DSS Monthly Newsletter

August 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

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. Thank you!

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. Thank you!

DISCOUNTINUED ISSUANCE OF 381-R LETTERS:
Starting 1 September 2014, the Defense Security Service (DSS) will discontinue 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. Once the change takes effect, 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. Once the change takes effect, the 381-R will no longer be a reviewable item at recurring Security Vulnerability Assessments.

OVERDUE PR'S: 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

JPAS SUBJECTS WITH N/A, NON-US CITIZEN OR BLANK: If you received a JPAS message indicating that the subject's JPAS record doesn't accurately reflect US Citizenship, please see the posting on the DMDC website on how to correct the record. Industry FSOs can manually update citizenship for subjects after verification of citizenship occurs. Industry FSOs may need the subject to update DEERS if the subject has a prior DoD affiliation. This can be determined if an Electronic Data Interchange Personal Identifier (EDIPI) is on the JPAS record. You can utilize the JPAS Data Correction Checklist as a tool to assist SO/FSO where to update the Citizenship information.
https://www.dmdc.osd.mil/psawebdocs/docRequest/filePathNm=PSA/appId=560/app_
key_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=JPAS+Data+Correct ion+Checklist.pdf

Please note that for Industry, DMDC will **not** automatically remove the subject's access on 10 August. DSS and DMDC will work together to identify records that need to be corrected and will coordinate on a way ahead.

POLICY NEWS AND POSTINGS FOR JULY

July 28: DSS Updates April 10, 2014 Posting on: Guidance on Managing Personnel Security Clearance Records in the Joint Personnel Adjudication System (JPAS) - Eligibility, Break in Access and Break in Employment. Click here.

July 15 : DSS posts information on the use of JPAS

July 16: Reporting Conduct Involving Marijuana

July 11: DSS posts frequently asked questions on the accountability of Top Secret documents on information systems and electronic media. Click here to view the FAQs

ATTENTION OBMS USERS: AN ISFD ACCOUNT IS NOT A REQUIREMENT FOR ACCESSING OBMS

To access OBMS, you are only required to have an NCAISS account. When OBMS first deployed, there were two mechanisms for users to use in gaining access to OBMS to assist with the rollout:

1) All active ISFD user account users received an email notification providing them step by step guidance on how to register their PKI certificate to obtain NCAISS and OBMS accounts. Knowing your ISFD username and password is required.

Note: If you did not receive the above auto generated email, please follow the below steps and reference the tutorials/user guides locate here: http://www.dss.mil/diss/ncaiss.html

2) Creating an OBMS account through self-registration (steps are located within the NCAISS Tutorial and the OBMS Integration Tutorial located on http://www.dss.mil/di ss/ncaiss.html A user will follow these high level steps (again, the tutorials and user guides are located her http://www.dss.mil/diss/ncaiss.html

- Navigate to https://sso.dss.mil
- Click Register for an Account and complete all required fields
- After clicking register, an email confirmation goes out notifying the user that an NCAISS account has been created
- Navigate to https://sso.dss.mil
- Click Register Certificate and put in the NCAISS ID and password
- you set during the above enrollment process (the user ID emailed to you)
- Click CAC/ECA Login and then select Request/Manage OBMS Access under the "OBMs Quick Links"
- Complete the required fields
- Upon completion the request must be approved. When approved, you will receive confirmation via email

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.

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 NEW COURSE AND WEBINAR: Introduction to the Risk Management Framework

Information technology and systems play an integral role in operations at Department of Defense (DoD). While these systems have brought great benefits to the battlefield and the office, they also represent potential vulnerabilities. DoD systems are subject to threats that can have adverse effects on organizational operations, and assets, as well as the Nation. In an effort to counter those threats, DoD has updated its Cybersecurity policy under DoDI 8500.01 and adopted the Risk Management Framework under DoD 8510.01. At this time there is no immediate impact to the Defense Industrial Base; training is being provided for your awareness. The Defense Security Service is providing two options for learning about this update:

- CDSE's newest Cybersecurity training offering is "Introduction to the Risk Management Framework" CS124.16. This course provides essential information on the transformation of the certification and accreditation process in DoD. Enroll today at: http://www.cdse.edu/catalog/cybersecurity.html.

- CDSE will also provide an overview of the Risk Management Framework during our August 14th Learn@Lunch webinar series. Register today at: http://www.cdse.edu/catalog/webinars/cyber-security/intro-risk-management-framework.html.

For the latest in security training, be sure to follow CDSE on twitter @TheCDSE and join our Facebook community at: http://www.facebook.com/pages/CDSE-Center-for-Development-of-Security-Excellence/111635548863732.

CDSE ANNOUNCES A NEW JOB AID: Industrial Security Facilities Database (ISFD) This job aid provides instructions on how to use the ISFD Facility Clearance Verification and Notification features which were enhanced during the most recent database update. To view the new job aid please visit: http://www.cdse.edu/resources/supplemental-job-aids.html

Thanks,
ISR
Defense Security Service