DSS Monthly Newsletter

January 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

Defense Security Service to Deploy the Annual National Industrial Security Program Cost Collection Survey

January 20, 2014 – February 7, 2014: 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 January 20, 2014 and remain open through COB February 7, 2014. Participation is anonymous. As in years past, the survey invitation will contain a **securitysurveys.net** survey link. Verification of the legitimacy of the Survey URL can be obtained through your Cognizant Security Office. If you have any questions, please direct them to our mailbox: AandE@dss.mil.

We appreciate your cooperation and submission of the cost information by February 7, 2014.

ELECTRONIC FINGERPRINT MANDATE
The USD/I mandate requiring all fingerprints for background investigations to be captured and submitted electronically has passed. Companies who have not yet selected an option for electronic fingerprint capture should review the updated version of the Electronic Fingerprint Capture Options for Industry posted on the DSS website.
(http://www.dss.mil/documents/psmo-i/eFP%20Guide-FINAL%20August%202013.pdf)

Please pay close attention to the 5 options listed which detail specific alternatives to comply. These options are as follows:

1. Company Purchases Equipment (highest cost option to the company but most convenient for larger companies)
2. Company Sharing Resources (companies split cost of equipment purchase and share use of the machine)
3. Company(s) Offering Service (smaller company can use larger company's previously purchased equipment, nominal fee may be associated with service)
4. Third Party Vendor Provides Electronic Fingerprint File (FBI Channelers used as a 3rd party vendor provide EFT file to company to transmit to OPM through SWFT, nominal fee may be associated with service)
5. Other Government Entities (companies can use military services and other government NISP agencies to capture and/or submit EFT file)

For additional resources click here
http://www.dss.mil/documents/about/eFP_Announcement_for_PAO_2.pdf

AskPSMO-I BI-MONTHLY WEBINARS
The PSMO-I will host its next bi-monthly webinar where we answer specific questions related to DoD CAF updates on January 28, 2014 at 1:30PM EST. FSOs should frequent the DSS website for the webinar announcements and registration link. Webinar slides and the mp3 recording of the session are posted to the Archived PSMO-I Webinars and Documents.

SWFT PK-ENABLED LOGIN
- On December 16, 2013, SWFT log on became PK-enabled.
    – Users will still be able to use their existing username and passwords to log into the SWFT
- Beginning April 2014, the username and password logon option will be removed from SWFT, and only PK-enabled log on will be allowed.
- Preparation and training
    – SWFT Newsletter (Volume 2, Issue 2)
    – PKI Frequently Asked Questions
    – SWFT PKI Test Procedures at
      https://www.dmdc.osd.mil/psawebdocs/docRequest//filePathNm=PSA/appId=560/app_key_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=SWFT_PKI_Test+Instructions+v2.pdf
- New HHS and EiD Passport Credentials have been tested in pre-production; Eid Passport is a new commercial PKI provider giving industry more options when it comes to purchasing logon certs for JPAS and SWFT

RRU
Please visit http://www.dss.mil/psmo-i/indus_psmo-i_maintain.html#research for new guidance posted related to RRU Actions.
- **Research**
  Research requests will be forwarded to the PSMO-I for action regarding any front end submission process concerning Interim eligibilities, overdue PR notifications and SF 312 processing. They can also be submitted for any official requests for information by the PSMO-I.

- **Recertify/Upgrade**

Recertify requests will be used by the DoD CAF to assist in any adjudicative action, issues or responding to official requests for information by the DoD CAF. When requesting the reciprocity of eligibility please submit an Upgrade Request to the DOD CAF-Industry Division.

PSI Submission Update
DSS received FY14 Funds Authorizations for Personnel Security Investigations for Industry (PSI-I) on Oct. 23, 2013. As a result, the Personnel Security Management Office - Industry (PSMO-I) was only able to start submitting FY14 e-QIPs to the Office of Personnel Management (OPM) on Oct. 24, 2013. There is currently a backlog of over 7,000 e-QIPs in the queue for review and submission to OPM; that is down from a high of 13,992. PSMO-I is reviewing the e-QIPs first in/first out. Please be patient as we continue to work through the backlog and return to a steady state.

If you submitted an e-QIP, but the subject no longer needs the clearance, please update JPAS with a separation date so we can stop the e-QIP. We will continue to provide status updates on the website.

Best Wishes for the New Year from PSMO-I!

Changes to USPS Express Mail and Use of Labels
Please click the below link for additional information:
 http://www.dss.mil/isp/policy_archives.html

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!

SECURITY EDUCATION AND TRAINING

CDSE WEBINARS
The beginning of a new year is a good time to get into a Learn@Lunch routine. Make plans now to join us on the second Thursday of each month for our monthly, 30 minute industrial security/ counterintelligence Learn@Lunch webinar series. Topics planned for 2014 include Insider Threat, Technology Control Plans, Potential Espionage Indictors, Standard Practice Procedures, Classified Foreign Visit Process, and Lifecycle of a System Security Plan (SSP).

We will kick-off our 2014 Learn@Lunch series with Insider Threat on Thursday, January 9, 2013 at 11:30 a.m. and 2:30 p.m. EST. Not only will this webinar help you to understand what an Insider Threat is, it will also help you to recognize the threat and provide appropriate countermeasures.

Go to: http://www.cdse.edu/catalog/webinars/counterintelligence/insider-threat.html to sign up for this webinar.

Don't forget that CDSE offers other webinars that might also be beneficial to you and your security program. You can check out all of the CDSE upcoming webinars at: http://www.cdse.edu/catalog/webinars/index.html.

Thanks,
ISR
Defense Security Service