# DSS Monthly Newsletter

# August 2012

(Sent on behalf of IS Rep)

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 me know.

## *Information*

***PERIODIC REINVESTIGATIONS-REMINDER***

Depending upon the level of access required, individuals holding security clearances are subject to periodic reinvestigations (PR) at a minimum of every five years for Top Secret, ten years for Secret, and fifteen years for Confidential. For more information on the PR requirement, click here. The FSO is responsible for reviewing access records to ensure employees are submitted for PRs as required in the Personnel Security Program regulation.

NISPOM paragraph 2-201d states that contractors may be subject to a Periodic Reinvestigation (PR) program as specified by the Cognizant Security Authority (CSA). Personnel security policy requires that contractors with access at the Top Secret and Secret levels be reinvestigated at 5 and 10 year intervals from the closing date of the previous investigation. Given that these dates are reflected in Joint Personnel Adjudication System (JPAS), and NISPOM paragraph 2-200b requires that contractors maintain the accuracy of their employees' access records, contractors are responsible for submitting the e-QIP for an employee's PR no later than the applicable due date.

To facilitate meeting this suspense, an employee's e-QIP for PR may be initiated up to **3** months in advance of the due date. DISCO will no longer accept investigations outside of the **90** day window and will start rejecting e-QIP submissions outside of the 90 day window starting August 1, 2012.

To monitor compliance with PR submission requirements, DISCO will run monthly reports of overdue PRs and request e-QIPs for the PRs. If the employee's e-QIP for a PR is not submitted within 30 days from issuance of the overdue notification, DISCO will administratively withdraw the eligibility without prejudice from JPAS and issue a No Determination Made (NDM). For

individuals with no owning Security Management Office (SMO) identified in JPAS, DISCO may enter an LOJ. The previous valid eligibility will be reinstated when the e-QIP is received by DISCO.

**Contractors are reminded to access JPAS accounts weekly and check notifications.**

**MOST COMMON JPAS SAR 'REJECT' REASONS**

The current rejection/disapproval rate for JPAS (JCAVS) System Access Requests (SAR) processed by the DoD Security Services (Call) Center continues to exceed 50 percent. Please see http://www.dss.mil/about_dss/news/20111207.html for the most common reasons for Call Center rejection/disapproval of JPAS SARs. Avoiding these pitfalls will enhance the processing/approval timeline of your JPAS SAR submission, if access eligibility requirements are met. Please contact the Call Center at 1-888-282-7682, if you have any questions. Thank you!

*Defense Information Systems Agency (DISA) Gold Disk is Retiring on December 31, 2012; A Frequently Asked Questions Document is Provided to Address Transitioning to SCAP Tools:*
*Gold Disk FAQs:*

*1*) Question: I've heard the gold disk will be phased out?

**Answer:** Yes. The gold disk project will be terminated on 31 Dec 12. The October 2012 will be the last "updated version" of the tool.

FSO will provide "help desk" support to the gold disk users until 31 Dec 2012. After December, the "Scan only" CD will be posted/available on IASE, however, FSO will NOT provide any further updates or provide trouble ticket support for the tool starting 1 Jan 2013.

FSO publishes "automated" STIG benchmarks which can be run in HBSS Policy Auditor, SCAP Compliance Checker (SCC) or any SCAP-compliant tool. STIG Benchmarks exist for various Windows and Unix platforms, limited Windows applications (i.e., IE8, IE9, etc.) and IAVMs. At present, the benchmarks do NOT fully automate compliance validation for all STIG requirements. The "truly manual" requirements will always be manual but as SCAP evolves and OCIL (open checklist interactive language) becomes an SCAP standard, FSO will "automate" the reporting of the manual policy type requirements as well.

The automated benchmarks are included in the STIG zip files available at - http://iase.disa.mil/stigs/scap/index.html.

IAVM Benchmarks for 2009, 2010, 2011 and 2012 are available at - http://iase.disa.mil/stigs/os/index.html under Windows tab.

**2)** Question: How do I check compliance once the gold disk is terminated?

**Answer:** FSO publishes "automated" STIG benchmarks which can be run in HBSS Policy Auditor, SCAP Compliance Checker (SCC) or any SCAP-compliant tool. The benchmarks exist for various Windows and Unix platforms, limited Windows applications (i.e., IE8, IE9, etc.) and IAVMs. At present, the benchmarks do NOT fully automate all STIG checks. The "truly manual" ones will always be manual but as SCAP evolves and OCIL (open checklist interactive language) becomes an SCAP standard, FSO will "automate" the reporting of the manual policy type checks as well. The current benchmarks contain "validated" DoD STIG requirements. FSO will continue to enhance the benchmarks with further automated checks as the OVAL content is developed and tested. FSO developed process guidance to assist with tool selection, instructions, and exporting the results file. The results file can be imported into the STIG Viewer tool to complete the review for the remaining non-automated and manual checks. STIG Viewer can create a VMS Import File. A recorded DCO session is available which provides guidance and instructions for the entire process.

The automated benchmarks, process guides, and tools are available at - http://iase.disa.mil/stigs/scap/index.html.

STIG Viewer tool and reference guide are available at - http://iase.disa.mil/stigs/stig_viewing_guidance.html.

IAVM Benchmarks for 2009, 2010, 2011 and 2012 are available at - http://iase.disa.mil/stigs/os/index.html under Windows tab

DCO Recorded session is available at - https://connect.dco.dod.mil/p63922313

**3)** Question: How do I remediate once the gold disk is terminated?
**Answer**: The Remediation SCAP standard is not complete, therefore, you will need to manually remediate vulnerabilities or purchase a third party tool to automate the remediation. To remediate missing patches, utilize the DoD Patch Repository (https://patches.csd.disa.mil/Default.aspx).

**4)** Question: How do I establish an initial STIG baseline without the gold disk?
**Answer:** Various Windows image files, which are STIG-compliant, are available for download at - http://iase.disa.mil/stigs/os/windows/dod_images.html. These images should be used as a 'build from' perspective. Layer your site-specific applications and features on top of this base image prior to testing and deployment. To remediate patches, utilize the DoD Patch Repository (https://patches.csd.disa.mil/Default.aspx) to download and apply hotfixes and patches applicable to your system.

**5)** Question: How do I patch my system once the gold disk is terminated?
**Answer:** To remediate patches, utilize the DoD Patch Repository (https://patches.csd.disa.mil/Default.aspx) to download and apply hotfixes and patches applicable to your system.

**6)** Question: Is training available for using the SCAP benchmarks and tools?
**Answer:** Yes. The Windows and Unix Security Readiness Review (SRR) classes have been updated to incorporate the benchmarks and tools. There is also a recorded DCO session which provides instructions on their use.

List of SRR classes is available at - https://powhatan.iiie.disa.mil/classroom_training/Schedule/Schedule.html?Sep12.xml

DCO recorded session is available at - https://connect.dco.dod.mil/p63922313

**7)** Question: Will Gold Disk support Windows 2008 R2 or Windows 7?
**Answer:** No. The gold disk will not support Server 2008 R2 or Windows 7. New development efforts for the Gold Disk were ended in early 2011. FSO developed SCAP STIG Benchmarks for those OS and the benchmarks are available at - http://iase.disa.mil/stigs/scap/index.html

## *Policy*

***DEFENSE SECURITY SERVICE (DSS) RELEASES FAQs REGARDING NATO ANNUAL REFRESHER BRIEFINGS***

Q: Do contractors have to record the most recent NATO Annual Refresher Briefing date in the Joint Personnel Adjudication System (JPAS)?

A: Paragraph 10-706 of the NISPOM only requires the NATO initial briefing date and the NATO debriefing date should be recorded in JPAS. The contractor should retain a verifiable record of the most recent NATO Annual Refresher Briefing.

Q: Is DSS required to provide NATO Annual Refresher Briefing to the Facility Security Officer (FSO)?

A: As DSS is required to provide the NATO initial briefing to the FSO, DSS should also provide the NATO Annual Refresher Briefing.

**VERIFICATION OF US CITIZENSHIP-REMINDER**

Reminder to all Government Cleared Contractor Facilities accordance to NISPOM Chapter 2-207 and 2-208:

- Contractor must require each applicant for a PCL who claims U.S. citizenship to produce evidence of citizenship. The only acceptable proof is as follow:

o Individuals born in the United States, a birth certificate is the primary and preferred means of citizenship verification. Acceptable certificates must show that the birth record was filed shortly after birth and it must be certified with the registrar's signature. It must bear the raised, impressed, or multicolored seal of the registrar's office.

o Individual claiming citizenship by naturalization, a certificate of naturalization is acceptable proof of citizenship.

o Citizenship acquired by birth abroad to a U.S. citizen parent or parents, the following are acceptable evidence:

(1) A Certificate of Citizenship issued by the Department of Homeland Security, .S. Citizenship and Immigration Services (USCIS) or its predecessor organization.
(2) A Report of Birth Abroad of a Citizen of the United States of America
(3) A Certificate of Birth.

o A passport, current or expired, is acceptable proof of citizenship.

o Record of Military Processing-Armed Forces of the United States (DD Form 1966) is acceptable proof of citizenship, provided it reflects U.S. citizenship.

*(Source Document: DoD 5220.22-M, February 28, 2006; and Industrial Security Letter 2010-01, dated, January 28, 2010.*

## *SECURITY EDUCATION AND TRAINING*

**CDSE WEBINAR'S**

Thank you to all who attended our July Learn@Lunch webinar, "Adverse Information Reporting". It was a huge success largely due to your participation! A reminder to those who had an opportunity to sign up; this month's Learn@Lunch webinar, "Security Rating Matrix," is scheduled for August 7. Also, next month's Learn@Lunch webinar, "Life Cycle of the Suspicious Contact Report (SCR)," is scheduled for Tuesday, September 11 at 11:30 a.m. and 2:30 p.m. EST. Additional information is forthcoming.

We look forward to providing webinar topics that continue to contribute to your successful security program—please don't hesitate to send any comments you may have or suggestions for future webinar topics to us at industrialsecurity.training@dss.mil.

**CDSE's NISP Certification and Accreditation Suite of eLearning Courses**

The Center for Development of Security Excellence (CDSE) offers the following four courses for security professionals seeking National Industrial Security Program (NISP) Certification and Accreditation (C&A) training. The courses build upon each other by beginning with the introduction to the NISP C&A process, followed by a more in depth discussion of the individual phases of the C&A process as it relates to the Defense Security Service (DSS) mission, culminating in a discussion on the technical aspects as students are guided through the Baseline Technical Security Configuration Guide. As part of the last course, the students practice configuring security settings within a Windows and Linux virtual environment. The target audience for this suite of courses is contractor professionals who have responsibility for evaluating information systems and certifying to DSS that information systems meet NISP

security requirements. The courses listed below do not contain the final examination; students must register for the exams separately in STEPP and will receive credit for the course upon receiving a passing score. Register for these courses at http://www.dss.mil/seta/enrol/stepp.html.

Introduction to the NISP Certification and Accreditation Process IS100.16 : This two hour eLearning course introduces the NISP Certification and Accreditation (C&A) process. The course discusses the policies and standards used to protect information within computer systems in support of the Defense Security Service mission; and identifies and defines the government and contractor roles and responsibilities.

NISP C&A Process: A Walk-Through Course IS200.16

This 3 hour course is a continuation of the Introduction to the NISP C&A Process Course (IS100.16). This course identifies in depth the individual phases of the C&A process, key characteristics of common system and network types that undergo the certification and accreditation process, and provides guidance on templates and attachments required for successful system package submission.

The Technical Implementation of Certification and Accreditation (C&A) – Configuration to DSS Standards Course IS310.16

This course is the last in the series examining the NISP C&A process. This course focuses on the more technical aspects of the C&A process and guides students by navigating them through a system using the DSS Baseline Technical Security Configuration Guide. It provides the opportunity for students to learn how technical security standards are implemented on an information system through the use of a virtual environment and demonstrations. In addition, it covers procedures for access, maintenance, and analysis of audit logs, Trusted Download procedures, data spills, and Network Security Plan (NSP) and Memorandum of Understanding (MOU) requirements as they apply to the NISP.

The Technical Implementation of Certification and Accreditation (C&A) – Configuration to DSS Standards Virtual Environment IS311.16

The Virtual Environment (VE) provides the opportunity for learners participating in the Technical Implementation of NISP C&A to practice what they have learned in the prerequisite courses in a non-production / test environment. The VE accurately simulates systems using the Windows XP, Fedora 10 Linux, and Windows 7 Operating Systems, allowing for continued development of skills, as well as reinforcing the information and concepts presented through the use of practical exercises without fear of irrevocably damaging a production system.

Thank you,
IS Rep
Defense Security Service