DSS Monthly Newsletter
June 2017

(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.

WHERE TO FIND BACK ISSUES OF THE VOI NEWSLETTER

Missing a few back issues of the VOI Newsletter? The Defense Security Service (DSS) Public Affairs Office maintains a library of the VOI Newsletter (and other important forms and guides) on its "Industry Tools" page.

DSS IN TRANSITION (DiT)

DSS is changing. Where the Agency once concentrated on schedule-driven National Industrial Security Program Operating Manual (NISPOM) compliance, it is now moving to an intelligence-led, asset-focused, and threat-driven approach to industrial security oversight. To achieve this, DSS has already taken a number of significant steps forward.

For example, the Agency is engaging the entire DSS enterprise in this change through an initiative called DSS in Transition (DiT). As part of this initiative, DSS has formed a Change Management Office, launched a comprehensive communications strategy, and is developing a new methodology for implementing this change.

In addition, the Agency has branded its DiT efforts under the tagline, "Partnering with Industry to Protect National Security." To help transform this sentiment into reality, DSS has coordinated with the National Industrial Security Program Policy Advisory Committee (NISPPAC) and assembled a core group of 18 volunteers from industry to regularly provide input on the development of the new methodology. This core group met twice in April, and again in May, and will be meeting monthly going forward. In addition, DSS has established another group of 40+ volunteers from industry to form a focus group to provide ongoing feedback on the effectiveness of DiT communication efforts.

More information about DiT may be found here.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

Coming soon! NISS will replace the Industrial Security Facilities Database (ISFD) and the Electronic Facility Clearance System (e-FCL) in the Fall of 2017. NISS will be the system of record for facility clearance information and for submitting Change Conditions packages, among additional features. For information regarding this critical information system transition, please visit the NISS informational webpage.

MEMO ISSUED REGARDING PERSONAL SECURITY CLEARANCE EXPIRATION

On December 7, 2016, the Undersecretary of Defense for Intelligence signed a memorandum reminding DoD Components that personnel security clearances do not expire. Individuals with current eligibility in JPAS should not be denied access based on an out-of-scope investigation. When the system of record shows current adverse information, but eligibility is still valid, access may continue. The memorandum is provided here for your ease of reference.

THE NISP AUTHORIZING OFFICE (NAO) CONFIGURATION TOOLKIT JOB AID

NAO has released the "Windows Configuration Toolkit for Windows 10" to assist industry in the baseline configuration of information systems. The tool can be accessed and downloaded by industry via the ODAA Business Management System (OBMS), in the Headquarters Bulletin Board, alongside the SCAP and STIG resources. For more detailed instructions, please reference the Job Aid titled "NAO Configuration Toolkit Job Aid" located here.

APPROVAL LETTERS FOR RISK MANAGEMENT FRAMEWORK (RMF) SYSTEMS

Federal Information Systems (FISs) approval letters within the RMF (formerly Guest System letters under the Certification and Accreditation framework) are required if a signed overarching Memorandum of Understanding (MOU) or Interconnection Security Agreement (ISA) is not in place under some circumstances. The relevant circumstances are when the MOU or ISA pertains to the process of standing up thin client terminals in DSS-authorized space, or when the signed MOU/ISA language specifies that an FIS approval letter is required for each contractor system connecting to the government Wide Area Network (WAN).

NOTICE TO CONTRACTORS CLEARED UNDER THE NISP ON INADVERTENT EXPOSURE TO CLASSIFIED INFORMATION IN THE PUBLIC DOMAIN

Issued by the Defense Security Service on June 12, 2017.

When accessing the internet on contractor information systems not authorized or accredited to process classified information, cleared contractor personnel shall not access or download documents that are known or suspected to contain classified information. NISPOM Paragraph 4-106 makes clear that the public posting of classified information does not mean the information is automatically declassified. Classified information in the public domain remains classified and must be treated as such until it is declassified by an appropriate U.S. Government authority. It is the responsibility of every cleared contractor to protect classified information and to follow established procedures for accessing classified information only through authorized means.

Contractor personnel who inadvertently discover potentially classified information in the public domain should immediately report its existence to their FSO. In the event this information is inadvertently discovered on contractor unclassified IT systems, cleared companies are advised to delete the offending material by holding down the SHIFT key while pressing the DELETE key for Windows-based systems, and to clear the internet browser cache. For other than Windows-based systems, a similar "delete" technique shall be used for the affected file(s). If these procedures are followed, subsequent administrative inquires and adverse information reports are not required from the company. These procedures apply only to the inadvertent exposure to classified information in the public domain and NOT to intentional searches for improperly posted classified information in the public domain (e.g., on the internet, Twitter or other media).

Questions regarding this notice should be addressed to the DSS ISR or ISSP assigned to your facility.

DoD CONDUCTING FEE FOR SERVICE STUDY ON CONTRACTOR PERSONNEL SECURITY CLEARANCE INVESTIGATIONS BETWEEN JUNE AND AUGUST 2017

The Counterintelligence & Security (CI&S) Directorate, Office of the Under Secretary of Defense for Intelligence (OUSD(I)), is sponsoring a Fee for Service Study (Study) regarding contractor personnel security clearance investigations.

The objective of the Study is to research options to more effectively manage DoD costs for personnel security clearance investigations, as discussed recently with DSS and the industry representatives of the National Industrial Security Program Policy Advisory Committee (NISPPAC).

The Study will:

- Examine the feasibility of charging cleared contractors a fee-for-service and/or creating a working capital fund from DoD acquisitions to DSS to fund contractor personnel security clearance investigations
- Include analysis of the impact on overall contract costs
- Take into account prior personnel security clearance investigation cost studies from the past 20 years.

The NISSPAC Industry representatives nominated a sample number of small, medium and large cleared companies to be interviewed as part of the Study. In addition, the NISPPAC industry representatives are providing a white paper to DoD for consideration in the Study.

The DoD has not made a decision to move to a fee-for-service or working capital fund model for contractor personnel security clearance investigations, and recognizes previous challenges identified in prior studies. The results of the Study will inform DoD's deliberations about the feasibility and costs associated with any model. Any questions concerning this Study should be directed to your NISPPAC representative.

SECURITY EDUCATION AND TRAINING

REGISTER FOR UPCOMING GETTING STARTED SEMINAR

The live, instructor-led training "Getting Started Seminar for New FSOs" contains two full days of security related and counterintelligence awareness training. Join us for our upcoming course on 15 and 16 August 2017 in Westford, MA.

This course offers new FSOs and security personnel the opportunity to discuss, practice and apply fundamental NISP requirements in a collaborative classroom environment and develop a network of professional associates.

UPCOMING INSIDER THREAT WEBINAR

CDSE invites you to participate in the following live webinar:

User Activity Monitoring in Insider Threat Programs
Thursday 13 July 2017
12:00 p.m. ET

This webinar will discuss the requirement of User Activity Monitoring in Insider Threat Programs. Our live session will focus on elements of successful UAM to support insider threat detection and mitigation.

NEW INSIDER THREAT AWARENESS GAME

Looking for a fun way to encourage Insider Threat awareness at your organization? Share CDSE's Trivia Twirl with your personnel. This popular game is a quick and easy way to remind the workforce of messaging associated with the Insider Threat.

SPeD CERTIFICATION UPDATE

The SPēD Certification Program will release new SFPC and SAPPC assessments on or about 2 October 2017 to include Cybersecurity fundamental knowledge and application level concepts. The Program will also update the SPēD Certification Program Candidate Handbook and Competency Preparatory Tools (CPTs) for each assessment to reflect these new standards. Stay tuned for additional news and updated resources!

CDSE WINS OMNI AWARDS

CDSE was a winner in the Omni Awards spring 2017 competition. Five training products scored silver and bronze awards in the categories of education and government. Information Security Management Course SF 700 Practical Exercise, Special Access Program (SAP) Security Incident Virtual Exercise, and DSS Annual Security Awareness Training each won silver; and SAP Security Incident Videos, and Counterintelligence (CI) Awareness Micro-Learning Video Lesson each won bronze. In total, CDSE earned 10 Omni Awards. Omni Awards recognize outstanding

media productions that engage, empower, and enlighten. As a nationally known award competition, Omni only recognizes those that exemplify the highest standards of quality.

NEW SECURITY AWARENESS HUB LOCATION

The Security Awareness Hub has moved. Please visit to take our courses and ensure that you update your bookmarks and clear your cache. For more information and updates about our new learning platform, follow us on Twitter (@TheCDSE) and on Facebook.

SOCIAL MEDIA

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

Thanks,
ISR
Defense Security Service