DSS Monthly Newsletter
November 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.

INSIDER THREAT IMPLEMENTATION

National Industrial Security Program Operating Manual (NISPOM) Change 2 promulgated on May 18, 2016 requires all cleared contractors under the National Industrial Security Program (NISP) to begin establishing the baseline requirements for an insider threat program. Your insider threat programs must be able to gather, integrate, and report relevant and available information indicative of a potential or an actual insider threat in accordance with NISPOM requirements. Additional resources and guidance on establishing your program may be found on DSS's Industry Insider Threat Information and Resources page and through the Center for Development of Security Excellence's (CDSE's) Insider Threat Toolkit. The Industry Insider Threat Information and Resources page also includes the balance of Change 2 requirements.

By November 30, 2016, you must accomplish the following:

- Establish your program;
- Appoint an Insider Threat Program Senior Official (ITPSO) who will finish ITPSO-specific training by November 30, 2016;
- Implement workforce training requirements related to insider threat; and
- Self-certify to DSS that your program can fulfill insider threat requirements.

RISK MANAGEMENT FRAMEWORK (RMF) TRANSITION/DEFENSE INFORMATION SYSTEM AGENCY (DISA) SCANNING TOOLS

For Information Systems (IS) authorized under RMF, DSS will conduct an assessment of the technical security controls and IS system configuration utilizing the DISA vulnerability scanning tools (Security Content Automation Protocol (SCAP) Compliance Checker (SCC) and DISA Secure Technical Implementation Guide (STIG) Viewer) in accordance with the NISP. The SCAP Compliance Checker, STIG Viewer, and applicable SCC content must be installed on the IS. If the IS cannot be assessed utilizing the specified scanning tools, please document the justification in the System Security Plan (SSP). The Getting Started with the SCAP Compliance Checker and STIG Viewer Job Aid is available on the DSS 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 Job Aid, please provide comments and questions to dss.quantico.dss-hq.mbx.odaa@mail.mil.

UPDATED RMF SYSTEM SECURITY PLAN

The NISP Authorizing Office (NAO) is excited to announce the upcoming release of an updated RMF SSP. The updated SSP will incorporate the feedback received from Industry. Our goal is to streamline both the SSP development and assessment process. The updated SSP will be released at the end of December 2016 and posted on the DSS RMF Website.

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

CLARIFICATION ON TYPE AUTHORIZATION

Under RMF, Self-Certification has been replaced with Type Authorization. Type Authorization means that "like" systems can be authorized under the same authorization package without going through the whole authorization process. This is similar to the self-certification process today. However, multiple Master System Security Plans (MSSPs) cannot be used to define "like" systems. The system must be "like" the system authorized in the MSSP. The Information Systems Security Manager (ISSM) may add “like” systems to the MSSP **AFTER** the Authorizing Official (AO) has determined that the ISSM has the requisite knowledge and skills to manage multiple IS under one MSSP. If Type Authorization authority is granted, it will be documented in the Authorization to Operate (ATO).

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

PROPOSAL SYSTEMS

As the transition to RMF continues, it is imperative that we change our approach with Assessment & Authorization (formally Certification & Accreditation). ISSMs should be meeting with their Program Manager (PM)/Information System Owner (ISO) and Government Contracting Authority (GCA)/Information Owner (IO) and discussing the transition to RMF. Under RMF, DSS will no longer have the ability to react to last minute requests. There is a defined process and we must follow it. Concerns have been raised regarding the authorization turnaround time for an IS supporting a Request for a Classified Proposal and the ability to respond in a timely manner. Options are available that will accommodate the needs of Industry and allow NAO to maintain appropriate oversight.

- Since the majority of Proposal Systems are stand-alone systems with the Categorization of Moderate-Low-Low, the ISSMs can take proactive measures utilizing the DSS Overlays and DISA Scanning Tools to prepare the SSP and configure the IS.
- The AO has the authority to issue an Interim Authorization to Operate (IATO) for a limited period of time with the option to waive the on-site validation. If the AO does not

concur with waiving the on-site validation, the on-site may still be required. The AO will make that determination.

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

RISK MANAGEMENT FRAMEWORK HELPFUL HINTS

RMF is a new process for both ISSPs and 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. In addition, helpful information can also be accessed at the RMF Knowledge Service Webpage.

KNOWLEDGE CENTER MONTHLY SHUTDOWN

As a reminder, Personnel Security inquiries to include e-QIP (option #2) of the DSS Knowledge Center closes the last business day of each month for the purpose of conducting internal training to deliver the highest quality customer service to Industry and Government callers. Please note, we will be closed on Friday, November 25, for this month only, and will reopen Monday, November 28. Please check the DSS website for the latest news and updates, go to www.dss.mil and click "News." Please also note that the menu options for personnel security clearance inquiries will be changing in the near future.

JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS) REMINDERS

Remember, credential sharing constitutes a misuse of JPAS. There has been a recent spike in credential sharing incidents within Industry. Additionally, Facebook and other social media are inappropriate venues to discuss and request JPAS access and records.

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS)

The Defense Information System for Security is set to deploy for Industry on March 27, 2017 and will replace JPAS once DISS reaches full operating capability. DISS will reform DoD Security and Suitability processes to improve timeliness, reciprocity, quality, and cost efficiencies through the design and implementation of a secure, end-to-end information technology system. The system will electronically collect, review, and share relevant personnel data government-wide, as mandated by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) and guided by relevant Executive Orders, Congress, and Government Accounting Office recommendations. Human Resource and Security Managers world-wide will be accessing DISS to review eligibility for access to classified materials and facilities, suitability for employment, and/or issuance of a Personal Identity Verification or a DoD Common Access Card to gain physical and logical access to DoD installations and IT resources.

REMINDER: STREET ADDRESS INFORMATION OF SF-86

PSMO-I is seeing an increase in rejections by National Background Investigative Bureau (NBIB) for incomplete street address information. Part of the SF-86 review to determine adequacy and completeness of necessary information includes valid/complete street addresses. Please also ensure the Requesting Official and their contact information is accurate as PSMO-I/NBIB may attempt to obtain information prior to determining that the request is unacceptable.

ASKPSMO-I@DSS.MIL DISCONTINUED

Effective immediately, PSMO-I will cease all outgoing communication through the AskPSMO-I email address. In the future, the email address will only be used to receive documentation when requested by PSMO-I. All inquiries should be directed to the DSS Knowledge Center at 888-282-7682, option #2.

SECURITY EDUCATION AND TRAINING

FACILITY SECURITY OFFICER (FSO) VIRTUAL ASSESSMENT

Are you a new or experienced FSO looking to test your knowledge?

If the answer is "yes," register for the "FSO Virtual Assessment!" In this virtual training, users navigate through "a day in the life" of an FSO and test their knowledge. Completing this training ensures that users have assessed their ability to respond to the various security scenarios within the virtual environment. Students must receive a grade of 75 or higher to receive credit for completing this assessment; however, this grade will NOT appear on the student's transcript.

Go here to check out the FSO Virtual Assessment.

COUNTERINTELLIGENCE WEBINAR NOW AVAILABLE

Did you miss our recent "DSS 2016 Targeting U.S. Technologies" webinar? No worries, the webinar recording is now available in our archive. Watch the webinar and learn about the latest trends in foreign targeting of U.S. defense technologies.

UPCOMING DECEMBER INDUSTRIAL SECURITY AND CYBERSECURITY WEBINARS

CDSE invites you to participate in the following live webinars:

Industrial Security
"Understanding your eFCL Submissions"
Thursday, December 8, 2016
11:30 a.m. Eastern Time
2:30 p.m. Eastern Time

This webinar will assist you in understanding your organization's business documents and the substantiating materials required in your Initial and subsequent Changed Condition electronic-Facility Security Clearance (e-FCL) submissions to DSS.

Cybersecurity
"Assessment and Remediation using the SCAP Tool and POA&M Template"
Thursday, December 15, 2016
1:00 p.m. Eastern Time

This webinar will assist the user in developing Assessment and Authorization packages using the SCAP and the Plan of Action and Milestones (POA&M) template.

Visit our webinar page to sign up 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, 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