DSS Monthly Newsletter

February 2016

(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.

eFINGERPRINT REPLACING HARDCOPY FINGERPRINTING

Effective October 1, 2016, all fingerprints associated with Submitting Office Number (SON) 346W must be submitted electronically to the Office of Personnel Management (OPM). All hardcopy fingerprint submissions and investigation requests will be rejected if OPM does not receive an electronic fingerprint within 14 days of the investigation submission date. In 2009, the Under Secretary of Defense for Intelligence directed DoD components to initiate a transition to electronic capture and submission of fingerprint images for all background investigations. Since then, the National Industrial Security Program has been a leader in submitting electronic fingerprints to the Secure Web Fingerprint Transmission (SWFT) application. Over 6,500 electronic fingerprints were submitted to OPM in December 2015, and less than one percent of the total (only 99 fingerprint cards) was submitted in hardcopy. The Personnel Security Management Office for Industry will be contacting Facility Security Officers (FSOs) and Requesting Officials who recently submitted hardcopy fingerprints in an effort to achieve 100 percent electronic submission. Click here to view the electronic fingerprint capture options for Industry.

PERSONNEL SECURITY INVESTIGATIONS (PSI) INDUSTRY DATA COLLECTION

DSS is responsible for projecting Personnel Security Investigations for Industry requirements each year. The data collection for PSI projection requirements will be conducted in March 2016 through the Electronic Facility Clearance System (e-FCL) Submission Site. Annual projections acquired from Industry through this collection are the key component in Department of Defense program planning and budgeting for NISP security clearances.

In preparation for this upcoming data collection, please ensure that your e-FCL login (your email address) and password are current by February 29, 2016. A completed e-FCL package is not required to participate in the data collection; only an established account is necessary to input the PSI requirements.

If you have forgotten your password or your password has expired, use the "Reset Password" link on the e-FCL Submission Site login page.

Additional instructions and information regarding the PSI data collection will be forthcoming prior to deployment. We look forward to your participation. If you have any questions, please contact us at: PSIprogram@dss.mil.

OUTGOING INTERNATIONAL VISIT REQUEST SUBMISSIONS

All visit request forms have been updated to include the following statement: "I hereby attest to the accuracy and certify the information to be released during this visit has been approved for release prior to the visit by the appropriate designated authority and/or an export authorization has been granted."

By signing the visit request, the facility security office is validating they have accurately completed all required fields on the form, verified each visitors' information in JPAS, and ensured the request complies with U.S. export laws and regulations.

Beginning April 1, 2016, DSS will no longer accept old versions of the forms that are missing the statement. The updated visit request forms can be found on the Visits webpage.

UNITED KINGDOM (UK) EMERGENCY VISIT SUBMISSION CHANGE

Effective immediately, the UK is no longer accepting emergency letters of justification written by the U.S. Government Customer or the UK site point of contact. The UK Visit Control Office will only accept emergency letters of justification written by the UK Government Sponsor. Letters of invitation do not qualify as an emergency letter of justification.

This information can be found under the country specific requirements section of the Visits webpage.

For questions or concerns please contact rfv@dss.mil.

DSS KNOWLEDGE CENTER

On March 28, 2016, The Defense Security Service will implement a new call center designed to be more customer-centric by providing improved and efficient solutions. The "Knowledge

Center" replaces the current DSS Call Center, but will retain the current phone number: (888) 282-7682.

The Knowledge Center will use an automated system, which offers comprehensive contact management capabilities with built-in queuing and interactive voice response. It will be deployed with "contact service queues" established across various DSS organizations.

As part of these queues, the caller will select which item best describes the subject area of their issue and will be routed to either the appropriate office and/or subject matter expert (SME) (normal business hours) or voicemail (after business hours). The options are:

1. System Access Issues (ISFD, e-QIP, etc.)
2. Personnel Security Inquiries
3. Facility Clearance Inquiries
4. OBMS
5. CDSE / STEPP
6. International
7. Policy

The Knowledge Center draws from customer service best practices for issue resolution. It is designed to efficiently identify and route the caller to the appropriate SME. For example, if an FSO has questions concerning Facility Clearances, the Knowledge Center will route the call directly to a SME in the Facility Clearance Branch. This program will enable DSS to assist Industry by providing accurate information in a timely manner.

DSS will continue to provide updates on the progress of the Knowledge Center through the Voice of Industry and www.dss.mil.

SECURITY EDUCATION AND TRAINING

CDSE LAUNCHES NEW COURSE – CONTINUOUS MONITORING (CS200.16)

This course provides students with in-depth knowledge and understanding of the Risk Management Framework (RMF) Step 6, and how RMF supports Information Security Continuous Monitoring (ISCM). The course also includes lessons on how configuration management, auditing, counterintelligence, and cybersecurity personnel support continuous monitoring.

Upon completion, students will have a better understand how maintaining ongoing awareness of information security, vulnerabilities, and threats supports organizational risk management decisions.

Full details and registration are available at:
http://www.cdse.edu/catalog/cybersecurity.html.

Check out some of CDSE's other cybersecurity course offerings at:
http://www.cdse.edu/catalog/cybersecurity.html

PREVIEW CDSE WEBSITE REFRESH – SITE LIVE ON THE 1ST OF MARCH

CDSE is excited to announce the launch of its refreshed website on March 1, 2016 - http://www.cdse.edu/ . Preview the site at http://betaweb.cdse.edu/. Users will notice an overall improvement in their experience, thanks to a new interface and several new qualities.

- Simple – fewer links on homepage, prominently displaying major sections of the website.
- Accessible – optimal viewing and interaction experience across a wide range of devices.
- Easy to Navigate – streamlined navigation and search menu dedicated to CDSE content.
- Social Media Integration – expanded and enhanced access to social media platforms.

Brand new features include Popular Content, Common Questions, and an A-Z Index to help find information. Please send comments or suggestions to cdseweb.requests@dss.mil.

Thanks,
ISR
Defense Security Service