DSS Monthly Newsletter
July 2016

(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.

DSS THANK YOU TO INDUSTRY RMF PILOT PARTICIPANT COMPANIES

On behalf of DSS, I would like to thank Harris Corporation, Lockheed Martin Corporation, L-3 Communications, Northrop Grumman, nou Systems, and SRI International for participating in our very important Risk Management Framework pilot project. We understand that as security professionals, your schedule (and that of your staff) is full and demanding.

The pilot's results helped us understand many of the challenges associated with risk management. Notably, the schedule implications led to us extend the implementation deadline. Your involvement played a crucial role in making this happen.

For all NISP facilities, if you need a refresher as you prepare for transition, take CDSE courses for general RMF baseline. You can also access the DSS RMF Resource Center at any time.

Thank you again for your time and valuable contributions to the NISP!

Sincerely,
Selena Hutchinson, GSLC
Deputy Assistant Director
NISP Authorizing Official
Defense Security Service

INDUSTRY e-QIP SUBMISSION UPDATE

To stay within its budget authority for PSI-Is, DSS metered the expenditure of PSI-I funds and maintained a daily limit on the number of cases submitted to the Office of Personnel Management (OPM). This limit caused a delay in processing industry submissions to OPM, and increased the inventory. DSS recently received additional funding for the PSI-I program through a reprogramming approved by Congress. With this reprogramming, DSS will continue to process all PSI-I requests and work down the inventory. As a result, industry should soon see improved timelines. Continue to submit initial requests and periodic reinvestigations.

RESEARCH, RECERTIFY, AND UPGRADE (RRU) REQUESTS

The Personnel Security Management Office for Industry (PSMO-I) is overhauling the RRU process and is now only accepting RRU submissions via JPAS under the following three classifications:

- RESEARCH: Reciprocity Requests.
- RECERTIFY: Official government requests for information from DoD CAF, DOHA or DSS. For example: Requests for information such as name changes, marriage to foreign nationals, follow-ups to Incident Reports, etc.
- UPGRADE: The FSO has reason to believe the eligibility line in JPAS is incorrect. For example: Eligibility states secret but should be TS, or it has an LOJ but should be an eligibility, etc.

All other personnel security related questions and concerns should be directed to the DSS Knowledge Center at (888) 282-7682.

INTERMIM SECRET DETERMINATIONS

Effective August 1, 2016, Industry interim Secret determinations will be based on the following: Acceptable proof of citizenship, favorable review of a completed Standard Form 86, favorable review of local personnel, base, military police, medical, and security records as applicable, an appropriate investigation opened by the Investigation Service Provider, and favorable review of the Federal Bureau of Investigation Criminal History Report (fingerprint report). The interim Secret determination will be processed after PSMO-I submits the investigation request to OPM and receives the fingerprint results.

e-FP UPDATE

Effective October 1, 2016, all fingerprints associated with SON 346W must be submitted electronically to OPM or the fingerprints will be rejected. OPM will also reject any investigation request if an electronic fingerprint is not received within 14 days of request submission. The National Industrial Security Program (NISP) is among the leading components in submitting electronic fingerprints to the Secure Web Fingerprint Transmission (SWFT) application, with more than 97 percent electronic submissions. PSMO-I will be contacting the Facility Security Officer and Requesting Official of those companies that recently submitted hardcopy fingerprints to achieve 100 percent electronic submission.

SECURITY EDUCATION AND TRAINING

MAINTAINING YOUR SPēD CERTIFICATION

Following recent changes to SPēD certification maintenance procedures, maintaining your SPēD certification is now easier than ever. Certification Maintenance Form (CRF) and SPēD certifications will now share a common expiration date. Certificants still must earn 100 Professional Development Units (PDUs) during their two-year certification maintenance cycle. Map out your maintenance strategy today, and keep your SPēD certifications active. Learn more here.

NEW INSIDER THREAT JOB AID

NISPOM Change 2 requires Industry to implement Insider Threat programs. Learn how to establish and maintain an Insider Threat program at your facility with our new job aid, “Insider Threat Program (ITP) for Industry.” The ITP job aid also provides information on conducting Insider Threat training, the requirements, definitions, resources and more. Access the job aid here.

NEW FOCI TOOLKIT

The Center for Development of Security Excellence (CDSE) recently launched the new “FOCI Outside Directors, Proxy Holders, and Voting Trustees Toolkit.” This toolkit steers users to the resources needed to help perform the role of Outside Director (OD), Proxy Holder (PH), or Voting Trustees (VT). Access the toolkit here.

NEW CRITICAL PROGRAM INFORMATION (CPI) SHORT

CDSE has released the Critical Program Information (CPI) short. The short provides security officers with an introduction to CPI, which includes definitions, requirements for enhanced security protection, and direction to applicable supporting policies. It replaces the previous CDSE CPI course. Access the short here.

NEW VIDEO LESSONS

CDSE is pleased to announce the release of the Counterintelligence Awareness Video lesson. Are you looking for an impactful way to provide threat awareness? Watch and learn how counterintelligence supports security efforts by identifying foreign, insider, and cyber threats. The video is less than four minutes and can be viewed independently, or as part of our micro lesson. Both avenues offer great ways to encourage threat awareness at your facility or installation. Access the video lesson here.

In addition, CDSE added “Social Media Incorporation into Federal Background Investigations” to the Security Awareness Hub. This video lesson developed from congressional testimony discusses the way ahead for U.S. government’s use of social media in Federal Background Investigations.

UPCOMING INDUSTRIAL SECURITY TRAINING

Seats are still available for the following CDSE class:

“Getting Started Seminar for New FSOs,” August 15-16, 2016 (Burlington, MA)

This course is open to Facility Security Officers (FSOs), Assistant Facility Security Officers (AFSOs), and Security Specialists. A prerequisite course titled “FSO Role in the NISP” is required to register and must have completed after November 23, 2015.

VIRTUAL INSIDER THREAT SYMPOSIUM FOR INDUSTRY - SEPTEMBER 15

The issuance of Change 2 to DoD 5220.22-M, “National Industrial Security Program Operating Manual (NISPOM),” will bring about new Insider Threat Program requirements. Join CDSE for a live online event following the policy release. We will discuss the requirements, available tools, and resources provided by DSS to help our industry partners. Sign up today for this and other webinars here.

Insider Threat
Virtual Insider Threat Symposium for Industry Requirements Under Change 2 to NISPOM
Thursday, September 15, 2016
10 am Eastern Time

ARCHIVED WEBINAR AVAILABLE

Did you miss the CDSE Speaker Series episode, “Economic Espionage” with Acting Chief John Hartnett of the Federal Bureau of Investigation Economic Espionage Unit? No problem! It is now available for your viewing. You can access this webinar and more in our archives.

SOCIAL MEDIA

Connect with CDSE on Twitter (@TheCDSE) and on Facebook.

Thanks,
ISR
Defense Security Service