DSS Monthly Newsletter
January 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.

ACCREDITATION/AUTHORIZATION EXPIRATION REMINDER

As stated in the Defense Security Service Assessment and Authorization Process Manual (DAAPM) Section 4.6 and the Defense Security Service Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM Sections 3.2.4 and 3.2.5, the authorization decision document (i.e., Approval to Operate/Authorization to Operate (ATO)) is time-driven. The Authorizing Official (AO) will identify an expiration date not to exceed three years. Processing beyond this date is unauthorized and will be considered a violation of the National Industrial Security Program Operating Manual (NISPOM). Failure to resubmit the System Security Plan (SSP) well in advance of the expiration date may result in an accreditation/authorization lapse.

If you have questions or concerns, please contact your assigned Information Systems Security Professional (ISSP).

NISP CONTRACTS CLASSIFICATION SYSTEM (NCCS)

NCCS establishes a centralized repository for the collection of classified contract security requirements and supporting data while automating the DD Form 254 (DoD Contract Security Classification Specification) processes and workflows. In June 2016, NCCS reached initial operating capability (IOC) and started implementation. We are proud to announce that on December 23, 2016, NCCS reached full operational capability (FOC).

DSS will be implementing NCCS in a phased approach for both government and industry as follows: Phase 3 (January-April 2017), Phase 4 (May-August 2017), Phase 5 (September-December 2017). If your company is interested in implementing NCCS, please send an email to DSS.NCCS@mail.mil. For additional information on NCCS, see the DSS website.

REVISION OF DD FORM 441 AND DD FORM 441-1

The "Department of Defense Security Agreement" (DD Form 441) and "Appendage to the Department of Defense Security Agreement" (DD Form 441-1) were revised and are available here.

Revisions to the forms include the removal of the prior requirement for a corporate seal. A witness to the contractor representative signing the DD Form 441 is required. A witness is not required for the DD Form 441-1. Existing records of DSS and contractors must be updated as changed conditions affecting the DD Form 441 and DD Form 441-1 occur; however, the forms do not need to be re-executed simply to use the new versions.

NOTICE OF SIX-YEAR SUBMISSION FOR PERIODIC REINVESTIGATIONS

Effective immediately, DSS will submit Tier 5 Periodic Reinvestigations (PRs) for industry personnel six years after the date of the previous investigation rather than at the five-year mark to the National Background Investigations Bureau (NBIB) of the Office of Personnel Management. This change in periodicity will be reevaluated prior to December 31, 2017. Additional information for Facility Security Officers on when and how to submit Tier 5 PRs at the six-year mark will be provided at a later date. Therefore, we are asking that industry no longer submit Tier 5 PRs unless directed by DSS. This change in Tier 5 PR submission periodicity will keep the Tier 5 PR investigations within the current seven year reciprocity guidelines, will continue reducing the backlog of personnel security investigations and will enable DSS to prioritize initial investigations and improve timeliness for interim determinations. Exceptions will be made for those Tier 5 PRs required for Special Access Programs (SAPs) as determined by the Government Contracting Activity (GCA). To identify new submissions under this caveat, please include the following:

- Applicant requires PR processing due to their involvement in a designated caveat program.
- *contact information for GCA*

In addition, T5 PRs currently residing with DSS will only be processed if the above exception is met. To identify those T5 PR exceptions for investigation requests currently with DSS, please submit an RRU (Recertify) with the following information:

- Applicant requires PR processing due to their involvement in a designated caveat program
- *contact information for FSO*
- *contact information for GCA*

As a reminder, the Office of the Undersecretary of Defense for Intelligence signed a memorandum on December 7, 2016, 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 ease of reference.

INTRODUCTION TO DISS

The Defense Information System for Security (DISS) is a family of systems that will serve as the system of record for comprehensive personnel security, suitability and credential management of all military, civilian, and DoD contractor personnel. DISS also provides secure communications between adjudicators, security officers and component adjudicators in support of eligibility and access management. DISS is undergoing a phased deployment and is set to launch for Industry in the 3rd Quarter FY17.

The Personnel Security Management Office for Industry (PSMO-I) hosted a webinar on Tuesday, January 24, 2017, with special guest speakers from the Defense Manpower Data Center (DMDC) who provided a demonstration of DISS, including a proposed timeline that ensures Industry readiness for deployment. PSMO-I webinars (to include the recorded mp3 of the audio and the slides in PDF form) are always posted to the DSS website two weeks after the live event. Past presentations and audio can be found here.

Finally, the DISS website is now available on the DMDC PSA site. Much like the JPAS link is used today, the DISS website will provide authoritative information to the DISS user community to include: Account Management Policy, Account Request Procedures, Release Notes, Frequently Asked Questions and DISS news/announcements. Remember to visit and bookmark the site to stay up-to-date on the latest DISS developments.

KNOWLEDGE CENTER CLOSURE REMINDER

Reminder: the Personal Security Clearance (PCL) portion of the DSS Knowledge Center typically closes on the last Friday of each month for internal training to deliver the highest quality customer service to Industry and Government callers. Normal Knowledge Center operations for PCL and e-QIP inquiries will resume on the first non-federal holiday business day following these closures.

PERSONNEL SECURITY INVESTIGATIONS (PSI) DATA COLLECTION

DSS is responsible for projecting PSI requirements each year. The data collection for PSI projection requirements will be conducted in March 2017 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 28, 2017. 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 PSI mailbox at: dss.ncr.dss.mbx.psiprogram@mail.mil.

MEMO ISSUED REGARDING PERSONAL SECURITY CLEARANCE EXPIRATION

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. 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.

UPDATED RISK MANAGEMENT FRAMEWORK (RMF) SYSTEM SECURITY PLAN (SSP)

The DSS NISP Authorization Office (NAO) has released the new Excel System Security Plan template for RMF plan submissions. The updated SSP incorporates the feedback received from Industry. The updated format will streamline both the SSP development and assessment process. The updated SSP is posted on the DSS RMF Website.

If you have questions or concerns, please contact your assigned Information Systems Security Professional (ISSP). If you have specific questions about the format or content of the SSP, please provide comments and questions to dss.quantico.dss-hq.mbx.odaa@mail.mil.

UPDATE TO SELF-INSPECTION CERTIFICATION IN e-FCL

On May 18, 2016, the Department of Defense published Change 2 to DoD 5220.22-M, "National Industrial Security Operating Manual (NISPOM)." NISPOM Change 2 requires contractors to establish and maintain an insider threat program to detect, deter and mitigate insider threats.

NISPOM Change 2 also requires a senior management official at the cleared facility to annually certify to DSS in writing that a self-inspection has been completed in accordance with the provisions of NISPOM paragraph 1-207b. Beginning January 2017, contractors must annually complete this certification in e-FCL. Additionally, contractors must make self-assessment reports available to DSS during security vulnerability assessments.

The self-inspection certification will be available on the organization summary page in e-FCL. Additional information can be found in the Self-Inspection Handbook for NISP Contractors and in the eFCL Submission Site User Guide (for Contractors), Section 6.2.

***UPDATE** Beginning in early February, in addition to checking the certification box in e-FCL, contractors will identify the name of the Senior Management Official that certified the self-inspection.*

SECURITY EDUCATION AND TRAINING

NEW WEBINARS NOW AVAILABLE IN ARCHIVE

Did you miss the "Understanding your e-FCL Submissions" or "Assessment and Remediation Using the SCAP Tool and POA&M Template" webinars this past December? Visit our archive now to view recordings that includes downloadable Center for Development of Security Excellence (CDSE) Certificates of Training for both webinars. Slides and handouts are also available. Access the Industrial Security webinar here and the Cybersecurity webinar here.

The CDSE Security Speaker Series Webinar on Behavioral Analysis in Insider Threat was a big success. Visit our archive and view special guest Dr. Robert Gallagher from the Defense Insider Threat Management Center, as he discusses the role of behavior analysis in Insider Threat Programs. The session focused on the unique insight this discipline brings to insider threat detection and mitigation.

UPCOMING CLOUD COMPUTING WEBINAR

Join CDSE on Thursday, February 9, 2017 at 11:30 a.m. or 1:30 p.m. Eastern for the "Cloud Computing" webinar. This webinar will cover basic storage technologies, specifically the DoD-approved cloud service providers (CISPs). It will also focus on the characteristics of cloud solutions, and the security features and requirements for cloud technologies. Sign up today!

NEW CYBERSECURITY VIDEO LESSONS

CDSE recently launched two new Cybersecurity video lessons. The "Social Media Video Lesson" highlights the risks and concerns associated with social media. The "Ransomware Video Lesson" covers the dangers of ransomware malware and how to protect against it. Access both videos here.

NEW INSIDER THREAT TOOLKIT TAB – VIGILANCE CAMPAIGN

Instilling a sense of vigilance in the general workforce is a basic tenant of establishing an insider threat program. Annual awareness training is a start, but the message can diminish over time. Developing a vigilance campaign for your organization is an effective solution. Deploying regular messaging, awareness, and communications materials ensures that the general workforce is prepared to recognize and respond to the insider threat. Visit the Insider Threat Toolkit and select the "Vigilance Campaign" tab for resources and materials to launch a campaign at your organization.

VIRTUAL FSO SEMINAR RESCHEDULED

Due to technical enrollment difficulties, the February 15-16, 2017 virtual seminar "Getting Started Seminar for New FSOs" (IS121.01) has been postponed until June 6-7, 2017. Please return to the course catalog and sign up for the June 6-7, 2017 iteration, which will also be

offered as a live instructor-led course in Linthicum, Maryland or virtually through Adobe Connect.

SOCIAL MEDIA

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

Thanks,
ISR
Defense Security Service