Establishment of a Single System of Record (JPAS will be taken offline during this phase).

Visit the DISS website for authoritative information for the DISS User Community to include: Account Management Policy, Account Request Procedures, Release Notes, Frequently Asked Questions, and DISS news/announcements. Remember to visit and bookmark this site to stay up-to-date on the latest DISS developments.

KNOWLEDGE CENTER PCL INQUIRIES CLOSED OCT. 27, 2017

Personnel Security (PCL) inquiries (Option #2) to include e-QIP Authentication Resets of the DSS Knowledge Center will be closed on Friday, Oct. 27. 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. 30. Also as a reminder, the PCL portion of the DSS Knowledge Center typically closes on the last Friday of each month.

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

ENTERPRISE MISSION ASSURANCE SUPPORT SERVICE (EMASS) FOR CLEARED INDUSTRY

The NAO has a phased transition to Risk Management Framework (RMF) that began Oct. 1, 2016, with full implementation scheduled for Jan. 1, 2018. To coincide with full RMF implementation, DSS plans to use the eMASS application starting in 2018 in place of the ODAA Business Management System (OBMS) as it is more suited to authorization actions.

The eMASS is a DoD owned web-based resource that automates the RMF process, includes reports required for the RMF process, and can tailor new reports to user needs. A key feature of eMASS is enabling users to share access to specific data in near real-time, and in a secure fashion.

The NISP instance of eMass will integrate several capabilities, such as:

- Reporting on a system's cybersecurity compliance
- Enabling real-time metrics on authorization activities
- Simplifying the RMF workflow automation
- Standardizing the exchange of information
- Monitoring systems security during the entire life cycle.

It is anticipated that by the Spring of 2018, System Security Plans will no longer be accepted via OBMS. This allows time to clear out the queues prior to transitioning.

The OBMS would still be used to access the SCAP, GPO, STIG Viewer, and other tools that support RMF until such items are transitioned to eMASS.

All dates at this time are tentative and every effort will be made to keep industry apprised of transition timelines and actions.

Please refer any questions or concerns to your assigned DSS ISSP.

WINDOWS 10 IMPLEMENTATION

The DoD CIO has directed all DoD components and agencies to migrate to Windows 10 NLT the end of 2017.

Facilities with systems connected to government networks should work directly with their sponsors to determine their requirement for compliance, especially for SIPRNet circuits.

REMINDER: PKI TOKENS NOW REQUIRED FOR SIPRNet CONNECTIONS

In accordance with the DoD Chief Information Officer Memo dated July 14, 2017, the following will become effective on Oct. 1, 2017:

a) All DoD sponsors of contractor-site SIPRNet connections must obtain SIPRNet PKI tokens for their cleared contractors. User names and passwords will no longer be used.

b) 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.

c) All users of contractor-site SIPRNet connections must use PKI tokens to authenticate to websites and applications.

d) 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 PKI webpage here.

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

SECURITY EDUCATION AND TRAINING

NATIONAL CYBER SECURITY AWARENESS MONTH 2017

National Cyber Security Awareness Month (NCSAM) 2017 is just around the corner! NCSAM is an annual campaign to raise awareness about the importance of cybersecurity.

In support of NCSAM, CDSE is proud to announce the upcoming release of three new Cybersecurity products:

- Short: Cybersecurity Attacks: The Insider Threat
- Short: Cybersecurity: Incident Response
- Game: Tomorrow's Internet.

Stay tuned for updates by following us on Twitter and on Facebook, and in the CDSE Flash news section.

NEW INSIDER THREAT CYBER CASE STUDY AVAILABLE

CDSE recently released a new "Insider Threat Case Study - Cyber." This job aid 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 it here.

UPCOMING COUNTERINTELLIGENCE WEBINAR

Join CDSE on Thursday, Oct. 26 at 12:00 p.m. ET for the "DSS 2017 Targeting U.S. Technologies – A Trend Analysis" webinar. During this webinar, DSS and CDSE will discuss the latest trends in foreign targeting of U.S. defense technologies that occurred in 2016. The webinar will focus on the foreign efforts to compromise and/or exploit cleared personnel in order to obtain unauthorized access to sensitive and classified information. This unclassified format will provide analysis of methods of operation and targeted technology. Sign up today at CDSE Webinars.

PERSEREC SUPPORT TO INSIDER THREAT PROGRAMS

The 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 from 1:00 p.m. to 2:00 p.m. ET. Sign up today at CDSE Webinars.

ARCHIVED INDUSTRIAL SECURITY WEBINAR

Did you miss our Industrial Security webinar "Conducting Initial and Refresher Briefings?" You can now view the webinar in our archive. This webinar will assist with understanding the initial and refresher briefings required by the NISPOM. It features exercises to ensure that participants know exactly what to incorporate into briefings and how to present them to their personnel. Access it today here.

CDSE RECOGNIZED AS TOP LEARNING ORGANIZATION

CDSE recently attended the 2017 Learning! 100 Awards Dinner at the Enterprise Learning! Conference. The event recognized the top 60 private and top 40 public organizations for their best-in-class learning and development programs. Private sector organizations included Amazon Web Services, IBM, and Facebook. CDSE was ranked #15 out of 40 public sector organizations for launching an Enterprise-Wide Distance Learning Strategy.

SOCIAL MEDIA

Connect with CDSE on Twitter and on Facebook.

Thanks,
ISR
Defense Security Service