DSS Monthly Newsletter

April 2017

(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.

REVISION OF STANDARD FORM (SF) 328, CERTIFICATE PERTAINING TO FOREIGN INTERESTS

On April 5, the SF 328, "Certificate Pertaining to Foreign Interests," supporting the National Industrial Security Program (NISP) was revised and has a new issuance date of March 2017, under Office of Management and Budget (OMB) Control Number 0704-0194. OMB approval for the SF 328 will expire on Sept. 30, 2019, unless the form is renewed prior to that date. Previous blank forms are obsolete. Revisions to the form include the removal of the prior requirement for application of a corporate seal. A single witness to the contractor representative signing the SF 328 is required, and that witness cannot be the government representative.

Forms may be obtained through the General Services Administration website, or the DSS Checklist for New Facility Security Clearances. Existing records of DSS and contractors must be updated as changed conditions affecting the SF 328 occur.

ELECTRONIC FACILITY CLEARANCE (e-FCL) SYSTEM UPDATED WITH REVISED SF 328

On April 5, 2017, DSS announced that the SF 328, "Certificate Pertaining to Foreign Interests," supporting the NISP was revised and has a new issuance date of March 2017, under OMB Control Number 0704-0194.

In the e-FCL system, the previous version of the SF 328 remains available to complete via digital form. Contractors should:

1) Continue completing the digital form in e-FCL as the questions on the form have not changed, and
2) Complete and upload a signed copy of the revised SF 328 as part of the Initial or Change Condition Package. *Note: The print button for the digital form has been temporarily disabled.*

A link to the revised SF 328 will be available in the system in the coming weeks. In June 2017, the e-FCL's digital SF 328 will be updated to the revised version, and the print button will be re-enabled.

If you have any questions, please contact your assigned ISR.

RISK MANAGEMENT FRAMEWORK (RMF) INFORMATION SYSTEM (IS) OBMS SUBMISSIONS

Effective immediately: IS that are transitioning to National Institute of Standards and Technology (NIST) Risk Management Framework in accordance with the DSS Assessment and Authorization Process Manual (DAAPM) are required to be submitted as new submissions. Industry should submit in the ODAA Business Management System (OBMS) as a new "Initial Accreditation." If Industry submits as a "Reevaluation/ Reaccreditation," DSS will reject the re-submission and direct the Information Systems Security Manager (ISSM) to submit as a new system. A new submission provides Industry with the opportunity to incorporate updated system plan information, new System Security Plan (SSP) and supporting artifacts, and levels of Confidentiality, Integrity, and Availability.

If you have questions or concerns, please contact your assigned Information Systems Security Professional (ISSP). In addition, information can be found at the DSS RMF Website.

SIPRNET PUBLIC KEY ENABLING (PKE) GUIDANCE

Government programs sponsoring cleared contractor SIPRNet connections can now sponsor a contractor for tokens directly within the Secure-Defense Enrollment Eligibility Reporting System (S-DEERS). Sponsors are advised to obtain tokens for their cleared contractors as soon as possible.

Contractors with systems authorized to connect to a government-sponsored SIPRNet connection are required to implement SIPRNet tokens in accordance with USCYBERCOM TASKORD J3-12-0863 by October 01, 2017 where technically feasible. Contractors will no longer be identified as "Temporary Exception Users" after this date.

Systems without a domain environment must wait for the 90 meter software vendor to provide a local login solution; however tokens for web site authentication will be used when required by the site.

Additional information can be found at the DISA SIPRNet PKE webpage.

Note: Personnel who used DoD-approved 90meter Smart Card Manager products on DoD Networks must have a valid licensing agreement with 90meter. Due to licensing agreements, DoD cannot provide 90meter Smart Card Manager V1.4.32S on the IASE Website. Users may acquire DoD-approved 90 meter products directly from sales1@90meter.com.

MEMOS ISSUED REGARDING PERSONAL SECURITY CLEARANCE EXPIRATION AND EXTENSION OF PERIODIC REINVESTIGATIVE TIMELINES

On December 7, 2016, the Office of the Undersecretary of Defense for Intelligence signed a memorandum reminding DoD Components that personnel security clearances do not expire. Individuals with current eligibility in the Joint Personnel Adjudication System (JPAS) should not be denied access based on an out-of-scope investigation. When the system of record shows current adverse information, but eligibility is still valid, access may continue. The memorandum is provided here for your ease of reference.

On January 17, the Office of the Undersecretary of Defense for Intelligence signed a memorandum extending DoD Periodic Reinvestigation (PR) timelines to address the background investigation backlog. Tier 3 PRs will continue to be conducted every ten years and Tier 5 PRs will be initiated six years after the date of the previous investigation. Please view the eMemorandum for specific guidance.

UPDATE ON INDUSTRY TIER 5 REINVESTIGATIONS (T5R) EXPIRATIONS AND REJECTIONS

PSMO-I is currently managing the investigation request inventory in order to stay within our budget authority, with priority given to requests for initial clearances. This may result in Tier 5 Reinvestigations either terminating from the system or being rejected if a Special Access Program (SAP) Caveat is not identified as described in the February 10, 2017 guidance available on the DSS website (News Archive, “Clarification on submission of Top Secret Periodic Reinvestigations”).

Note: A SAP Caveat applies only where DoD Policy explicitly states an investigation must be conducted at five year intervals for personnel within a certain program. The SAP Caveat does not apply to every person on a SAP, but only specific programs designated by DoD in writing.

Please do not submit/resubmit for Top Secret reinvestigation unless the requisite SAP Caveat criteria is met and clearly identified. PSMO-I will provide additional guidance on submission of requests for Non-SAP Caveat Tier 5 Reinvestigations through public communications and a system of record messaging.

To facilitate the change in periodicity of Top Secret Reinvestigations and clearance timeliness issues, on December 7, 2016, the Office of the Undersecretary of Defense for Intelligence signed a memorandum reminding DoD Components that personnel security clearances do not expire. Individuals with current eligibility in JPAS should not be denied access based on an out-of-scope investigation. This memorandum is available on the DSS website and was disseminated to non-DoD NISP signatories on March 28, 2017.

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) DEPLOYMENT UPDATE FOR INDUSTRY

Once DISS is fully deployed, it will replace the Joint Personnel Adjudication System (JPAS), to serve as the system of record to perform comprehensive personnel security, suitability and credential eligibility management for all military, civilian, and DOD contractor personnel. DISS provides secure communications between Adjudicators, Security Officers and Component Adjudicators in support of eligibility and access management. DISS will deploy in a phased approach, with Phase 1 (DISS 1.0) rolled out to users incrementally, starting with White House Staff and finishing with Industry. Deployment for Industry has shifted from 3rd Quarter FY17 to a date yet to be determined. In the meantime, DSS continues to work with Industry to review DISS capabilities and identify requirements. See the DISS website for the most up-to-date information.

KNOWLEDGE CENTER CLOSED APRIL 28, 2017

Personnel Security (PCL) inquiries (option #2)—to include e-QIP authentication resets of the DSS Knowledge Center—will be closed on Friday, April 28, 2017 to conduct internal training to deliver the highest quality customer service to Industry and Government callers. Normal operations for PCL and e-QIP inquiries will resume on Monday, May 1, 2017. Remember, the PCL portion of the DSS Knowledge Center typically closes on the last Friday of each month.

SECURITY EDUCATION AND TRAINING

REGISTER FOR AN UPCOMING GETTING STARTED SEMINAR

The live, instructor-led training "Getting Started Seminar for New FSOs" contains two full days of security-related and counterintelligence awareness training. Join us at one of our upcoming iterations:

- "Getting Started Seminar for New FSOs," June 6-7 (Linthicum, MD)*
- "Getting Started Seminar for New FSOs," June 19 (NCMS Conference, Anaheim, CA)**
- "Getting Started Seminar for New FSOs," August 15-16, 2017 (Westford, MA)

*Although this course will be offered as both a live session at our Linthicum, Maryland facility and a virtual session via Adobe Connect, registration is only available for the live session at this time.

**This is a modified, one day version of the course.

Register today!

NEW CASE STUDIES AVAILABLE

The Center for Development of Security Excellence (CDSE) has three new case studies available for easy inclusion into an organization's security education, training and awareness programs.

- **Counterintelligence Awareness Case Study**: **Front Companies**
  This job aid discusses how the dual citizen owner of Arc Electronics Inc. attempted to use his company to export microelectronics to Russia.

- **Insider Threat Case Study: Mozaffar Khazaee**
  This job aid serves as a reminder that Insider Threats can have complex and unforeseen motivations. In this case, Mozaffar Khazaee attempted to transfer sensitive technology in an attempt to gain employment with the government of Iran.

- **Unauthorized Disclosure (UD) Case Study: Benjamin Bishop**
  This job aid identifies the impacts UD causes to National Security. In this case, Mr. Bishop was successfully targeted by a much younger Chinese woman who travelled to the U.S. on a student visa.

All of the case studies are suitable for printing or easy placement in a company or command newsletter, email, or training bulletin. Access the new job aids here.

NEW AND UPCOMING INSIDER THREAT PRODUCTS

- **New Insider Threat Micro-Learning video lesson**
  Watch, Think, and Dig Deeper in less than five minutes. Find it here.

- **New Insider Threat Awareness Game**
  Looking for a fun way to encourage Insider Threat awareness at your organization? Share CDSE's Insider Threat Crossword Puzzle with your personnel. This popular game is a quick and easy way to remind the workforce of messaging associated with the Insider Threat.

- **New Insider Threat Vigilance Campaign Guidance Document**
  Want more information on implementing an Insider Threat Vigilance Campaign at your organization? See the guide for frequently asked questions, links to resources, and a sample implementation plan.

- **New Insider Threat Posters**
  CDSE introduces the customizable Insider Threat Poster. Add a reporting or hotline number, and even your organization's name and logo.

All CDSE awareness posters are available for download in multiple sizes. Browse the catalog.

COMING SOON: INSIDER THREAT “SHORT” FOR SENIOR EXECUTIVES

Thanks to the community for providing subject matter expertise in the development of our latest learning product. This “Short” is designed for the Insider Threat Senior Executive who does not have day-to-day oversight of the Insider Threat Program. The product provides a policy and standard overview in less than 12 minutes. Find the short and all of our learning products in the CDSE Insider Threat Training Catalog.

MARKING CLASSIFIED INFORMATION JOB AID UPDATED

CDSE recently released the updated Marking Classified Information Job Aid to reflect recent policy changes. This job aid provides the requirements and methods for marking classified documents and other classified materials. It addresses general marking requirements, marking originally classified information, derivatively classified information, special types of documents and materials, changes, foreign government information, and Atomic Energy information. Access the job aid here.

SOCIAL MEDIA

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

Thanks,
ISR
Defense Security Service