DSS Monthly Newsletter
December 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.

SELF-INSPECTION CERTIFICATION FOR INDUSTRY

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 certify to DSS, on an annual basis, that a self-inspection has been completed in accordance with the provisions of NISPOM paragraph 1-207b. Beginning January 2017, contractors must complete this certification in Electronic Facility Clearance System (e-FCL). Additionally, contractors must make self-assessment reports available to DSS during security vulnerability assessments.

Starting January 3rd, the self-inspection certification function 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 e-FCL Submission Site User Guide (for Contractors), Section 6.2.

GUIDANCE FOR ITPSO RECORDS IN JPAS

Insider Threat Program Senior Officials (ITPSO) must be identified as Key Management Personnel (KMP) and must have eligibility equivalent or higher to the level of the Facility (Security) Clearance (FCL). Facilities must establish an owning relationship with the ITPSO's record in the Joint Personnel Adjudication System (JPAS).

In cases where a corporate-wide ITPSO has been appointed, each subsidiary (legal entity) must also identify the ITPSO as a KMP and must grant the ITPSO access to the level of the FCL. Subsidiary facilities must take an owning relationship with the ITPSO's record in JPAS.

Since a corporate-wide ITPSO is not required to be cleared in connection to the FCLs at branch/division locations, those facilities do not need to own the ITPSO's record in JPAS.

However, when the ITPSO requires access to classified information at branch/division locations, those facilities must take a servicing relationship with the ITPSO's record in JPAS and document the ITPSO's level of access to classified information.

REMINDER ON SUBMITTING eFINGERPRINTS

Electronic fingerprints should be submitted at the same time or just before an investigation request is released to DSS in JPAS. You can confirm National Background Investigation Bureau (NBIB) has processed the fingerprints by checking the Security/Suitability Investigations Index (SII) in JPAS which indicates a "SAC" closed. Fingerprint results are valid for 120 days, the same amount of time for which e-QIP signature pages are valid. Therefore, submitting electronic fingerprints at the same time or just before you complete your review for adequacy and completeness should prevent an investigation request from being rejected for missing fingerprints. A high level process flow outlining this and other personnel security clearance (PCL) activities associated with obtaining a security clearance for Industry is provided here for your ease of reference. Step #2 outlines the submission activities.

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.

OPTION #2 OF THE KNOWLEDGE CENTER CLOSED DECEMBER 30, 2016

Personnel Security inquiries (telephonic selection option #2) to include e-QIP authentication resets of the DSS Knowledge Center will be closed on Friday, December 30, 2016, for internal training to deliver the highest quality customer service to Industry and Government callers. Reminder, the PCL portion of the DSS Knowledge Center typically closes on the last Friday of each month. Normal Knowledge Center operations for PCL and e-QIP inquiries will resume on the first non-federal holiday business day following these closures.

RISK MANAGEMENT FRAMEWORK (RMF) HELPFUL HINTS

RMF is a new process for both Information Systems Security Professionals (ISSPs) and Information Systems Security Managers (ISSMs). In order to be successful, we must all familiarize ourselves with the Defense Security Service Assessment and Authorization Process Manual (DAAPM) and utilize available resources. The DSS Risk Management Framework Information and Resources webpage provides links to Policy/Guidance, Resources, Training, and Toolkits.

If you have questions or concerns, please contact your assigned ISSP.

SECURITY EDUCATION AND TRAINING

COUNTERINTELLIGENCE (CI) SPEAKER SERIES NOW AVAILABLE

Did you miss our recent Security Speaker Series with DSS CI Director William Stephens? If so, the webinar recording is now available in our archive. Watch and learn about the DSS CI mission to identify and articulate threats to U.S. technology and programs resident to industry.

NEW INFORMATION SYSTEM SECURITY MANAGER (ISSM) TOOLKIT

The Center for Development of Security Excellence (CDSE) is pleased to announce the release of the Information System Security Manager Toolkit, updated with new National Industrial Security Program (NISP) assessment and authorization (A&A) resources in accordance with RMF. This toolkit quickly points ISSMs to the resources they need to help them perform their role as an Information System Security Manager. Access the toolkit today!

REGISTER FOR NEXT "GETTING STARTED" SEMINAR

FSOs! Are you looking for a virtual training experience? The February 15-16, 2017 iteration of the "Getting Started Seminar for New FSOs" will be offered both in-person at our Linthicum, Maryland facility and a live, virtual session via Adobe Connect. This seminar contains two full days of security-related and counterintelligence awareness training. Register today!

NEXT CDSE SECURITY SPEAKER SERIES FEATURES DR. GALLAGHER

Join CDSE and our special guest Dr. Robert Gallagher, Defense Insider Threat Management and Analysis Center (DITMAC), on January 12, 2017, 12 p.m. Eastern Time for a discussion on the role of behavior analysis in Insider Threat Programs. Our live session will focus on the unique insight this discipline brings to insider threat detection and mitigation. Join us and be part of the conversation!

SOCIAL MEDIA

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

Thanks,
ISR
Defense Security Service