DSS Monthly Newsletter
May 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.

CRIMINAL AND TERRORIST THREATS RELATED TO SOCIAL MEDIA

The Department of Defense (DoD) has recently noted several incidents where criminal or terrorist organizations are actively targeting military and cleared defense contractor employees for their type of skill set and associations to certain sensitive government or military programs. These criminal and terrorist organizations are using individuals' Facebook and LinkedIn accounts and open source research to acquire personal information for the individuals working on these programs to include names, addresses, and personally identifiable information (PII) to specifically target them and their families.

Government, military, and cleared industry personnel should take the necessary steps towards the responsible use of social media accounts and practice good Operations Security (OPSEC) when using social media sites. The DoD Identity Awareness, Protection, and Management Guide provides procedures and information on securing social media accounts. The Center for the Development of Security Excellence (CDSE) provides information to inform the responsible use of Social Media through its Cybersecurity Toolkit. In addition, Security Officers need to ensure personnel are provided general safety information and OPSEC to their workforce. CDSE also offers the OPSEC Awareness for Military Members, DoD Employees and Contractors Course which provides information on the basic need to protect unclassified information about operations and personal information.

DOD RELEASES CHANGE 2 DoD 5220.22-M FOR INSIDER THREAT

On May 18, 2016, the Department of Defense approved Change 2 to DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM). The change includes requirements for contractors to implement an insider threat program, adds reporting requirements for Cleared Defense Contractors (CDC) relative to cyber incidents on CDC information systems approved to process classified information and can include activities occurring on unclassified information systems, and addresses alignment with Federal standards for classified information systems. The release incorporates and cancels NISPOM Supplement 1.

- Change 2 to DoD 5220.22-M can be found here.
- A Summary of Changes can be found here.

In order to keep industry updated, DSS's website will soon host an Insider Threat webpage under "Most Requested Links" for program implementation information. The webpage, "Industry Insider Threat Information and Resources," will provide information, tools, training, and resources for implementing your Insider Threat programs.

OFFICE OF THE DESIGNATED APPROVING AUTHORITY (ODAA) NAME CHANGE

Due to DoD's implementation of Risk Management Framework, the term "Approving Authority" is obsolete, and shall be replaced with "Authorizing Official." As a result, ODAA will change its name to the NISP Authorization Office (NAO), and "Regional Designated Approving Authority" will become Regional "Authorizing Official" (AO). DSS has not released official notice of the name change—this information is only provided to put the following paragraph into the proper context.

PROTECTED DISTRIBUTION SYSTEM (PDS) TRANSITION GUIDANCE

Cleared contractors are required to have compliant PDS by September 30, 2018 in accordance with the Committee on National Security Systems Instruction (CNSSI) 7003 dated September 2015 (available here). In an effort to transition from old guidance to new, cleared contractors should work with their assigned Information Systems Security Professional (ISSP) to assess their existing PDS configuration against the CNSSI 7003 requirements. A PDS Plan of Action and Milestones (POA&M) needs to be created to document when non-compliant PDS will be remediated prior to the September 30, 2018 deadline. This POA&M must be submitted to the NISP Authorization Office (NAO) (formerly ODAA) mailbox, *dss.quantico.dss-hq.mbx.odaa@mail.mil* by September 30, 2016. Please include your assigned Information Systems Security Professional (ISSP) and Industrial Security Representative (ISR) on the email submission.

The CNSSI 7003 also requires the approval of PDS by the DSS Regional Authorizing Official (AO) (formerly the RDAA). Effective immediately, all PDS Installation Plans will be submitted to the NAO mailbox noted above. Once the plan has been reviewed and validated by the ISSP, the RAO will sign and forward an approval letter to the originator. As a note, the Facility PDS Installation Plan is approved separately from the Information System Authorizations (formerly Certification and Authorization process). Once approved, the PDS Installation Plan and approval letter would then be uploaded into OBMS for each system Unique Identifier (UID) (that uses the PDS), as a supporting artifact to a System Security Plan (SSP). Previously approved PDS are authorized to continue in support of information systems (IS). However, any PDS that is not currently compliant could affect the expiration dates of Approvals to Operate (not to exceed September 30, 2018) for new or revised information systems. Please consult with your ISSP for questions concerning PDS.

PDS Guidance will be included in the upcoming promulgation of the DSS Assessments & Authorization Process Manual (DAAPM) (formerly the ODAA Process Manual).

AFFILIATED OPERATIONS PLAN (AOP) GUIDE RELEASED

In response to Industry feedback, the Business Analysis and Mitigation Strategy Division has published *Navigating the Affiliated Operations Plan: A Guide for Industry*" to assist companies with mitigating and managing affiliated operations per their Foreign Ownership, Control, or Influence (FOCI) mitigation agreements. The guide explains how companies can prepare, submit, and comply with their own AOP, and offers best practices on every step involved in the AOP process. The AOP Guide can be found here.

SECURITY EDUCATION AND TRAINING

SECURITY AWARENESS HUB (FORMERLY KNOWN AS OPEN ELEARNING)

The Center for Development of Security Excellence (CDSE) announces, the new "Security Awareness Hub" website formerly known as "Open eLearning." The new and improved site offers quick and easy access to security awareness courses with no registration requirements. Please note that while certificates are provided to document completion of a course, CDSE does not maintain individual records of course completion for these online offerings. The courses are provided for individuals who need to fulfill security awareness requirements as directed by their organization, or who simply want to improve their security awareness but do not require transcripts. Take a course now!

NEW CYBERSECURITY SMART CARDS

CDSE has released four new Cybersecurity Smart cards for Facebook and Twitter. These Smart card job aids describe the recommended and optional security settings, as well as general social media security concepts. Access the cybersecurity job aids here.

CDSE RECEIVES "DISTINGUISHED AGENCY" AWARD

CDSE was recognized in the 2015 Horizon Interactive Awards competition as a Distinguished Agency, which is a title given to agencies and developers who consistently demonstrate high quality work. The Horizon Interactive Awards competition, now in its 14th season, is one of the most prestigious awards in the field of interactive and creative media. Since 2009, CDSE has won a total of 43 Horizon Interactive Awards. View CDSE's award winning products here.

NEW COUNTERINTELLIGENCE AWARENESS VIDEO.

Want to improve your National Security posture in less than four minutes? Watch and learn how counterintelligence supports security efforts by identifying threats and helping you to develop and deploy effective countermeasures. The video is a great way to kick off an awareness briefing or a monthly security newsletter. Find it here.

NEW INSIDER THREAT CASE STUDIES

Robert Mo - http://go.usa.gov/cuVQh
Charles Eccleston - http://go.usa.gov/cuwnH

These job aids reinforce the adverse effects of the Insider Threat and are suitable for printing or easy placement in a company or command newsletter, email, or training bulletin. CDSE issues two new case studies per quarter, so check back often.

UPCOMING CDSE SPEAKER SERIES WEBINAR: INTERVIEW WITH THE DIRECTOR OF INDUSTRIAL SECURITY FIELD OPERATIONS (IO), MAY 26, 2016

On Thursday, May 26, 2016 from 1:00 pm- 2:00 pm EST, CDSE is pleased to host Mr. Gus Greene, Director of IO for the DSS as part of our Security Speaker Series. The CDSE Security Speaker Series delivers live, one-on-one interviews with knowledgeable, respected leaders in the security community. Speakers discuss trending topic areas such as insider threat, personnel security investigations, counterintelligence, and more. Conversation is driven by hot topics and the audience may ask questions.

Join us and find out more about Industrial Security and the critical role DSS serves in Industrial Security oversight. Register for this Adobe Connect online virtual event here.

UPCOMING CDSE SPEAKER SERIES WEBINAR: ECONOMIC ESPIONAGE, JUNE 30, 2016

CDSE is pleased to host Acting Chief John Hartnett of the Federal Bureau of Investigation Economic Espionage Unit for a live discussion on the national security implications of Economic Espionage. Register here.

ARCHIVED WEBINARS AVAILABLE

Did you miss the “CDSE Cybersecurity Products and Resources” or the “Developing an Incident Response Capability” webinar? No problem! They are now available for your viewing. You can access both webinars and more in our archives.

REGISTER NOW FOR UPCOMING INDUSTRIAL SECURITY TRAINING

Seats are still available for the following CDSE class:

"Getting Started Seminar for New FSOs," June 6 & 10, 2016 (Nashville, TN):

Please note the two-day "Getting Started Seminar for New FSOs" training course in Nashville will be delivered in conjunction with the 2016 NCMS Annual Seminar, and will be presented in a split schedule. Day one of the course will be on Monday, June 6 and day two will be on Friday, June 10, 2016. This will give you the opportunity to attend both the CDSE training and the NCMS Annual Seminar. It is required that you attend on both Monday and Friday in order to receive a CDSE course completion certificate.

CYBERSECURITY WEBINAR: RISK MANAGEMENT FRAMEWORK (RMF) FOR INDUSTRY JUNE 15, 2016

CDSE is pleased to host Ms. Tracy Brown, Sr. ISSP, National Industrial Security Program (NISP) Authorizing Office (NAO)—formally the ODAA—for a live webinar on the NISP transition to RMF. This webinar will walk through an overview of the RMF process, roles and responsibilities and the program's accompanying benefits. Register for the webinar here.

Thanks,
ISR
Defense Security Service