DSS Monthly Newsletter
February 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.

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 (PCLs) 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.

CLARIFICATION ON TOP SECET PERIODIC REINVESTIGATION SUBMISSIONS

Effective February 10, 2017, DSS implemented the following change(s) to the January 6, 2017 guidance posted on www.dss.mil concerning Tier 5 Periodic Reinvestigations (T5 PR) caveat programs. The following National Security e-QIPs will be submitted to the National Background Investigations Bureau (NBIB) for scheduling by the Personnel Security Management Office for Industry (PSMO-I):

1. New T5 PR e-QIPs for Special Access Programs (SAP) where the SAP policy, as of February 10, 2017, explicitly states a T5 PR is due every 5 years. (This will be considered a caveat program.) Note: SCI is NOT considered an exception and should not be submitted to PSMO-I. The Security Assistance Policy Coordinating Office (SAPCO) guidance was posted to the DSS website for reference.
2. Existing T5 PR e-QIPs (those in current DSS inventory).
3. New and existing initial investigations T3 and T5 e-QIPs.
4. New and existing T3 PR e-QIPs.

Please do not submit RRUs for caveat T5 PRs. If you previously submitted a RRU for T5 PR prioritization, please attempt to cancel the RRU. If you are unable to cancel the RRU, PSMO-I will process the RRU. DSS will be processing the T5 PR inventory by oldest to newest prior to investigation package expiration. Also, the expiration date for e-QIPs in JPAS was increased from 90 days to 120 days. Therefore, e-QIPs will not expire until they reach negative (-30) 30 days. DSS will be monitoring expiration dates on all e-QIPs.

For new T5 PR Caveat requests, please include the following in the "Special Handling Instructions": 1) Statement indicating the e-QIP is in support of a caveat program (as identified in this new criteria), and 2) GCA contact information.

We encourage FSOs to regularly check the DSS website at www.dss.mil for this topic and other updates.

KNOWLEDGE CENTER HIGH CALL VOLUME

Due to the increased inventory, we are experiencing a high call volume and increased wait times. We appreciate your patience as we work down our inventory based on budget allocations

SF-86 QUALITY CONTROL

Please note that it is the responsibility of the FSO to review investigation packages (SF-86) for accuracy and completeness prior to submittal to DSS. The following are the top reasons the Office of Personnel Management will reject cases based on quality:

1. Fingerprints not be available (it is important that the electronic fingerprint submissions are made as close to the time of e-QIP submittal to DSS as possible);
2. Mailing addresses incomplete;
3. Background investigation items incomplete (cohabitant information, spouse SSN, unemployment/self-employment verification); and
4. Subject information discrepancies.

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) INTRODUCTION WEBINAR NOW ON-DEMAND

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. Go here for the introduction webinar (listed under January 24, 2017), and here to keep up on DISS updates.

DISS Portal (EX101.16) and DISS Hierarchy Management (EX100.16) shorts are both about 15 minute classes and are available on the Security Training, Education and Professionalization Portal (STEPP). Individuals must have a STEPP account in order to access these shorts. Once signed into STEPP, students can locate the shorts by entering "DISS" or the corresponding codes listed above into the STEPP search function.

DSS MAKES SECURITY CONTENT AUTOMATION PROTOCOL (SCAP) CONTENT AVAILABLE TO INDUSTRY WITHIN OBMS

The DSS National Industrial Security Program (NISP) Authorization Office (NAO) in collaboration with the Defense Information Systems Agency (DISA) and the Space and Naval Warfare Systems Command (SPAWAR) has made the SCAP Compliance Checker available to

industry via OBMS. Installation files for the SCAP Compliance Checker are posted in the "ODAA Bulletin Board" section of OBMS for all supported Operating Systems. For additional information, please view the updated SCAP Job Aid posted on the DSS RMF Website. Applying for sponsorship through MAX.gov is no longer necessary as all PKI-protected SCAP content is available within OBMS.

If you have questions or concerns, please contact your assigned Information Systems Security Professional (ISSP). If you encounter issues accessing the SCAP content on OBMS, contact DSS NAO via the mailbox at dss.quantico.dss-hq.mbx.odaa@mail.mil.

MEMORANDUM OF UNDERSTANDING TEMPLATE AVAILABLE IN OBMS

NAO provides a template for Memorandums of Understanding to facilitate connections between government and contractor systems. This template has the appropriate signature block and references, and will be the most up-to-date approved version. The template can be found in the ODAA Bulletin Board within OBMS, under "Headquarters Bulletin Board." Industry is not required to use the DSS template; however, doing so may expedite the coordination and approval process.

ELECTRONIC FACILITY CLEARANCE (e-FCL) NISP PSI DATA COLLECTION

DSS data collection of NISP Personnel Security Investigation (PSI) Projections will be opened on March 13, 2017 ending April 7, 2017 and can be accessed through the e-FCL system. DSS is responsible for projecting PSI requirements each year. Annual projections acquired from Industry through this collection are the key component in DoD program planning and budgeting for NISP security clearances.

Please note that submitting the PSI projections is independent of e-FCL package submissions; submitting information related to the facility clearance is not required as part of the PSI data collection.

A 12-minute tutorial video can be found here (under "Alerts") to assist in completing the PSI projections. For the best viewing of this video, hover your cursor over the link on the webpage, right-click and "save target as ...", so that you're saving the video to your computer. It can be viewed using Windows Media Player, QuickTime, and VLC Player.

We look forward to your participation. If you have any questions, please contact the PSI team at: dss.ncr.dss.mbx.psiprogram@mail.mil.

SECURITY EDUCATION AND TRAINING

THE CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE) RELEASES NEW INSIDER THREAT CASE STUDY

CDSE recently posted a new Insider Threat case study within the collection of Insider Threat job aids. The James Michael Wells case study is an example of a disgruntled employee who became an active shooter. Access the new and previously issued job aids here.

CYBER STANDARDS ADDED TO SPĒD ASSESSMENTS

The SPēD Certification Program was recently approved to include cyber standards in its Security Fundamentals Professional Certification (SFPC) and Security Asset Protection Professional Certification (SAPPC) assessments, and will implement these changes in late 2017. The Program will also update the SPēD Certification Program Candidate Handbook and Competency Preparatory Tools (CPTs) for each assessment to reflect these new standards. Stay tuned for additional news and updated resources!

CDSE FISCAL YEAR 2016 YEAR END REPORT NOW AVAILABLE

This past fiscal year has been busy for CDSE, from hitting over one million completions, to the launch of our Speaker Series. Check out the FY16 Year End Report to see all that was accomplished.

UPCOMING INDUSTRIAL SECURITY WEBINAR

Join CDSE on Thursday, March 2, 2017 at 11:30 a.m. or 1:30 p.m. Eastern Time for the "Conducting Effective Self-Inspections" webinar. This webinar will cover the importance of conducting thorough self-inspections and provides techniques a Facility Security Officer can use to validate the answers to questions asked throughout the Self-Inspection Handbook for NISP contractors. Sign up today!

SOCIAL MEDIA

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

Thanks,
ISR
Defense Security Service