DSS Response to AIA Conference Questions

1. **When (estimate) do you think the National Interest Determination (NID) decision will be made?**

   Currently, an estimate time cannot be provided; however, there are policy changes regarding the NID process under consideration for the Department of Defense (DoD) level policy by Office of the Undersecretary of Defense for Intelligence (OUSD (I)).

2. **When does derivative classifier training become effective? Will guidelines be provided to industry?**

   Derivative classifier training will become effective with the issuance of the National Industrial Security Program Operating Manual (NISPOM) Conforming Change #1. The Defense Security Service (DSS) will provide guidance on training requirements upon issuance of the NISPOM, conforming change. Pending final determination of training requirements by DSS, cleared contractors may take derivative classification training that is available through the DSS, Center of Development and Security Excellence (CDSE).

3. **When can we expect a faster turnaround on adverse information adjudication cases? Will the new DoD Central Adjudication Facility (CAF) help this?**

   All reportable adverse information outlined in Section 3 of the DoD 5220.22-M is processed by the DoD CAF through the Joint Personnel Adjudication System (JPAS) and the Case Adjudication Tracking System (CATS) regardless of how it is received at the DoD CAF (mail, email, fax, JPAS). The DoD CAF has recently implemented new procedures for tracking and processing adverse information reports. It is anticipated that these changes will reduce the processing times for adjudicating incidents once all pertinent information has been received; however, because the changes are recent, metrics are not available to determine the effectiveness. Facility Security Officers (FSO) can help facilitate quicker processing of adverse information reports by including the basic information covering "who" (who was involved; for example: subject, law enforcement agency, court name), "what" (what is/was the incident), "where" (where did the incident happen; for example: city, state), and "when" (when did the incident occur).

4. **What actions are taking place by DSS to work with Defense Manpower Data Center (DMDC) to properly disseminate policy/guidance to industry?**

   DSS Policy Division is actively coordinating with DMDC to determine the best way to disseminate policy/guidance to industry to prepare for policy or operational changes.

5. **Industry is required to send copies of JPAS summaries to various agencies. Is any guidance coming to provide official approval for industry to do this?**

   Please refer to Industrial Security Letter (ISL) 2010-01, article 5. When a Government Contracting Activity (GCA) requires a JPAS printout, the contractors should provide the

JPAS printout and also advise DSS. We believe the only GCA requiring the JPAS Printout is the Department of State (DoS). If there are other GCAs beside the DoS requiring contractors to provide JPAS printouts, please provide the name of the GCA and a point of contact. Submit the information to the DSS Policy email inbox at Policy_HQ@dss.mil.

6. **What is the status of the JPAS replacement program? Please summarize the improvements/enhancements.**

Status of JPAS replacement, the Joint Verification System DISS (JVS), will be fully deployed in FY2015 decommissioning JPAS in FY2016.

Summary of improvements/enhancements :

- JVS is the evolved future state system to replace the JCAVS module of JPAS for security management
- JVS is an automated management tool that will provide the following enhancements for approximately 80,000 Security Managers:

– Common Access Card (CAC) enablement
– Efficient management of accesses
– Enhanced visit request capability
– Simplified ability to manage incidents
– Simplified Security Management Office (SMO) management
– Connection with Portal / Enterprise Services
– Increased automation
– Improved user experience and ease of use
– Industry specific data including Key Management Personnel (KMP), Commercial and Government Entity (CAGE) codes, and Facility Clearance Level (FCL)

7. **Has the DSS looked at current and future facilities under stress because of layoffs/closures?**

DSS routinely reviews current cleared and incoming facilities to get a clear picture of a company's financial condition. This review does not focus specifically on layoffs and closures, but on the overall financial condition of a company. When looking at the condition of cleared companies, DSS searches key indicators that determine whether a company is financially vulnerable or has undergone a material change without notifying DSS.

8. **Is there increased diligence to deter violations from distracted or disgruntled employees, insider threat, etc.?**

Addressing and resolving issues such as security violations, insider threat or other significant issues within industry are among the highest priorities within DSS. There is a clear standard for addressing and reporting violations by all cleared employees. When a reportable event occurs, whether it is a suspicious contact, security violation or adverse information, it is critical that the FSO report this information to DSS. FSO's should also be cognizant of factors impacting their workforce, and take steps to ensure that employees are aware of security policies, are trained appropriately, and remain diligent in their duties to protect classified information. DSS continues to stress this during security assessments and is also continuously working to improve training for FSOs and the cleared community.

9. **What is the DSS view on the potential impact of sequestration?**
   DSS is awaiting DoD guidance on sequestration and has no view or comment until then.