DSS Monthly Newsletter

April 2015

(Sent on behalf of ISR)

Dear FSO,

This is the monthly email 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.

DSS Releases ISL 2015-01 to Add Millennium Challenge Corporation (MCC) to NISPOM Paragraph 1-103b, Agency Agreements). DSS releases ISL 2015-01, updating the list of Federal agencies that have entered into an agreement with DoD for Industrial Security services. The ISL can be accessed at http://www.dss.mil/documents/isp/ISL2015-01.pdf.

March 13, 2015

Directive-type Memorandum (DTM) 15-002, "Policy Guidance for the Processing of National Interest Determinations (NIDs) in Connection with Foreign Ownership, Control, or Influence (FOCI)" was promulgated and effective on February 11, 2015. The DTM provides guidance to the Government Contracting Activities (GCAs) within the DoD Components about the industrial security procedures and practices related to NIDs and the role of DSS proposing NIDs on behalf of the GCAs if the U.S. contractor requires access to proscribed information under a special security agreement (SSA). The NISPOM (DoD 5220.22-M) continues to provide guidance to NISP contractors about actions and issues related to FOCI and NIDs. The DTM can be accessed at http://www.dtic.mil/whs/directives/corres/pdf/DTM15002.pdf.

ATTENTION JPAS/SWFT/ISFD SYSTEM ACCESS APPLICANTS - SYSTEM ACCESS REQUEST (SAR) PROCESS Please see http://www.dss.mil/about_dss/news/20110818.html for important information pertaining to the JPAS/SWFT/ISFD system access request processes. Thank you!

JPAS Account Maintenance:

According to DMDC, JPAS account holders are prohibited from looking up their own record in JPAS. DMDC is conducting account auditing. See DMDC JPAS website for more information.

Be sure to logon to JPAS daily. REMINDER: JPAS accounts are inactivated after 30 days of no activity and are terminated at 45 days.

Announcing the next PSMO-I Webinar
Topic: OPM Updates
Date: Tuesday, April 28, 2015
Time: 1:30 p.m. EST
To register and submit questions, visit
http://www.dss.mil/psmo-i/indus_psmo-i_webinars.html.

March 12, 2015

The protection of the national security starts with the RIGHT clearance and RIGHT access. To protect our national interest, all DoD employees and contractors, along with our Industry partners are responsible for data quality of the DoD Personnel Security System of Record – JPAS -- that serves our country with the right information, at the right time, to the right people, for the right decisions.

Defense Manpower Data Center's (DMDC) overall mission is to provide a secure Department of Defense system of record for personnel security that performs comprehensive management for the entire DoD community including DoD Industry partners. In order to effectively manage DoD personnel security clearances, JPAS must maintain accurate PII and current eligibility throughout the entire database.

While implementing the guidance from the DoD Privacy Program, DoD 5200.11-R (May 4, 2007), regulation at C1.2 through C1.2.2 (Standard of Accuracy) and DoD personnel security polices, DMDC generates monthly users' audit reports and as a result, has identified several trends that pose potential risk to the DoD personnel security program. The main three trends are Incorrect Legal Name, Test or Fake SSNs, and Viewing One's Own Record.

-----Incorrect Legal Name----- The DoD Privacy Act Regulation requires the use of a legal name in JPAS. In reviewing the data, it appears that many names in JPAS are nicknames and not the legal name (e.g., Bob vs Robert, Mary vs Maryann) as written on a subject's SSN and/or passport. Please review all JPAS person's information to ensure the name is the legal in JPAS. If it is not accurate, please update the name per the JPAS Data Correction Checklist and use proper syntax for JVS Data migration (click link for Proper Syntax). This could mean that the subject needs to go to their personnel center, PDR, or security office. *Non-compliance could result in users' account being locked until their legal name is corrected.*

-----Inserting, Using or Testing Fake Social Security Numbers----- As part of the JVS Data Migration, DMDC audited users who were inputting or using test or dummy SSNs in order to clean up the database prior to migration. Department of Defense Regulations and Defense Manpower Data Center (DMDC) Joint Personnel Adjudication System (JPAS) Account Management policies that prohibits users from entering or using false or inaccurate information including, entering test or "dummy" personal

information into the Department of Defense (DoD) personnel security system of records. JPAS is a fully audited database that reflects anytime a user selects, add, modifies, or delete anything in JPAS.

-----Look Up or View Your Own Record----- As part of the JPAS user monthly audit, JPAS systematically audits the database for various misuses to include users who query and/or look up their own records by viewing their Person Summary screen in JCAVS or selected themselves in JAMS. The DMDC JPAS Account Management Policy states that all users consent to the terms of use of the DoD System of Records and agree to comply with the Privacy Act of 1974, applicable DoD regulations, other applicable laws, and JPAS policies. The Account Management policy prohibits users from querying and/or looking up their own records into the Department of Defense (DoD) personnel security system of records, this a DoD Privacy violation and constitutes a misuse of JPAS.

YOUR WINS IN COUNTERING THE CYBER THREAT

Several of you recently reported discovering evidence of intrusions on your company unclassified information systems associated with possible Foreign Intelligence Entities (FIE). These discoveries came when your company applied the cyber threat indicators we sent to you and to your information security manager (ISM)[1] in our last Cyber Threat Alert (CTA). We select the CTA-included indicators based on their level of association with threat sources related to FIE, nature of use, capability, and lifespan.

Your FIRST find of intruder presence occurred within HOURS of the CTA release! Each such discovery and remedy is:

- A win against cyber threats that want to stay hidden while they compromise information on your networks
- Greater assurance the US keeps its national security advantage, and your national security products and programs get closer to being delivered uncompromised
- A reminder and call to report cyber incidents under the NISPOM

How did YOUR Company do in applying the CTA?

Knowing what you find IS CRITICAL to DSS in evaluating and countering the threat. This information drives changes to countermeasures and indicators, and becomes CRITICAL to you and other cleared contractors in improving your cyber threat detection and protection and minimizing your company's intellectual property and profit loss Be careful not to presume you're safe if your systems at first do not detect the indicator. The attacker may have not yet targeted the system, may have erased the indicator or the path to it, or may have hidden it or put it to sleep for later use. So, a good practice is to keep the system alert for the indicator or periodically check the system for it, and setup a cutoff point to move it to inactive.
For reporting of cyber incidents, follow the NISPOM and the requirements found in ISL 2013-05, *Applicability of National Industrial Security Program Operating Manual (NISPOM) Paragraph 1-301*

Reporting Requirements to Cyber Intrusions, . Where you believe the possible FIE actor is or has been in your information system, drop a copy of the unclassified reporting to DSSCYBERCI@dss.mil.
For more information, check with your supporting DSS Counterintelligence (CI) Special Agent (CISA) or Industrial Security Representative (ISR).

[1] The CTA was sent to ISMs for whom we have contact information. To add your ISM to the distribution list, send their name, position, and contact information, followed by a company email they have digitally signed using the DoD-approved External Certificate Authority (ECA) certificate, to DSSCYBERCI@dss.mil. If you are not receiving the CTA via encrypted email, send a company email likewise signed to that same address with your contact and position information and CAGE code.

SECURITY EDUCATION AND TRAINING

SOUTHERN REGION GETTING STARTED SEMINAR FOR NEW FSOs (IS121.01)

The details for our southern region iterations of the "Getting Started Seminar for New FSOs" have been finalized. See dates and locations below:

- May 4 – 5, 2015: Lockheed Martin, Orlando, FL
- May 13 – 14, 2015: Georgia Tech University, Atlanta, GA

Space is limited so make sure to reserve your seat today!

For full details and to register for any of these classes, go to:
http://www.cdse.edu/catalog/classroom/IS121.html.

APRIL INDUSTRIAL SECURITY WEBINAR

The Certification and Accreditation (C&A) process is an integral part of Information Systems Security Manager (ISSM) responsibilities. This presentation discusses the process as it relates to industry, as well as how to maintain the accredited security posture throughout the system lifecycle.

To sign up for this webinar, go to http://www.cdse.edu/catalog/webinars/index.html and select the time you would like to attend.

CDSE DEVELOPS ITAR/EAR DESKTOP REFERENCE

As part of our Counterintelligence Awareness Job Aid Series, CDSE is pleased to introduce the International Traffic in Arms Regulation (ITAR) and Export Administration Regulation (EAR) Desktop Reference. The ITAR/EAR Desktop Reference was developed in order to provide the

best counterintelligence awareness training for the DoD enterprise and cleared defense contractor security communities. This job aid will foster a better understanding of the regulations, their application, and consequences of violations.

The loss of U.S. defense technology continues to undermine the U.S. economy and military capability. ITAR and EAR regulated items within cleared industry are a prime target of many foreign intelligence collectors and foreign government economic competitors. Many of the suspicious contact reports received by the DSS involve the illegal transfer of these items. CDSE recognizes the crucial role that both ITAR and EAR compliance play in national security. The new job aid provides a one-stop shop for numerous resources including policy and guidance, database access, case summaries, and frequently asked questions

Visit the CDSE Catalog's Counterintelligence Resource page to access the ITAR/EAR Desktop Reference: http://www.cdse.edu/resources/resources-ci.html.

SPēD Competency Preparatory Tools

Wonder how your knowledge and experience match up to the competencies evaluated in the Security Professional Education and Development (SPēD) Certification assessments?

The Competency Preparatory Tools (CPTs) are an online suite of resources that provide candidates with the means to gauge their experience in and knowledge of the security competencies against those tested in the SPēD Certification assessments.

The CPTs have three components: The Experience Checklist, the Knowledge Test, and the Sample Test. Also available are the Areas of Expertise, which consist of policies and available resources for further study.

Knowledge Tests for Industrial Security Oversight Certification (ISOC) and Physical Security Certification (PSC) were recently added, with additional resource development currently underway.

CPTs for each assessment are available at no cost at http://www.cdse.edu/certification/prepare.html.

Special Program Security Certification Now Available

The Special Program Security Certification (SPSC) assessment, a new specialty certification in the Security Professional Education Development (SPēD) Certification Program, is now online and available for government and industry security professionals.

The SPSC measures candidates' knowledge on such competencies as: classification management, information assurance, information security, personnel security, physical security, program security, the fundamentals of special access programs, and vulnerability assessments.

This certification is ideal for the Department of Defense (DoD) and other U.S. government personnel (civilian and military) and contractors who will be or are already performing Security Officer functions for and/or on behalf of DoD Special Access Programs. Candidates must be conferred the Security Fundamentals Professional Certification (SFPC) before taking the SPSC assessment.

For more information on the SPSC and other SPēD certifications, visit the DSS website: http://www.cdse.edu/certification/sped_what.html.

Connect with CDSE for your training and certification solutions!

- www.cdse.edu
- Twitter @TheCDSE
- Facebook https://www.facebook.com/TheCDSE
- YouTube https://www.youtube.com/user/dsscdse#p/u for 24/7 access to Webinars, Shorts, and more.

Thanks,
ISR
Defense Security Service