DSS/NCMS Leadership Quarterly Meeting
15 November 2013

1. **Kudos: FSO Toolkit and our continued partnership in light of challenges.**
2. **Government Shutdown Update**
    a. Personnel Security Clearance backlog & PR's. Can you provide us an update? With the recent PR suspension & now the recent shutdown our community is being negatively impacted in getting critical positions filled due to these challenges. Can you let us know if DSS has a mitigation plan to address these challenges?

DSS started submitting PSI request to OPM on 25 Oct. There are currently 13,600 in the Queue with the oldest date of 7 Oct(as of 8 Nov). PSMO-I is working the PSI request based on first in first out. PSMO-I receives approximately 600 request/day and, through the use of overtime, projects to have the backlog worked in Q2-FY14. We request industry notify PSMO-I if a PSI request in the queue is no longer needed.

3. **DSS Webinars/Brown Bags** – we would like to see these expand to at least 50 minutes and proof of training/attendance provided. Our members who attend this training are not able to earn continuing education credit unless the training is at least 50 minutes. With limited training dollars and time constraints imposed on everyone we request your consideration. Most professional certification programs require CE points to retain the certificates and 50 minutes is the minimum time.

Learn@Lunch webinars are by design 30 minutes or less to prevent companies from having to bill for security training over 30 minutes. This 30 minute structure was discussed with NCMS at the onset to maximize contractor opportunities and attendance. CDSE recommends NCMS address the PDU allocation with the accrediting institution as follows: Members are allowed to accumulate continuing credit for training less than 50 minutes. For example, credit would be earned after attending two 30 minute Learn@Lunch webinars versus attending one 50 minute presentation. CDSE currently provides all attendees with a "thank you" email after each webinar which provides proof of attendance. This email includes the name of the webinar, date of attendance, and length of training.

4. **CDSE Review** – we have a concern that no one from NCMS was afforded an opportunity to participate in the CDSE review and feel that we are best suited to ensure industry perspective is represented. We would like to request that our board is afforded an opportunity to appoint someone to participate in the CDSE reviews going forward.

NCMS has routinely been invited to the annual CDSE Industrial Security Curriculum Review meeting in the past. The invitation process for this year's meeting was changed and NCMS was inadvertently omitted. When this oversight was discovered, it was too late to process a non-DoD attendee for access into the Pentagon. CDSE apologizes for this year's oversight. We request NCMS provide a primary point of contact and so that this oversight does not happen for future curriculum review meetings.

5. **ISFD**
    a. **Status** – we would like a status of the new ISFD and would like to know if we will have an opportunity to review and provide comments?

DSS is in requirements definition phase for the National Industrial Security System, NISS. The NISS is DSS' future information system architecture and will replace Industrial Security Facilities Database (ISFD) capabilities, while integrating access to DSS and partner applications and data, to develop an on-demand, data-driven environment that strengthens the National Industrial Security Program (NISP). NISS will serve as a one-stop CAC-login enabled interface providing DSS, Industry, and Government personnel a single point-of-entry to access a diverse set of NISP information system activities. In CY 2014 DSS will coordinate details on NISS capabilities with Government and Industry partners for comments.

We will submit recommendations to the ISFD sustainment team for inclusion in future rollouts. In the meantime, Field Office addresses and additional information can be found at - http://www.dss.mil/isp/dss_oper_loc.html

b. **Recommendations** – we would like to see the following added to the Summary sheet:
   i. **FSO email address**
   ii. **Facility Category Code and the Facility's Field Office address**

6. **Derivative Classification Training** – industry has experienced issues in gaining access to the DTIC training. We realize that this is not a DSS system but you are our line to the training is this something you can assist with? The ISL that was issued Oct 8th included a link and it is not working? Security professionals can complete the training via ENROL but that is not feasible for those CDC's that want to use the training for employees.

(CDSE) CDSE apologizes for the inconvenience caused by the inability to access the CDSE Derivative Classification Course, since the partial government shutdown. We worked diligently with the web service provider to restore the site. We are pleased to report that access was restored on 31 October 2013.

(IP) The site is now available. It was back online on 10-31-2013. It was down due to furlough and the government closure. DSS posted notices once we were aware it was down and a notice when the site was re-established.

7. **Assessment Categories & Frequency Inconsistencies** - We have heard from some local DSS representatives that there are now some new facility categories that will determine frequency of assessments. There seem to be some inconsistency in how these are assigned. Can you discuss the new frequency assessment categories: 1, 2 and 3 and how they are determined in conjunction with the size: AA, A, B, C, and D & E?

The DSS method for scheduling assessments for facilities has not had any recent changes nor any scheduled process modifications. DSS considers the known assets, threats, and vulnerabilities of a facility in conjunction with the size, scope, and complexity of NISP operations to effectively identify the timing and team size for recurring vulnerability assessments. It is the DSS goal to schedule vulnerability assessments 90 days in advance when at all possible.

8. **eFingerprint Status**:

Industry is at 33% electronic submissions/month with the December 2013 deadline approaching. DSS provided 5 options for Industry to leverage in meeting the electronic fingerprint submission directive. NCMS has been a great enabler in working with companies to assist in implementing the eFP solutions. Recommend continuing to promote options and lessons learned through NCMS channels as preparation for the change in the Interim eligibility process (ECD 1 Jan 2014).

9. **Information Systems Security:**

a. We previously had established a **partnership with ODAA and the NCMS ISSC** to work on various initiatives. Henry Yeh was the ODAA rep that had been working with our committee be we have learned that he now have a new position. We think this partnership is critical and would like to request a new ODAA Rep be appointed to work with our committee. Can you address this request?

DSS agrees that our partnership with industry and the NCMS ISSC is important. It is unclear what work is being done by the committee. DSS will support as resources allow, but does not have the staffing to assign an individual person as all employees are pulled in many directions in support of the current mission.

b. Can you provide us an update on the following: ODMS AND ODAA Process Guide?

The Process Guide has completed coordination and is expected to be issued/released November 15, 2013. Once it is issued, there will be a six-month transition period.

OBMS deployment is dependent the DSS National Industrial Security Program (NISP) Common Access Information System (NCAISS). Successful deployment of NCAISS will dictate the timeline for deployment of OBMS. We estimate this will occur sometime during 1QCY14.

c. **"IS" Self-Certification confusion**: Can you provide us clarification as to the requirements for Self-Certification? Some of our members indicate that they have been told there is now a requirement to complete seven (7) courses to obtain self-certification authority. However, they state that they could only find three (3) courses.

There are only three online courses required of ISSMs seeking self-certification authority. The three required courses are updates to replace the retired "NISPOM Chapter 8" course that was previously required. The exams for the three courses may be misunderstood as three additional courses due to the sign up process. There is another optional Chapter 8 Implementation course. The basis for the information regarding "7" courses is unclear. If further details can be provided, we can follow up with the source.

d. **Data Spill Policy –** we had a member convey that they feel this policy is too rigid, costly, time consuming, excessive and non-value added. For example: they contend that instead of a 3 time over-write a one-time over-write is more than sufficient and would save time and considerable dollars for desk tops and servers. Another example cited as "unproductive" was the requirement to wipe the free space from a server since most servers are set-up in a RAID configuration. They feel this serves no purpose and degrades the processing capabilities. Due to advances in technology a one-time overwrite is more than adequate. There are several other examples provided that suggest ODAA should consider re-evaluating the data spill policy and our Information Systems Security Committee (ISSC) would love to partner with you on this effort. Can you address this concern?

Three-pass overwrites are standard practice. The data owner does the final evaluation and approval of data spill cleanup. It is possible the data owner could approve a process requiring more, or less, overwrites.

e. When a stand-alone Information System is needed for processing a classified RFP, and a DD254 is provided for this purpose, is there a process for DSS to provide any expedited service for an IATO given that the response timeline will be short? Additionally if an RFP requires classified storage is there a process to expedite storage capability authorization for the same reason?

In general, system accreditations are granted in a timely fashion. System accreditations are processed in a first in, first out process based on the assigned staff supporting the area of responsibility. Systems deemed “warfighter critical” and justified as such by the GCA may be expedited.

10. With the CCRI transitioning from DISA/USCYBERCOM to DSS, how will this affect the annual vulnerability assessment? Will CCRI become annual? When?

The CCRI process and the annual assessment will be treated as separate DSS activities. DISA and DSS are still working out the details of the transition to include how the CCRI schedule will be set and executed. It is unlikely DSS will be able to conduct CCRIs at all NISP sites annually. That said, SIPRNet systems should be configured and managed in accordance with applicable requirements from cradle to grave. SIPRNet systems should be maintained in a compliant state at all times.

11. Are there any plans to update the JCAVS users’ guide?

DMDC owns JPAS and is responsible for the JCAVS user’s guide.

12. Can DSS clarify the application of the “separation date” in JPAS? Some ISRs will tell FSOs that entering a separation date is required in all cases as part of the debrief process, even if the debrief is only to remove access, not for a termination. Others will say that the separation date should be entered when the individual actually terminates employment with the organization or if a requirement for future access is not expected. Please clarify. Will this be clarified in the recent ISL draft that was just sent out; we were not afforded an opportunity to provide feedback on this ISL?

Procedures to address the management of personnel security records in JPAS for break in access and break in employment is forthcoming. Once approved, the guidance will be available on the DSS website.

13. What does DSS believe will be the implementation timeline for the proposed NISPOM Conforming Change #2?

The Office of the Under Secretary of Defense Intelligence, Security Policy and Oversight Directorate is the executive agent for the NISPOM. DSS does not have a timeline for its release to provide. When the NISPOM is approved for release, we will ensure that industry is notified.

14. What actions (if any) does DSS anticipate Cleared Defense Contractors will be required to take regarding Executive Order 13556 (Controlled Unclassified Information) in 2014? Does DSS envision CUI becoming a new DD254 performance category?

DSS does not manage the policy for Controlled Unclassified Information. We do not have any information on what actions contractors under the NISP will be required to take regarding the EO. The DD Form 254, Classified Contract Security Specification conveys security requirements for classified contracts. It can be used to convey requirements for FOUO or other categories of unclassified information associated with classified contracts.

-ISOO has the responsibility to develop the national policy for CUI.