DSS Monthly Newsletter
October 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 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)

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 help achieve this, the Agency launched the kick-off meeting for the first of two planned Practical Exercises with the Huntsville, AL Field Office in September 2017. This first Practical Exercise will operationally test the integrated Concept of Operations for the DiT methodology. At this meeting, Field Office personnel received an overview of the DiT methodology and were provided detailed information on the timelines, milestones, and objectives for the Practical Exercise.

In addition, a site visit was made to the cleared contractor facility that will be participating in the Practical Exercise. During this visit, key management and security personnel were briefed on the company’s role in the Practical Exercise, with the ultimate objective for the company to develop a Tailored Security Program. This Practical Exercise is planned to run to mid-February 2018.

For more information on the DiT methodology, click here.

NATIONAL INDUSTRIAL SECURITY SYSTEM DEPLOYMENT UPDATE

The National Industrial Security System (NISS) is currently in a "soft launch" test state and DSS has been receiving user feedback. Formal NISS deployment and transition off of the Industrial Security Facilities Database (ISFD) and Electronic Facility Clearance System (e-FCL) is on hold pending remedy of NISS application issues. A system update will be deployed on Oct. 30, 2018 for additional testing. For more information about this transition, visit the NISS Site or contact DSS.NISS@mail.mil.

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

This is a notice to Cleared Industry for the immediate removal of Kaspersky Labs software and/or hardware from all DSS Authorized Information Systems.

On Sept. 28, 2017, DSS issued a Memorandum signed by NISP Authorizing Official Karl Hellmann directing that, effective immediately, all NISP contractor facilities possessing classified information systems under DSS cognizance and authorization are directed to remove all Kaspersky Labs software and/or hardware from the Authorized Information System.

Further, companies will identify any use or presence of Kaspersky products on their classified information systems in the next 30 days; within the next 60 days, develop detailed plans to remove and discontinue present use and avoid future use of Kaspersky products; and within 90 days from the date of the Memorandum, begin implementing the plans to discontinue use and remove the Kaspersky products from the Information System.

This Memorandum is being implemented due to recent directives and orders issued by various federal government agencies and can be found on the DSS Website.

Questions or concerns should be directed to your Information System Security Professional (ISSP).

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 the National Background Investigations Bureau (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.

SECURITY EDUCATION AND TRAINING

CDSE LAUNCHES THE MARS JOB AID

The Center for Development of Security Excellence (CDSE) has released the “Mergers, Acquisitions, Reorganizations, Spin-off/Splits (MARS)” job aid. This job aid is designed to help

Facility Security Officers (FSOs) and Senior Management Officials (SMOs) to recognize reporting thresholds and procedures, understand the potential impacts of mergers, and appreciate the benefits of advanced reporting. The target audience includes FSOs, SMOs, other defense contractor security personnel, and other personnel working in the NISP.

Access the job aid on our site at any of the links below:

- CDSE Catalog Industrial Security
- CDSE Newest Job Aids
- CDSE Industrial Security Job Aids
- CDSE FSO Reporting Toolkit.

UNAUTHORIZED DISCLOSURE TRAINING VIDEO

The Unauthorized Disclosure Training (YouTube version) was launched on Sept. 18, 2017. What is the difference between unauthorized disclosures, leaks, and whistle blowing? What are the impacts of unauthorized disclosure, and what are the potential penalties for those who divulge our Nation's secrets? Sit back and watch the video. Check it out here.

NEW CYBERSECURITY SHORTS AND eLEARNING GAME

In support of National Cyber Security Awareness Month, which encourages building a strong culture of cybersecurity, CDSE released two new shorts and an eLearning game. Access these products at CDSE Catalog Cybersecurity.

Cybersecurity Attacks - The Insider Threat – This short addresses the types of attacks facilitated by the witting and unwitting insider and methods to mitigate the threat.

Cybersecurity: Incident Response – This short discusses the importance of and approaches to building an effective incident response capability.

Tomorrow's Internet eLearning Game – This trivia game is designed to test the user's general cybersecurity knowledge through a series of questions. Users are awarded badges and provided with relevant feedback.

UPDATED INDUSTRIAL SECURITY SHORT

CDSE recently launched an updated version of the "You're a New FSO: What Now?" short. This short was updated to add new content and a new look. This short introduces the CDSE FSO curriculum, and provides newly appointed FSOs with a high-level overview of their responsibilities and guides them to essential resources. It's only 10 minutes long but it's filled with information for new FSOs or those interested in the role of an FSO.

For more information and to check out this short here.

UPDATED CI AWARENESS COURSE

Check out the new Counterintelligence (CI) Awareness and Reporting course. In this course you'll learn to identify the threats and methods of Foreign Intelligence Entities (FIE), recognize FIE use of cyber attacks, describe the Insider Threat, identify intelligence and security anomalies, and understand CI awareness and reporting requirements. Visit the newly updated course here.

UPCOMING INSIDER THREAT SPEAKER SERIES

Join us on Thursday, Nov. 30, 2017 at 12:00 p.m. ET for a live discussion with the DoD Insider Threat Enterprise Program Management Office (EPMO) Chief, Ms. Kristen Cahill. The EPMO is a component proponent that supports the OUSD(I) by providing senior officials with a cross-cutting enterprise view to help inform and shape appropriate Insider Threat decisions and policies. EPMO focuses on evaluating program effectiveness, strengthening partnerships, advancing data sharing, and delivering transparency and responsiveness across the enterprise. Sign up today at CDSE Webinars.

ARCHIVED PERSEREC SUPPORT TO INSIDER THREAT PROGRAMS

Did you miss our live discussion with the DoD Personnel Security Research Center (PERSEREC) on their recent active shooter/ kinetic violence studies and research for Insider Threat? No problem. Access the webinar in our On Demand webinars and earn a certificate at CDSE On Demand Webinars or view in the webinar archive (non-certificate option) at CDSE Previously Recorded Webinars.

SOCIAL MEDIA

Connect with CDSE on Twitter and on Facebook.

Thanks,
ISR
Defense Security Service