DSS Monthly Newsletter
October 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.

UPDATE ON INDUSTRY INSIDER THREAT IMPLEMENTATION

On October 20, 2016, DSS posted an update to "Industry Information and Resources - Notices". Click here for the update.

NEW CHANGE CONDITIONS REPORTING JOB AID

We are excited to announce that a Change Conditions Reporting Job Aid was published on October 19, 2016. This Job Aid provides guidance for reporting change conditions in accordance with NISPOM 1-302g. It includes examples of what to report, how to report, and required supporting documentation. It is posted to the FSO Toolkit "Reporting" section, and is available in e-FCL when completing a Change Condition package.

If you have questions on a specific Change Condition, contact your assigned Industrial Security Representative. If you have specific questions about the format or content of the Job Aid, please provide comments and questions to DSS.NISS@mail.mil.

RISK MANAGEMENT FRAMEWORK (RMF) TRANSITION FOR STAND-ALONE SYSTEMS[1]

On Monday October 3, 2016, DSS began the transition to RMF for authorization of classified systems under the NISP. The first phase of the transition is limited to stand-alone systems, either Single User Stand-Alone (SUSA) or Multi-User Stand-Alone (MUSA) systems. All new and existing stand-alone systems which require re-authorization must be submitted to DSS using the RMF process, templates and security controls. Systems previously accredited under the Certification and Accreditation (C&A) process may continue to operate through the expiration

[1] A stand-alone information system (IS) is a single desktop or similar component. It is not connected to any other system or Local Area Network (LAN), has no network interface card (NIC) or protected distribution system (PDS) in place. *Source: DSS Assessment and Authorization Process Manual (DAAPM)*

date listed on the Approval To Operate (ATO) letter. However, a security-relevant change to the stand-alone system would require re-authorization under RMF.

DSS has posted a new "Getting Started with Risk Management Framework" guide to the existing NISP Risk Management Framework Resource Center located on the DSS Home Page. Additional information, training, templates, job aids and configuration guides are already available and located on the Resource Center here. Contact your assigned Information Systems Security Professional (ISSP) or local Field Office if you have questions.

KNOWLEDGE CENTER TEMPORARILY UNAVAILABLE

Personnel security inquiries to include e-QIP (option #2) of the DSS Knowledge Center will be unavailable on Monday, October 31, 2016, but will resume normal business hours on Tuesday, November 1st.

INTERNATIONAL OUTGOING FOREIGN VISIT SUBMISSIONS

At this time the dss.rfv@mail.mil email is unable to accept or access encrypted emails. To email the international visit paperwork, please password-encrypt the PDF, and send the password in a separate email. If you choose this method, after digitally signing the request, please print and scan the request prior to password protecting the file. If you prefer, you can still fax your visit request to 571-305-6010.

REMINDER ON IDENTIFYING THE GOVERNMENT CUSTOMER FOR PERSONNEL CLEARANCE (PCL) INVESTIGATIONS

DSS requests assistance in assuring that all of your requests for personnel security investigations (PSIs) in the Joint Personnel Adjudication System (JPAS) identify the government customer in the contract number field when requesting PCLs. Accurately identifying the source of the investigative requirement is essential to effectively manage and validate PSI submissions. We have provided guidance here.

DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS) PORTAL AND DISS HIERARCHY MANAGEMENT SHORTS

DISS Portal (EX101.16) and DISS Hierarchy Management (EX100.16) shorts are now available on the Security Training, Education and Professionalization Portal (STEPP). Individuals must have or create 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. For questions, contact CDSE.

IMPLEMENTATION OF TIER 5 FEDERAL INVESTIGATIVE STANDARDS

In December 2012, the Office of the Director of National Intelligence (ODNI) and Office of Personnel Management (OPM) jointly issued revised federal investigative standards on the conduct of background investigations for individuals that work for, or on behalf of, the federal

government in order to bring consistency to investigative quality expectations. Effective on October 1, 2016, the Tier 5 investigation was implemented as part of the phased approach for implementation of the federal investigative standards. As a result, the Single Scope Background Investigation (SSBI) has been replaced with the Tier 5 investigation when Top Secret and SCI access to classified information are required.

Starting October 1, 2016, users may have noticed the Tier 5 investigations versus SSBI when reviewing investigative information in JPAS. For example, an investigation line may appear as "T5 From OPM, . . ." vice "SSBI From OPM, . . ."

Periodic Reinvestigation will be designated as "T5R" to represent Tier 5 Reinvestigation, instead of “SBPR.”

REMINDER ABOUT SUBMITTING ELECTRONIC FINGERPRINTS

As of October 1, 2016, all fingerprints associated with SON 346W must be submitted electronically to the Office of Personnel Management, or the fingerprint will be rejected. OPM will also reject any investigation request if an electronic fingerprint is not received within 14 days of request submission. Click here to view the electronic fingerprint capture options for Industry.

DEFENSE INTELLIGENCE AGENCY (DIA) UPDATE

On February 10, 2016, the Deputy Secretary of Defense signed an Action Memo that directed the transfer of the DoD SCI adjudicative mission from the DIA Central Adjudication Facility to the DoD Consolidated Adjudication Facility. The agreed Initial Operational Capability date for this transfer was July 1, 2016. For more information about the transfer, submit your questions to 4thestatetransinfo@dodiis.mil. For all other inquiries, email DIActrAdjudications@dodiis.mil. Answers to frequently asked questions regarding DIA conducting SCI determinations can be found here. Refer to question #25.

INVESTIGATIONS FOR OTHER THAN ACCESS TO CLASSIFIED INFORMATION

The processing of investigations for purposes other than access to classified information related to a classified contract is the responsibility of the government contracting activity (GCA). When the GCA requests that contractors process investigations which do not require access to classified information, contractors are to advise their customer that they cannot process those investigations through DSS. Examples of investigations for other than access to classified information include, but are not limited to: base access, suitability for logical access to unclassified information systems, positions of trust, and unclassified information systems administrator access (IT Levels). The GCA is responsible for funding, submitting, and managing these types of investigations which are outside the National Industrial Security Program.

SECURITY EDUCATION AND TRAINING

NEW CYBERSECURITY WEBINAR NOW AVAILABLE

In support of National Cybersecurity Awareness Month, the Center for Development for Security Excellence (CDSE) is proud to announce the release of the three new Cybersecurity products:

- Webinar - "Greater Security in 7 Days" which focuses on what you can do to stay safer online. Access the webinar here.
- Webinar – "Online Scams and Fraud" which discusses hot topics and trends affecting everyone with an internet connection. The webinar will highlight the top current threats and ways to avoid becoming a victim. Access the webinar here.
- Video Lesson – "Social Media" which highlights the risks associated with social media and how to use social media responsibly and effectively in official and unofficial capacities. Access the video lesson here.

CDSE COURSES APPROVED FOR COMPTIA CONTINUING EDUCATION UNITS (CEUs)

CDSE is excited to announce that more than 40 of the security courses and curricula hosted on our website have been approved for CEUs from CompTIA. CDSE courses can now be applied as CEUs in maintaining the following CompTIA certifications:

- A +
- Network +
- Security +
- CompTIA Advanced Security Practitioner (CASP)

View a complete listing of eligible CDSE courses here. Other CDSE cybersecurity offerings are found here.

NEW INDUSTRIAL SECURITY SHORT

CDSE recently launched a new Security Short, "Managing Electronic Classified Information." This short provides a refresher on handling classified information (especially in the electronic environment) including marking, retrievability, accountability, destruction, and retention of electronic classified information. Access the short here.

NEW SPECIAL ACCESS PROGRAM (SAP) JOB AID NOW AVAILABLE

CDSE has released a new job aid on the responsibilities and procedures for the SAP Nomination Process (SAPNP). It is suitable for viewing online and can also be printed as a handy desk reference. Access the job aid at the SAP Job Aids page or the "Determining SAP Access Eligibility" page.

RETIREMENT OF CDSE JPAS/ JCAVS VIRTUAL TRAINING FOR SECURITY PROFESSIONALS COURSE

On November 1, CDSE will no longer offer the JPAS/Joint Clearance and Access Verification System (JCAVS) Virtual Training for Security Professionals course (PS123.16). As a result, students will not be able to register for, access, or complete the course and exam after October 31, 2016. Alternate CDSE JPAS training courses are listed below:

- JCAVS User Level 7 & 8: PS181.16
- JCAVS User Level 10: PS182.16
- JCAVS User Levels 2 thru 6: PS183.16

Please visit Defense Manpower Datacenter's (DMDC's) JPAS webpage (click on account manager policy) for information regarding DMDC JPAS account training requirements after October 31.

INSIDER THREAT SYMPOSIUM

Did you miss our recent Insider Threat Symposium? No worries, the webinar recording is now available in our archive. Watch the webinar and learn about the requirements, available tools, and resources provided by DSS to help our industry partners implement NISPOM Change 2.

NEW REGISTRAR REQUEST FORM WILL LAUNCH NOVEMBER 1, 2016

Do you have an issue using STEPP and need the CDSE Registrar's assistance?

On November 1, 2016, the CDSE Registrar's Office will launch the new Registrar Request form to help us serve you better. It's easy to access from our website and will only take a few seconds to complete. Requests via email will no longer be processed.

NEXT CDSE SECURITY SPEAKER SERIES FEATURES DSS CI DIRECTOR STEPHENS

CDSE will host a Security Speaker Series webinar on November 10, 2016 featuring DSS Counterintelligence Director William Stephens. The webinar is intended for an audience of Department of Defense DoD enterprise and industry partner security personnel. Sign up today!

SEATS AVAILABLE FOR UPCOMING "SAP MID-LEVEL SECURITY MANAGEMENT" COURSE

CDSE's "SAP Mid-Level Security Management" course will be held in Linthicum, Md., from December 5 to 9, 2016. If interested, complete the required prerequisites and register for this class (via STEPP) no later than November 2, 2016.

This course focuses on the student's ability to determine enhanced security requirements based on the threat and vulnerability of Special Access Programs. Students will review, revise, or write

security-related supporting documentation such as treaty, physical security, and transportation plans.

The course requires SAP Central Office (SAPCO) approval to attend. To review the course prerequisites and to register, go here. Should you have any questions regarding this course, please email dss.sapsecuritytraining@mail.mil

SOCIAL MEDIA

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

Thanks,
ISR
Defense Security Service