Questions for DSS (AIA/NDIA)

October 2014

1. Does DSS have a time frame established for its shift to the Risk Management Framework (RMF)?

   Response: There is no definitive time frame for DSS to transition to the RMF. With the release of the NISPOM Conforming Change 2 (CC2); however, DSS will start to incorporate RMF terminology and additional security controls into its processes. Subsequent to the CC2 release, DSS will start its development of an RMF process and incorporate it into the ODAA Process Manual at that time.

2. Is DSS still supporting an 18 month assessment cycle if the contractor has received a Superior rating in the past?

   Response: Yes, however there are certain circumstances that would override the 18 month assessment cycle to include Foreign Ownership, Control or Influence (FOCI) and Accredited Information Systems (AIS) etc. In these circumstances, the assessment would be every 12 months.

3. If said contractor has a SIPRNet connection, does this immediately move the facility up to an annual assessment cycle?

   Response: Yes, the Defense Information Systems Agency (DISA)/DSS Memorandum of Agreement (MOA) for DoD CIO approved NISP contractor Secret IP nodes (SIPRNet) requires an annual oversight visit and may require an adjustment to an annual assessment cycle.

4. Will DSS be advocating using the Security Content Automation Protocol (SCAP) tool if all government entities will use a standard for RMF compliance?

   Response: At this time there is no requirement to utilize the Security Content Automation Protocol (SCAP) and associated benchmarks unless documented within a contract or memorandum of agreement/understanding. However, the SCAP tools and associated benchmarks can be used to verify compliance with an operating system baseline as long as it meets NISPOM requirements. The contractor Information System Security Manager (ISSM) can demonstrate compliance to the Information System Security Professional (ISSP). As DSS transitions to RMF, we will re-evaluate the possibility of use and availability of SCAP tools for use within the NISP.

5. In regards to Special Access Program (SAP) contracts in which DSS is the cognizant security office (CSO), has the DoD SAP Central Office provided any guidance and/or direction to DSS as it pertains to accrediting contractor SAP information systems?

Response: The Director, DoD Special Access Program Central Office (SAPCO) issued a letter concerning the "Transition to the Risk Management Framework" (RMF) implementing the Joint Special Access Program Implementation Guide (JSIG) for all departmental Special Access Program (SAP) information systems on Dec 18, 2013. DSS has implemented a phased JSIG/RMF approach for contractor SAP information systems in which DSS is the CSO when required by contract.

6. Is DSS aware that ISSPs across the country are forcing contractors to utilize OBMS immediately? We have a 6 month grace period for compliance.

   Response: We are still in the transition period for OBMS. OBMS is required for Industry's use by March 15, 2015.

7. We are still receiving conflicting guidance across the country by some ISSPs. Some ISSPs are considering Windows XP as a non-compliant OS and are requiring Risk Acceptance Letter (RAL). Will DSS put out any formal policy, if so when?

   Response: Guidance for legacy (e.g. XP) operating systems is being finalized and is expected to be posted by the end of the November.

8. The current OBMS tool is issuing new UIDs to existing information systems (IS). Is there a fix in the works to ensure that the existing UIDs can remain?

   Response: This issue has been addressed. New accreditation actions can be taken against existing UIDs within the OBMS application.

9. We have seen the implementation of OBMS enforcing policy changes. We had been told to reaccredit an IS whenever the MSSP undergoes a change.

   Response: This issue has been addressed. Industry now has the ability to add additional IS profiles for review under an approved MSSP.

10. Regarding the new Removable Media Controls required – what is the retention period for the new log that tracks removable media use (either one year/or one inspection cycle, whichever is longer or life of the system)?

    Response: In accordance with existing NISPOM requirements, all logs should be reviewed weekly and kept logs should be maintained for at least one year/ or inspection cycle whichever is longer.

11. There is confusion when to use the Contractor to Government and Contractor to Contractor MSSPs since these are new "system types" for Master Plans that were rolled out with the new templates.

    They aren't addressed at all in the ODAA Process Manual. Is there any plan to release any guidance on these?

    Response: Guidance for Interconnected Networks is found in Section 3.2.12.2, Page 21 of the ODAA Process Manual. An interconnected network consists of two or more separately accredited systems connected together. There are two types:

    Contractor-to-Government (C2G) systems are interconnected systems Wide Area Networks (WAN) supported by MOUs for connections to Government networks.

    Contractor-to-Contractor (C2C) systems are interconnected systems /WANs of network host(s) or node(s) that become part of a Network Security Plan (NSP). A separate NSP is required to approve interconnecting nodes with for different Facilities, accreditation letters and/or ISSMs for the DSS approved WAN Interconnected WAN.

12. Why does OBMS require that the Facility Security Officer (FSO) must grant access to the ISSM before the ISSM can submit a plan in the database?

    Response: NCAISS/OBMS requires a member of a Facility's Key Management Personnel (KMP) to manage who gains access to their OBMS profile for each Cage Code. As a KMP, the FSO often is required to sponsor the NCAISS/OBMS accounts.

13. Are contractors prohibited from printing JPAS summary pages? The posted guidance says U.S. government personnel cannot print, but it does not specifically state that contractors cannot? If no, then why not? Contractors are allowed to print personnel reports, PR reports, RRU's, which all contain PII and are a snapshot in time, so why not the JPAS summary reports?

    Response: When a Government Contracting Activity (GCA) requires a JPAS printout, the contractors should provide the JPAS printout and also advise DSS Policy at Policy_HQ@dss.mil. DSS has provided this guidance in the following posting: http://www.dss.mil/documents/isp/DSS_Response_to_AIA_Conference_Questions_November2012.pdf

14. If a contractor/industry company already has a relationship with the FBI and we submit suspicious contact reports directly to the FBI (which they prefer) who then opens the investigation, will we still receive the "extra" enhancement credit?

Response: In accordance with NISPOM 1-302b, contractors must report efforts by any individual to obtain illegal or unauthorized access to classified information or to compromise a cleared employee to the CSA (i.e. DSS). Additionally, NISPOM 1-301 requires contractors provide a copy of the written reports made to the FBI, concerning actual, probable or possible espionage, to the CSA (i.e. DSS). DSS's ability to prioritize work, identify threats and vulnerabilities, and educate cleared industry on risk is directly linked to cleared industry reporting. Intentional withholding of reports to DSS, pertaining to requirements outlined in NISPOM Chapter 1, Section 3, is considered to be noncompliant with NISPOM reporting requirements, and a vulnerability can be cited during Security Vulnerability Assessments (SVAs). Please direct any questions from other government agencies related to this guidance to DSS.

As such, in order to be eligible for credit in enhancement category 7b, a facility must have an open investigation linked to a Suspicious Contact Report (SCR) that was reported from the contractor facility to DSS.

Additional guidance on the recent CI enhancement updates can be found here: http://www.dss.mil/isp/fac_clear/security-rating-matrix.html. Please feel free to submit further questions to Rating.Matrix@dss.mil."

15. NISPOM 2-100c states that a contractor shall not use its FCL for advertising or promoting purposes. Does this include listing the level or personnel clearance requesting for an open job posting? If so, can the requirement be written more specifically and clearly?

    Response: A personnel security clearance (PCL) requirement and level (Top Secret, Secret, Confidential) may be included in an open job posting as long as the context of the posting is not for advertising or promotional purposes.

16. Several sections of the NISPOM require personnel briefings, debriefings and training. Are electronic signatures acceptable in lieu of hand written signatures? If so, what are the minimum requirements to satisfy the validation of an employee's participation and completion of required training? Are CAC and/or company software that requires an employee to authenticate their participation and completion of required security training?

    Response: There are no provisions for industry to use digital signatures or company software to authenticate employee participation in required security training to meet NISPOM 3-107, 8-104(4), 8-105. However, electronic signatures have not been approved for non-disclosure agreement (NDA) or other official forms.

17. Are derivative classifier markings required to be put on production hardware?

    Response: Physically marking classified information with appropriate classification markings serves to warn and inform holders of the information of the degree of protection required. As a general rule, the markings specified in paragraphs 4-202 through 4-208 of the NISPOM are required for all classified information regardless of the form in which it appears. Some material, such as documents, letters, and reports, can be easily marked with the required markings. Marking other material, such as equipment, IS media, and slides may be more difficult due to

size or other physical characteristics. Since the primary purpose of the markings is to alert the holder that the information requires special protection, it is essential that all classified material be marked to the fullest extent possible to ensure the necessary safeguarding. If an original classification decision has been made for hardware being produced then the government contracting activity source document or classification guide must be followed. This guidance provides the contractor with security classification guidance needed during the performance of the contract. However, please keep in mind the duplication or reproduction of existing classified information is not derivative classification.