DSS/NCMS Leadership Quarterly Meeting
NCMS Agenda Items
July 31, 2014

The attached document is offered to clarify questions raised at the quarterly leadership meeting between DSS and NCMS on July 31, 2014. The document provides clarification only and does not serve as an official policy document. Facility Security Officers should direct further questions to the local Industrial Security Representative.

1. **Please share with us the latest DSS Updates/initiatives/challenges & how can NCMS assist with any of them**?

   - Director of National Intelligence (DNI) issued an Executive Correspondence dated October 31, 2013(Validate Clearances/Overdue Periodic Reinvestigations) advising Federal agencies that access to classified information is a privilege and decision to entrust individuals with access is a critical decision "that the United States Government takes seriously." In line with this guidance, DSS is placing additional emphasis on existing requirements to keep Personnel Security Clearances to a minimum. New interim clearance process will include an automated solution and all interim clearances will not be granted without a completed fingerprint check or with a positive result. Industry will be given a 30 day advance notice of implementation.
   - National Industrial Security System (NISS) - Will replace ISFD and expand capabilities for automating manual processes and facilitate collaboration across the industry and government agencies
   - NISP Contract Classification System (NCCS) - Automated system designed to streamline the workflow between contracting offices and allow transparency to industry.
   - The CI Enhancement portion of the Rating Matrix is being updated. The existing enhancement will be divided into two separate enhancements. One will focus on process and the other on performance.

2. Overdue Periodic Reinvestigation Notices. Numerous members have cited a concern that they are getting messages from there DSS representative and/or PSMO-I citing overdue PR's that are either already in progress or not applicable. Many have Secret clearances that are not due but are being told they are overdue in error. **Can you address this concern as many are upset that they are getting this email from their rep and they are concerned it will be viewed negatively during their assessment?**

   The system generated email and JPAS messages sent on behalf of the IS Reps and PSMOwere not intended to have a negative impact on the facility's security vulnerability assessment. We apologize for instances where messages were sent in error. With over 30,000 JPAS records appearing to be Overdue for a periodic reinvestigation, the only way to attack this problem was through mass messaging. If the messages were sent in error, please disregard them.

   Currently DSS has funds available to execute toward PRs. In the future FYs, personnel security investigation funding may be limited due to sequestration. Now is the time to submit to ensure timely processing!

Please coordinate with your personnel overdue on their PR to initiate processing as soon as possible. We need FSOs to take one of the five following options:

- If access is required, please complete and transmit an electronic Questionnaire for Investigations Processing (e-QIP).
- If an employee no longer has a requirement to access classified information, please debrief the employee and remove access in JPAS.
- If the subject is no longer employed with your company, please debrief and enter the separation in JPAS.
- If an investigation request has been submitted through another Government Agency please transmit an RRU to DoD CAF IND providing information as to which Agency and when the request was submitted.
- If this is received in error, please submit an RRU to DoD CAF IND to let us know message was an error.

3. Numerous members received a notice that their DSS NCAISS accounts have been disabled due to inactivity? This is a brand new system and most have just established the account. When calling the help desk they were give the following response. If you received a message indicating that your NCAISS has been disabled due to inactivity, please be aware that the DSS Help Desk does not yet have guidance on how to reactivate these accounts. **At present, there is no action that they can take to reactivate accounts. Can you please address this issue?**

In general, when a user does not access NCAISS within 90 days of their last login, an email is sent to the user notifying them that their account will be disabled in 5 days. The Call Center (888-282-7682) is then able to reactivate.

To assist with the OBMS deployment, existing users were imported from ISFD to automatically create NCAISS and OBMS accounts using their ISFD credentials. As of the OBMS deployment (7/15/2014), those selected users had 10 days to complete the sync process or else their NCAISS account would be disabled. If the user's account is disabled then the DSS Call Center (888-282-7682) must reactivate. The NCAISS team will continue to work with the Call Center to ensure they are provided documentation, guides and responses to assist the users.

4. Information Security Topics: We have received a number of concerns and issues members are having with the OBMS. A poll of the ISSC committee members on 7/22/14 reflected that no one had been able to successfully upload an SSP to OBMS. **Is DSS aware of this problem and is there guidance on how to proceed?**

DSS is aware of and has been working issues related to authentication and access to OBMS over the past couple of weeks. ISSMs are now able to upload SSPs after NCAISS issues were resolved during the week of 7/21/14. If specific ISSMs are still unable to access OBMS, he/she should first contact the DSS Call Center. Issues related to working within OBMS can be forwarded to ODAA@DSS.MIL. In either case, if an ISSM is unable to access or use the application, contacting ODAA through the email box provided will result in assistance being provided.

5. Several of our members have indicated that the OBMS process and cross system utilization is not user friendly. They cite some of the following examples: You have multiple sites that require multiple user names and because of the complexity of the passwords required, the rules are not consistent between sites. Both sites require 15 character passwords;

however, one site allows the @ symbol the other does not. One site allows two consecutive characters, the other doesn't. User names are completely different from site to site, e.g., STEPP and OBMS. There are numerous other examples that were provided.

NCAISS is the solution that OBMS is using for authentication purposes. NCAISS is a web-based application that provides Public Key Infrastructure based authentication services to DSS application and information systems for authorized users. Through the NCAISS portal, an authorized user can access their DSS NCAISS portal account via a single sign on (SSO) capability using PKI certificates (either a Common Access Card or DoD approved External Certification Authority). The username and password authentication mechanism is not used for access into OBMS. Additionally, when requesting an OBMS account via NCAISS the user is able to add more than one cage code/site linked to their account.

6. I got an email to approve my ISSM's account in OBMS and it worked with no problem. I then tried to set up my own account in OBMS as the FSO and got the following error message that made no sense to me: **[DefaultSponsorEmail Sponsor was not found.]" Can you please advise us how to resolve this issue?**

This may be an individual account/profile configuration problem. Such "one-off" issues with OBMS may be forwarded to ODAA@DSS.MIL for assistance.

7. We have been told that ODAA will no longer accept any SSP submissions via email only via OBMS. This is a major concern especially since we were told there would be a six month period to still submit via email and for many the system is not working effectively. **Can you please address this very significant concern as we have to be able to submit SSP's immediately? ODAA**

We are allowing six months from the 7/15/14 deployment to migrate over to OBMS. For facilities that have not transitioned to OBMS, the ISSM should continue to submit SSPs via email as they have been doing. If there are specific examples/cases of differing guidance being provided, that information should be forwarded to the appropriate Regional DAA and/or ODAA for resolution.

8. There were some concerns raised regarding ambiguity with "Flaw Remediation." The concern is regarding compliance "at all times." Members from our ISSC feel that it is the ambiguity in the policy that leaves us with a spectrum of interpretations when trying to implement flaw remediation. **Can you address this concern?**

Each system is required to address patch management requirements (flaw remediation) through the accredited SSP. System patching is a routine part of system management. The SSP should include patch management procedures based on the system being accredited. Once the system is accredited, the ISSM should ensure the system is patched in a timely manner after an applicable patch is released.

9. Our ISSC has expressed that there have been some questions in regards to implementation of the new DSS MSSP templates. **Can you address under what conditions ODAA will accept a plan that is not using the new template?**

ODAA Guidance for implementation of the MSSP templates follows:

- If the current accreditation was processed, or was in process by May 15, 2014, no changes are necessary.
- If an IATO or ATO is already established, accreditation is valid until approval

expires, or security relevant changes require reaccreditation.
- If a new system is submitted or is scheduled for reaccreditation, use the new templates.
- Existing templates (to include applications that generate templates) that have been vetted and approved by DSS can be used assuming they are updated to include new verbiage and requirements.

The MSSP templates are posted on the external website at
http://www.dss.mil/isp/odaa/odaa_links.html under "Guidance" for download
They are also available from ODAA at
http://www.dss.mil/isp/odaa/request.html as a zip file

10. RRU Concerns. Why are RRUs taking so long to process? We would like to request a real estimate of how long an RRU should take for action. One of our members indicates that he has been told 18 months due to back log. **Now with people putting in RRUs regarding the PR debacle won't that further extend the RRU closures/process time? PSMO**

On June 17, PSMO-I started providing an initial response to RRUs within 5 days. PSMO-I currently has no backlog of RRU and our goal is 2 working days or less. PSMO-I will answer questions regarding e-QIP, Interim Clearances, and other DSS related issues. RRUs that require a DoD CAF response are forwarded to the CAF for response and adjudicator action. DSS has no control over queries directed at the DoD CAF.

We are aware of a backlog at the DoD CAF. This would be a good topic for Industry to address at the NISPPAC PCL WG.

11. Partnership in decline? There is a perception by many that the industry partnership with DSS & DMDC is suffering. There seems to be a constant stream of changes imposed by both agencies where industry is not being given an opportunity to weigh-in and they are having negative non-value added impacts on our companies. We thought this was the purpose of the NISP & the ultimate formation of the NISPPAC and believe that we had been making great progress but now it appears we are going in the wrong direction. SOME RECENT EXAMPLES CITED:

DMDC: "Contractor security functions can be accomplished without printing from JPAS." "As a reminder, all JCAVS printouts must be protected from unauthorized disclosure and in accordance with the requirements for privacy/sensitive information and For Official Use Only (FOUO), Privacy Act of 1974. Privacy Act requests must be made according to the JPAS SoRN Record Access procedures." The government exchange FOUO information with contractors on a daily basis and we do not have to submit a privacy act request as our contracts authorize this exchange. The same can be stated for JCAVS information. How is the printout any different than the normal visual access? J**PAS Printout restrictions:** Not trusting security professionals with printing JPAS records yet we can handle Top Secret/SCI information every day without violating any laws. We handle PII daily and to impose such a restriction on the entire community for what is purported as some violating privacy laws without any industry input is and continues to be counterproductive and adds little value in our opinion. **We think DSS should revisit this restrictive decision. DMDC is enforcing guidance that was initiated by DSS. Can you speak to this ongoing concern by many of our members?** Is anything being done about the printing visits from JPAS? Now I know why some agencies request both JPAS and letters to be sent…military especially. We have to

duplicate work by sending two visits! What is the difference between printing out a visit in JPAS and having one via Visit Request Letter? Both contain the same information and the letter often contains more.

DSS has addressed this issue and is working closely with DMDC to clarify procedures for printing JPAS records for the non DoD government agencies who do not have access to JPAS. Please see the DSS website providing guidance by DMDC on the use of JPAS printouts. http://www.dss.mil/about_dss/news/20140527.html

12. The new requirements to log into various systems (JPAS, ISFD, OBMS, etc.) within 30 days is unreasonable and treats us as if we are all large companies. They have a need to log-in every 30 days due to the volume of personnel they manage. Most small companies have security professionals that wear multiple hats and they do not have hundreds of personnel clearances to manage or facilities to verify so why do they need to log into these systems every 30 days? Cutting off accounts is severely hurting our industry not helping. We understand your challenge in getting rid of the ghosts in your systems but this solution is creating more problems than its solving. We have so many members now who do not have an ISFD account or some other system and they cannot function. It is very time consuming to re-initiate these accounts, go through various hoops and then risk losing them again. **OCIO**

The 30-day log-in requirement is a U.S. Cyber Command policy. "Dormant" accounts are a risk to the security of the system.

13. New requirement to now have 100% accountability on all TS material within an Information System has significant cost impacts and most feel they will not be able to meet this new requirement, especially large companies. **Why is this change being driven and why were we not afforded a chance to address it before implementation? POLICY**

The FAQ http://www.dss.mil/about_dss/news/20140527.html does not establish new policy requirements; rather it provides a consistent response to the questions on accountability of Top Secret material in accordance with the requirements outlined in the NISPOM.

14. DMDC: We need assistance with challenges many in industry are reporting they are having with DMDC. There is a problem with the reports function in JPAS. Depending on who you talk to (DMDC says it isn't much of a problem) but some people in Industry think it is a big problem; it may or may not impact you. As best we can figure, the new reports functionality is in a different format, and if you take a report from JPAS and use it to update another database, it doesn't work right now. They were expecting to release a correction July 18 but we are being told the problems persist. **Can DSS assist with this challenge?**

According to DMDC, they hope to have the reports fixed by October. They apologize for the delay. Reestablishing this functionality has taken longer than expected.

15. Members have expressed concern that they are still experiencing problems when one contacts DMDC to get changes made in JPAS/DEERS. **Is there anything DSS can advise to address this concern? PSMO**

Please provide specific name and SSNs to the askPSMO-I@dss.mil email address. See DMDC/JPAS website for checklist. https://www.dmdc.osd.mil/psawebdocs/docRequest/filePathNm=PSA/appId=560/app_key_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=JPAS+Data+Correction+Checklist.pdf

Recommend industry consider addressing during the NISPPAC PCL WG.

16. We would like to seek guidance and counsel from DSS and possibly work on some strategic initiative to address the on-going concern of Public Trust (POT) clearances with various User Agencies and the lack of real reciprocity resulting in costly multiple background investigations across organizations. We realize that DSS has no involvement in this process but since your agency is the only central entity in the NISP for personnel clearances we thought we would seek your advice. Many of our companies have multiple contracts across the spectrum that says they honor reciprocity but depending on the agency using the SF 85 P process many clearances are taking between 1 to 2 years for folks who may already have a Secret, Top Secret or SCI clearance. We believe this is a true example of an ineffective use of limited resources to manage the clearance process. **Is there any chance that DSS can get involved in this process or is this something that perhaps the NISPPAC should pursue? (POLICY)**

Recommend Industry approach this during the NISPPAC PCL WG.

17. We still need to find out why clearances are taking so long when they go to what used to be DOHA. We have a member that indicates they have one clearance that has been sitting for almost 2 years now and unfortunately this is not unusual. Also, since they changed the NACLC process they are taking up to 18 months! Just to clarify – when mentioning the NACLC process…in this case they are referring to Positions of Trust in which our Gov't customers have to process. They are taking a year to 18 months to get a favorable or unfavorable decision and consequently it is hindering our companies from being able to execute on contracts. **Can DSS address this concern?**

Recommend Industry approach this with the DoD CAF and DOHA during the NISPPAC PCL WG.

18. During a DSS assessment in northern Virginia, a member indicated that a DSS rep said he wanted separate PSM Nets for cleared employees and then those who the customer requires to be 'owned' by the company in order to get POTs or CACs but do not have DoD clearances. The rep stated that he knows of companies that have done this but could not provide the contractor any guidance on how to accomplish this or the name of any of the companies to contact. The FSO called the DMDC help desk and they said this proposal was not possible to their knowledge. **Is this a possibility and, if not, might that be something DSS or PSMO-I takes into consideration for the future? POLICY**

Please send specific examples (command name/POC) to HQ_Policy@dss.mil and we recommend Industry approach this during the NISPPAC PCL WG.

19. A member has requested DSS assistance in helping to smooth out the process of transferring adjudication of active investigations from one agency (e.g. NSA) to another (e.g. DOD) so the employee doesn't lose their eligibility when the losing agency (NSA) enters the Loss of Jurisdiction in the system. Administrative lag or delay in processing employee transfers from agency to agency sometimes cause temporary break in eligibility,

loss of access and loss of revenue. For small businesses this can be devastating. **Can DSS address this concern?**

Be sure to submit a JPAS RRU to DoD CAF IND.
Please provide specific name and SSNs to the askPSMO-I@dss.mil email address if it's taking more than 15 days. The DDNI is addressing reciprocity metrics.
This would be a good topic to address during NISPPAC PCL WG.

20. On multiple occasions, DIA is adjudicating SCI eligibility on an old investigation instead of the newest one. That makes the adjudication out of scope, and the SSO (at the Joint Staff) has to request that DIA fix the investigation date in JPAS to reflect the newer one instead of the out of scope date. As a result, the eligibility is null until the proper investigation is used. **Can DSS advise us on how they think we could address this challenge? Any and all assistance on getting that problem resolved would be appreciated**.

Please send an email to askPSMO-1@dss.mil requesting assistance. PSMO-I will then contact the email sender to obtain further information on the subject.