DSS Monthly Newsletter
January 2018

(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)

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.

As we move into 2018, DSS is starting to train the field on DiT, which is based on knowing the assets at each facility, establishing tailored security plans, and applying appropriate countermeasures based on threat. Four facilities have been selected by DSS to participate in the first phase of implementation of DiT and will be the first of our industry partners to complete the entire DiT process outside of the direct supervision of the Change Management Office.

The first of a series of cross-directorate internal trainings was held at the Center for Development of Security Excellence (CDSE) in Linthicum, MD. The purpose of this training was to familiarize the field with the DiT methodology and to complete a series of exercises that walked training participants through a mock facility evaluation to assess their understanding of the methodology.

Moving forward, DSS plans on launching four tests of the integrated Concept of Operations (CONOP) in January and incrementally expand the number of facilities, while training and leading the next set of personnel and facilities through the process by the end of 2018. The goal of these tests will be to develop the Standard Operating Procedure (SOP) and train the initial mobile training team members who will in turn train others on the SOP.

For more information on the DiT methodology, click here.

SECURITY VULNERABILITY ASSESSMENT RATINGS UNDER DiT IMPLEMENTATION

The Letter to Industry on DSS in Transition from the Director, DSS was distributed Jan. 19, 2018 and conveyed the incremental process in which Phase 1 assessments of select facilities will occur in FY18.

Facilities subjected to Phase 1 assessments will not be rated until DSS returns to assess them in FY19. At that time, these facilities will demonstrate their efforts to implement their Tailored Security Plans, and DSS will score them under a new assessment model that will be developed with industry involvement during FY18.

Facilities that are not selected for Phase 1 efforts will continue to be assessed and rated under the traditional security vulnerability assessment model as they have in the past.

SUBMITTING DD254 FORM, NOV 2017 FOR FACILITY CLEARANCE REQUESTS

The new DD254 Form, NOV 2017, includes a "Classification (when filled in):" section at the top and bottom of the form. This section should only be completed if the form is classified. This section does not pertain to the clearance and safeguarding level of the facility security clearance (FCL) required for the classified contract and should not be confused with the FCL level. Please ensure that you complete this section ONLY when the DD254 Form is classified. A classified DD254 should only be submitted through properly accredited classified information technology systems.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS) REGISTRATION UPDATE

We have received feedback that some Industry members are unable to register for the NISS Application. DSS is actively working to resolve this issue and will notify the impacted users when they are able to register. If an Industry member encounters an error in the National Industrial Security Program (NISP) Central Access Information Security System (NCAISS) when registering for their NISS account ("An error occurred while determining the approver for the CAGE Code specified."), please send an email to DSS.NISS@mail.mil with the CAGE Code and the assigned DSS Industrial Security Representative. We will remedy this issue and provide a direct notification when fixed. All other questions should be directed to the DSS Knowledge Center (888-282-7682).

If your account has been locked, please call the Knowledge Center at (888-282-7682) and select Option 1. The Knowledge Center can unlock your account. Please note, the menu recording will be updated shortly to include NISS in Option 1. For more information about NISS, please visit the NISS Website. Thank you for your continued support and patience during the transition!

EVALUATING INSIDER THREAT PROGRAM EFFECTIVENESS

NISPOM Change 2 requires contractors to establish and maintain an insider threat program to detect, deter, and mitigate insider threats. The Industrial Security Letter 2016-02 Revised (06/29/17) provides further clarification of those requirements. As a reminder, your insider threat programs must be able to gather, integrate, and report relevant and available information indicative of a potential or actual insider threat in accordance with NISPOM requirements.

During Security Vulnerability Assessments, DSS is verifying 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 follow-on assessments, DSS will evaluate the effectiveness of industry's insider threat programs. DSS has begun developing that process and 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.

While the process for evaluating effectiveness is being developed, DSS will solicit feedback from industry. Once the process is finalized, industry will be informed prior to implementation.

Although DSS has not begun to evaluate the effectiveness of industry's insider threat programs, we do strongly encourage you to set aside some time to test your own insider threat program for effectiveness. 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.

ANNUAL NATIONAL INDUSTRIAL SECURITY PROGRAM COST COLLECTION

As the Executive Agency for the National Industrial Security Program (NISP) under Executive Order 12829, the Department of Defense is required to provide the Information Security Oversight Office (ISOO) with an estimated annual cost to Industry of complying with NISP security requirements. We determine the costs by surveying contractors who possess classified information at their cleared facility. Results are forwarded to ISOO and incorporated in an annual report to the President.

To meet this requirement, DSS conducts a stratified random sample survey of contractor facilities using a web-based survey and Office of Management and Budget (OMB)-approved survey methodology. Since the sample of cleared facility participants is randomly selected, not all facilities will receive the survey. The survey will be fielded on Jan. 16, 2018 and remain open through COB Jan. 29, 2018. Participation is anonymous. The survey invitation will contain a foreseeresults.com survey link. Verification of the legitimacy of the Survey URL can be obtained through your Cognizant Security Office. Please direct any questions to dss.ncr.dss.mbx.psiprogram@mail.mil.

We appreciate your cooperation and submission of the cost information by Jan. 29, 2018.

E-FCL NISP PSI DATA COLLECTION

The DSS data collection of NISP Personnel Security Investigation (PSI) Projections will open and be available on Jan. 26, 2018 and will end Feb. 23, 2018, and can be accessed through the Electronic Facility Clearance (e-FCL) system. DSS is responsible for projecting Personnel Security Investigations requirements each year. Annual projections acquired from Industry through this collection are the key component in Department of Defense program planning and budgeting for NISP security clearances.

Please note that submitting the PSI projections is independent of e-FCL package submissions; submitting information related to the facility clearance is not required as part of PSI data collection.

A 12-minute tutorial video can be found at Electronic Facility Clearance System (e-FCL) webpage (under "Alerts") to assist in completing the PSI projections. For the best viewing of this video, please save it to your computer (hover the cursor over the link on the web page, and right-click to "save target as ..."). It can be viewed using Windows Media Player, QuickTime, and VLC Player.

We look forward to your participation. If you have any questions, please contact the PSI team at: dss.ncr.dss.mbx.psiprogram@mail.mil.

CREATION OF INTERNATIONAL TRANSFERS WEBPAGE

The DSS Technical Oversight of Programs and Services (TOPS) Division has updated the external DSS.mil website to include a webpage dedicated to International Transfers. This page, much like the Visits and Assurance pages, will serve as a quick reference for those in industry who are unfamiliar with International Transfers or do not handle them on a regular basis.

Visit the International Transfers webpage for more information.

SECURITY EDUCATION AND TRAINING

NEW CI AND INSIDER THREAT CASE STUDIES AVAILABLE

CDSE recently released new Counterintelligence and Insider Threat Case Studies:

- Counterintelligence Case Study – Exploitation of Relationships - Nuclear
- Insider Threat Case Study – Edward Lin (Unreported Foreign Contact)

These case studies can easily be included in an organization’s security education, training, and awareness programs. Both case studies are suitable for printing or easy placement in a company or command newsletter, email, or training bulletin. Access the new case studies today!

UNAUTHORIZED DISCLOSURE BRIEFINGS AVAILABLE

The Unauthorized Disclosure (UD) Program Management Office recently made two of their UD briefings available through CDSE. The UD Security Professional Briefing and the UD Workforce Briefing are both available for download from CDSE. Look for these briefs under UD Training here.

UPCOMING UNAUTHORIZED DISCLOSURE SPEAKER SERIES

Unauthorized Disclosure is the hot topic for our Speaker Series this month. CDSE will host the Unauthorized Disclosure Program Management Office (UDPMO) on Feb. 1, 2018 at noon. Ms. Jeannie Alnidawi from the UDPMO is our guest speaker. She will discuss the requirements for reporting questionable government activities, the differences between Whistle Blowing and Unauthorized Disclosures, and some of what constitutes Unauthorized Disclosure. Register and be part of the conversation! Sign up today at CDSE Webinars**.**

UPCOMING INDUSTRIAL SECURITY WEBINAR

Join CDSE on Thursday, Feb. 15, 2018 at 11:30 a.m. or 2:30 p.m. ET for the "Visits and Meetings in the NISP: What's New?" webinar. This webinar will discuss why it was necessary to make changes to the course, "Visits and Meetings in the National Industrial Security Program (NISP)." It will also address the definitions of visits and meetings in accordance with the NISPOM. Sign up today at CDSE Webinars.

GETTING STARTED SEMINAR FOR NEW FSOs FY18 SCHEDULE

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.

Take a look at our FY18 schedule to see if we will be presenting this course in your neighborhood:

Apr. 3-4, 2018, Atlanta, GA, go here

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

We will also be offering this class at CDSE in Linthicum, MD on Feb. 13-14 and June 12-13, 2018. This course will be given in the hybrid format (instructor-led and Adobe Connect) for the June 12-13 iteration. Please see the website here for additional details regarding the hybrid course.

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). Once completed, register for the course you would like to attend. We look forward to seeing you soon!

SOCIAL MEDIA

Connect with CDSE on Twitter and on Facebook.

Thanks,
ISR
Defense Security Service