



DSS Monthly Newsletter
June 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 WEBPAGE

In the May VOI Newsletter, DSS advised industry that we would be hosting a dedicated Insider Threat webpage on dss.mil. The "Industry Insider Threat Information and Resources" webpage has been established and is located [here](#). The webpage has links to information, tools, training, and resources to assist industry in implementing an insider threat program as required by NISPOM Change 2.

RISK MANAGEMENT FRAMEWORK (RMF) UPDATE

To assist NISP companies and agencies with the transition to RMF, DSS has created the [NISP RMF Resource Center](#). The site provides policy, resources, training and toolkits. A few items are listed for release in the next three months so continue to check in on the RMF Resource Center.

This information is also available on the [NCMS website](#), [Twitter](#) and [Facebook](#).

**PARTNERSHIP WITH THE DEPARTMENT OF COMMERCE ON
SURVEY OF CLEARED INDUSTRY**

The U.S. Department of Commerce, Bureau of Industry and Security (BIS), Office of Technology Evaluation (OTE), in coordination with DSS is conducting a survey and assessment of organizations responsible for the research, development, manufacture, test, and integration of defense and high-technology products, components, and related services. The resulting data will provide a baseline understanding of the structure and interdependencies of organizations that participate in DOD acquisition programs and their associated supply chains. This effort will also assist DSS in its mission to provide security oversight and education on behalf of the DOD and other U.S. Government departments and agencies.

The first surveys were sent to Industry in November 2015, with the goal of surveying every NISP facility over the following two years. The surveys are being mailed to the Facility Security Officer's attention. The survey will arrive via postal mail and email. If your company uses a spam filter, please enter CriticalFacility@bis.doc.gov as a trusted email to avoid issues with receiving the survey email.

Commerce and DSS representatives have begun engagement with multiple facility organizations to assist survey accomplishment, as required. Additionally, a representative will work with the National Industrial Security Program Advisory Committee (NISAPAC), to inform and discuss the survey as it continues.

Finally, BIS has created a [survey website](#) that provides basic information about the survey (FAQs and guidance), so that Industry can become familiar with the survey in advance of receiving notification to accomplish from BIS. Additional questions can be directed to CriticalFacility@bis.doc.gov (preferred) or (202) 482-7808.

RESEARCH, RECERTIFY, UPGRADE (RRU) REQUESTS

The Personnel Security Management Office for Industry (PSMO-I) is overhauling the RRU process and is now only accepting RRU submissions via JPAS under the following three classifications:

- **Reciprocity:** PSMO-I will attempt to verify the eligibility via Scattered Castles¹/Central Verification System² (CVS) prior to contacting the agency directly. If the eligibility is not verified in the available databases, a hardcopy reciprocity request will be submitted to the appropriate agency. Timeframes will vary depending on the action needed or agency response.
- **Upgrade:** Official government requests for information from DoD CAF, DOHA or DSS.
- **Recertify:** The FSO has reason to believe the eligibility line in JPAS is incorrect. All other personnel security-related questions and concerns should be directed to the DSS Knowledge Center at (888) 282-7682.

KNOWLEDGE CENTER

The DSS Knowledge Center replaced the DoD Security Services Center on March 28, 2016. Under Option #2, PSMO-I will field Personnel Security Clearance-related issues between the hours of 8AM and 5PM EST. Our agents utilize their subject matter expertise on e-QIP, RRU, Incident Report, JPAS, CATS to ensure timely resolution for our Industry partners. An average of 1,800 calls is received each week. PSMO-I operates with a 92% On Call Resolution Rate, and the remaining calls are resolved within 48 hours.

¹ A classified Personnel Security Database that verifies personnel security access and visit certifications.

² CVS contains information on security clearances, investigations, suitability and fitness determinations, Homeland Security Presidential Directive 12 (HSPD-12) Personal Identification Verification (PIV) credentials, and polygraph data. This information is provided from agency sources, OPM legacy systems, and via a bridge to JPAS.

SECURITY EDUCATION AND TRAINING

NEW CYBERSECURITY SECURITY SHORT

The Center for Development of Security Excellence (CDSE) is excited to announce the release of their latest Cybersecurity security short – Cybersecurity and the Use of New Personal Devices. This security short is designed to raise security professionals’ awareness of the threats associated with personal electronic devices in the workplace. View the short [here](#).

NEW FOREIGN OWNERSHIP, CONTROL OR INFLUENCE (FOCI) TRAINING

CDSE recently launched the new “FOCI Outside Directors, Proxy Holders, and Voting Trustees Training.” This six module course is specifically designed for the Defense Security Service's Outside Director (OD), Proxy Holder (PH) and Voting Trustee (VT) community. Updates are made on a continual basis with beneficial information and materials for those serving in these roles. Learn more about the course [here](#).

NEW INDUSTRIAL SECURITY ASSESSMENT FOR FACILITY SECURITY OFFICERS (IS104.06)

This assessment provides an opportunity to test the knowledge gained through the completion of the FSO Program Management for Possessing Facilities Curriculum or to refresh the security knowledge learned through your FSO experiences. Students will take on the role of an FSO at a small possessing facility and experience a series of typical security scenarios an FSO might encounter. The FSO will explore the 3D virtual facility, analyze the information presented, and make security-related decisions. Scores from each scenario are accumulated for a final score.

This course is designed to enable students to:

- Carry out day-to-day FSO responsibilities
- Assist facility employees with industrial security processes and procedures
- Evaluate the facility’s compliance with industrial security requirements and address security vulnerabilities or deficiencies as they arise.

[Sign up and test](#) your industrial security knowledge today!

REGISTER NOW FOR THE VIRTUAL INSIDER THREAT SYMPOSIUM FOR INDUSTRY – SEPTEMBER 15

The issuance of Change 2 to DoD 5220.22-M, “National Industrial Security Program Operating Manual (NISPOM),” will bring about new Insider Threat Program requirements. Join CDSE for a live online event following the policy release. We will discuss the requirements, available tools, and resources provided by DSS to help our industry partners. Sign up today for this and other webinars [here](#).

Insider Threat

Virtual Insider Threat Symposium for Industry Requirements Under Change 2 to NISPOM

Thursday, September 15, 2016
10 am Eastern Time

ARCHIVED WEBINARS AVAILABLE

Did you miss the “FSO Effectiveness” or the “Security Chat with Mr. Gus Greene” webinar? No problem! They are now available for your viewing. You can access both webinars and more in our [archives](#).

SOCIAL MEDIA

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

Thanks,
ISR
Defense Security Service