DSS Monthly Newsletter

September 2014

(Sent on behalf of ISR)

Dear FSO,

This is the monthly email 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.

INFORMATION

FOURTH ANNUAL VOICE OF INDUSTRY SURVEY

From October 6th to the 31ST, Defense Security Service (DSS) will conduct the fourth annual DSS Voice of Industry Survey. This survey of all Facility Security Officers (FSOs) provides an opportunity for feedback on DSS' performance with respect to the administration and implementation of the National Industrial Security Program. While participation in this survey is voluntary, DSS is requesting a 100 percent response rate in order to maintain and improve the quality of our relationship with cleared industry. This survey will be sent directly by email to all FSOs from DSSVOISurvey@dss.mil with a unique https://www.securitysurveys.net link to your facility's survey. Please send any questions regarding the survey to DSSVOISurvey@dss.mil.

RATING MATRIX UPDATE- CI ENHANCEMENT

Last fall, DSS implemented an update to the Security Vulnerability Assessment Rating Matrix, a tool that enables our representatives to consistently and systematically account for vulnerabilities and enhancements during assessments. As a result of your feedback, DSS is updating the Counterintelligence (CI) enhancement (presently Category 7) by splitting it into two separate categories. One enhancement will focus on "process" (Category 7a) and the other on "performance" (Category 7b):

- **Category 7a:** "Threat Identification and Management" - Encourages facilities to build a CI focused culture by implementing polices, processes, and programs within the security program to detect, deter, and expeditiously report suspicious contact reports (SCR) to DSS.

- **Category 7b:** "Threat Mitigation" - Requires facilities to have SCR reporting that instigates an open investigation by another government law enforcement or intelligence agency. The open investigation must be validated by DSS CI for the rating period. This category can only be awarded if a facility receives credit for Category 7a. There will be no penalty for contractors without open investigations, as achievement in this category will afford *additional* enhancement points for eligible facilities.

The CI enhancement update will further improve the rating process by adding clarity, driving consistency, and properly identifying enhancements that have the most positive impact on contractor security programs. Scoring for the Rating Matrix will remain the same, and there will be *no* changes to the weights attributed to vulnerabilities or enhancements for any facility category.

DSS is targeting October 1, 2014, for full implementation, and will be releasing additional information, including frequently asked questions, on our website soon. Please check back at www.DSS.mil.

DISCOUNTINUED ISSUANCE OF 381-R LETTERS

Effective September 1, 2014, the Defense Security Service (DSS) discontinued the issuance of 381-R letters. Currently, a 381-R is provided to a facility when a company is issued a Facility Clearance (FCL) or a changed condition affecting the information on the 381-R is processed, whereas now, an email will be sent to the facility in lieu of a 381-R requesting the facility perform an Industrial Security Facilities Database (ISFD) FCL verification to view the change. ISFD is the official system of record for facility clearance verification, and the 381-R will no longer be a reviewable item at recurring Security Vulnerability Assessments.

POLICY NEWS AND POSTINGS

August 1, 2014: DSS provides an update on the National Industrial Security Program (NISP) Contract Classification System (NCCS). Link to posting - http://www.dss.mil/isp/policy_news.html

August 27, 2014: DSS provides information on pending insider-threat program requirements for industry. Link to posting - http://www.dss.mil/documents/isp/Policy_InsiderThreat.pdf

OVERDUE PERIODIC REINVESTIGATIONS

Reminder to FSOs to check the PSMNet to determine if personnel have an overdue PR. If they are overdue a PR or are within 90 days of needing a PR, please submit an e-QIP as soon as possible. If the subject no longer requires access, please remove access in JPAS and no PR will be due until the subject needs access again. If subject no longer works for your company, be sure to remove from access and add a separation date. http://www.dss.mil/documents/isp/DSSUpdatesApril10,2014Posting.pdf

ATTENTION JPAS/SWFT/ISFD SYSTEM ACCESS APPLICANTS - SYSTEM ACCESS REQUEST (SAR) PROCESS

Please see http://www.dss.mil/about_dss/news/20110818.html for important information pertaining to changes affecting JPAS/SWFT/ISFD system access applicants; changes were implemented on June 1, 2013, in conjunction with the transfer of various DSS Call Center customer support services to the DMDC Contact Center.

ATTENTION DSS CALL CENTER CUSTOMERS - REVISED CUSTOMER SERVICE MENU OPTIONS

Effective July 15, 2014, the DSS Call Center (888-282-7682) revised its customer service (phone tree) menu options. Specifically, menu options were added in support of NCAISS and OBMS users. Please see http://www.dss.mil/about_dss/contact_dss/contact_dss.html for our current top-level menu options.

ACCESS MAGAZINE

Please see the below link for the most recent Access Magazine:
http://www.dss.mil/documents/about/DSS%20ACCESS%20v3i3%20Web.pdf

SECURITY EDUCATION AND TRAINING

SEPTEMBER 2014 IS CDSE COUNTERINTELLIGENCE AWARENESS MONTH

In honor of the Center for Development of Security Excellence's (CDSE) Counterintelligence Awareness Month, we invite industry personnel to utilize the Counterintelligence (CI) training options available to our partners in industry. CI and security are mutually supportive disciplines with shared objectives and responsibilities associated with the protection of secrets and assets. CDSE has designed CI awareness training material for all cleared defense industry personnel.

NATIONAL CYBERSECURITY AWARENESS MONTH (OCTOBER)

CDSE is pleased to announce our participation in the 11th Annual National Cybersecurity Awareness Month this October. We will be releasing two new webinar topics: Top 20 Security Controls and Trusted Downloading. During this time, we will also be highlighting our current Cybersecurity offerings and how organizations can use these offerings to increase their Cybersecurity posture and awareness. Come check out CDSE as we participate in the 11th Annual National Cybersecurity Awareness Month this October, and don't miss the new training opportunities!

Simply click on **Cybersecurity** under **Training** on our CDSE website or follow this link directly: http://www.cdse.edu/catalog/cybersecurity.html.

Please visit the CDSE catalog at http://www.cdse.edu/catalog/index.html and check out the eLearning courses, the short courses (shorts), and webinars listed in the CI section. There are three new CI courses for Facility Security Officers (FSOs) and several others to choose from. Register at http://www.cdse.edu/catalog/webinars/index.html to participate in the webinar *Critical Elements of a Suspicious Contact Report* scheduled for September 11. Additionally, CDSE has a CI button on the FSO Toolkit. Quick answers to CI questions and easy access to resources are just a click away at: www.cdse.edu/toolkits/index.html.
For new FSOs, join us for a *Getting Started Seminar* where we feature a full day of CI training. Register for the seminar at: http://www.cdse.edu/catalog/classroom/IS121.html. Finally, be sure to join CDSE on social media.

Twitter: www.twitter.com/TheCDSE

Facebook: //www.facebook.com/pages/CDSE-Center-for-Development-of-Security-Excellence/111635548863732

CDSE ANNOUNCES A NEW CYBERSECURITY TOOLKIT

CDSE is pleased to announce the release of a new training product for industry and other entities involved with Cybersecurity. The Cybersecurity Toolkit is an online tool that will provide access to a variety of security resources. This toolkit was developed to assist Cybersecurity personnel accomplish common tasks associated with their key roles and responsibilities. This eliminates the need to search for or recreate Cybersecurity information that is already available. The Cybersecurity Toolkit contains a variety of great information that can be modified and/or adapted to meet the security needs of any organization.

Start using the Cybersecurity Toolkit today! Simply click on **Cybersecurity** under **Toolkits** on our CDSE website or follow this link directly: http://www.cdse.edu/toolkits/cybersecurity/index.html.