NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

MINUTES OF THE MEETING
(Finalized February 26, 2008)

The NISPPAC held its 29th meeting on Thursday, November 15, 2007, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, N.W., Washington, D.C. Mr. J. William Leonard, Director, Information Security Oversight Office (ISOO) chaired the meeting. The meeting was open to the public.

A. Welcome, Introductions, and Administrative Matters – The Chair greeted the membership and attendees. The participation of two new Industry members to the NISPPAC, Mr. Chris Beals and Ms. Sheri Porter, was acknowledged. In addition, the Chair also recognized the service of two departing Industry members, Mr. Ray Musser and Ms. Donna Nichols.

B. Old Business – The Chair requested that Mr. Greg Pannoni (ISOO) lead a discussion reviewing the eight (8) action items from the May 16, 2007 NISPPAC meeting.

1. **Federal Information Security Management Act (FISMA)**

   "The Federal Information Security Management Act (FISMA) Industry White Paper will be continued as an open action item. The paper will be submitted to the Office of Management and Budget (OMB) for the purpose of requesting more explicit implementation guidance vis-à-vis industry. The scope of the paper will be specific regarding the origin of FISMA-related issues, e.g., whether issues are resulting from agency FISMA implementation or being generated as a result of other agency activity such as new directives on the protection of sensitive acquisition-related information. FISMA problems will be defined and framed with as much precision as possible."

   At the request of the Industry representatives, the action item was closed. Based on feedback provided by Mr. Musser, the NISPPAC Industry spokesman, concerns regarding FISMA were overtaken by events, particularly in light of Defense Industrial Based Information Assurance (DIB IA).

2. **Secret Internet Protocol Router Network (SIPRNET) Access**

   "The Chair, on behalf of NISPPAC, will explore options with the Defense Information Systems Agency (DISA) regarding the extension of SIPRNET access to industry partners, and report back to the NISPPAC membership."

   The Chair reported on his recent meeting with senior DISA management. The results were positive. Solutions regarding possible funding were discussed. Further meetings are planned to work out specific plans and details.

   ACTION: The NISPPAC Chair will continue to explore options with the Defense Information Systems Agency (DISA) regarding the extension of Secret Internet

Protocol Router Network (SIPRNET) access to industry partners.

3. **Homeland Security Presidential Directive 12 (HSPD-12)**

"ISOO Staff will solicit a formal response from the Office of Management Budget (OMB), Ms. Carol Bales, on overarching issues and questions regarding HSPD-12 submitted previously by Department of State (DOS) and Department of Energy (DOE). The responses will be forwarded back to the NISPPAC membership. It was agreed that from an industry perspective, as a stand-alone issue, HSPD-12 is a closed action item."

The OMB response included input from the Office of Personnel Management (OPM) and was obtained and forwarded to the DOS and DOE on August 2, 2007. With the concurrence of both agencies, the response was then forwarded to the NISPPAC membership. Ms. Kim Baugher (DOS) stated that issues regarding INTERIM SECRET Personnel Security Clearances (PCL) have increased, especially since HSPD-12 standards were included in a Memorandum of Understanding (MOU) between DOD and DOS for the issuance of Common Access Cards (CAC) in Iraq. There are large numbers of contractors in Iraq without security requirements in their contracts. Without clearances, CACs cannot be issued unless the contractors are able to provide evidence that the HSPD-12 requirements are being met. DOS is being forced to process contractors for investigations who do not need to be cleared, but require CACs. Ms. Geralyn Paskievicz (DOE) stated that efforts towards common adjudicative criteria will facilitate reciprocity throughout the Executive branch. However, the response from OMB and OPM indicates that suitability determinations are presently agency-centric and thus, when made in this manner, work against reciprocity. Ms. Kathy Dillaman (OPM) stated that there is a multi-agency effort to reach a standard baseline for suitability determinations. OPM is taking the lead on establishing common adjudicative criteria for categories of individuals who are not covered by 5 C.F.R .731, and also expanding a database to provide visibility into the decisions made across the Government for the affected populations. The timelines for the latter efforts are aggressive.

ACTION: At the next NISPPAC session, the Office of Personnel Management (OPM) and the Office of Management and Budget (OMB) will provide an update regarding current efforts to promote reciprocity for suitability determinations to include common adjudicative criteria.

4. Suitability

"Mr. Vincent Jarvie (Industry) will complete a review on the appropriateness of a suitability primer which was provided by OPM and is currently posted to the ISOO NISPPAC web-page. ISOO staff will facilitate any recommended changes with OPM."

Mr. Pannoni reported that the review was completed and one change was agreed upon between Mr. Mark Pekrul (OPM) and Mr. Jarvie. The change concerned the effects of an adverse suitability decision on security clearances and was agreed as follows:

"An adverse suitability determination may result in a decision that a period of debarment for up to three years from all positions in the competitive Federal service is warranted. An agency may deny a security clearance based in part on the presence of a previous negative determination, but there is no administrative procedure mandating automatic government-wide debarment for security clearance determinations."

This change replaced the following:

"An adverse suitability determination may result in a decision that a period of debarment for up to three years from all positions in the competitive Federal service is warranted, while an adverse security decision is only pertinent to the specific position under consideration."

The suitability primer, which is currently posted to the ISOO NISP page (http://www.archives.gov/isoo/oversight-groups/nisp/), will be amended with the agreed upon change. The action item was closed.

5. Electronic Attachment of Releases

" The Defense Security Service (DSS) will provide feedback on the electronic attachment of releases by June 30th to the NISPPAC, and on options and alternatives regarding fingerprints, including the potential for the use of GSA service centers or other alternative sources.

Mr. Pannoni reported that DSS provided feedback on October 12, 2007. The feedback on the action item was provided to the NISPPAC membership in an ISOO email (November 13, 2007) and also included in the NISPPAC meeting folder. The specific action item was closed. The electronic attachment of releases will be further addressed through the report of the PCL Ad Hoc Working Group, which is on the meeting agenda.

6. **Analysis of end-to-end Clearance Processing**

" Representatives of the Industry NISPPAC membership, OPM, and DSS will meet in order to analyze key data points that measure end-to-end clearance processing for industry. The work of the group will focus on data points associated with transmission of applications and cases between DSS and OPM. In addition, the group will produce projected trend lines with respect to reducing pending cases through the end of the calendar year. Specific recommendations for process improvements should be reported back to the NISPPAC membership by June 30th. Recommendations should identify current and desired states as well as approaches, plans, and time lines for achieving results.

Mr. Pannoni stated that this action item would also be addressed through the report of the PCL Ad Hoc Working Group.

7. **DSS Office of Designated Approving Authority (ODAA)**

The Chair of the NISPPAC will meet the Director of DSS in order to assess how the NISPPAC can contribute to enhancements of the DSS Office of Designated Approving Authority (ODAA) process.

Mr. Pannoni reported that on July 13, 2007, the Chair of the NISPPAC met with Ms. Kathy Watson (Director, DSS), Ms. Mary Griggs (DSS), and Mr. Stephen Lewis (DSS). An agreement was reached that DSS and Industry would participate in a working group on enhancements of the DSS ODAA process and would make a joint presentation to the NISPPAC. The report of this group is addressed under new business.

C. New Business

1. **Personnel Security Clearance Ad Hoc Working Group Report** – A report on the working group's progress was the subject of a joint presentation by Ms. Deborah Smith (OPM) and Mr. John Haberkern (DSS).

   a. Ms. Smith stated that the working group is tasked with developing a comprehensive system of metrics, to include key data points, in order to measure the timeliness of end-to-end clearance processing for Industry. The metric data presented for the 2007 fiscal year covers a sampling of approximately 124,000 adjudicated cases. The sampling was confined to cases using Electronic Questionnaires for Investigations Processing (e-QIP) in order to measure processes from the time that the Subject's request for clearance is initiated in e-QIP to final adjudication. Average processing times were computed for specific clearance types and then for the overall population. Average timeliness was also computed for the first 90%, 85%, and 80% of cases completed.

b. The following chart presents the computations:

Industry's National Security End-To-End Metrics

FY 07 Adjudication Decisions Analyzed	Top Secret Initials 13,077	Secret 92,320	Top Secret Reinvestigations 18,886	Overall National Security 124,283
Average Timeliness	312 Days	228 Days	367 Days	258 Days
90% completed in an average	280 Days	198 Days	339 Days	226 Days
85% completed in an average	268 Days	188 Days	327 Days	213 Days
80% completed in an average	257 Days	178 Days	316 Days	202 Days

*Sampling limited to those actions with required data fields -e-QIP submissions

c. The following key data points and processes were captured:

INDUSTRY e-QIP Initiation – time reflects the date subject is initiated in e-QIP until e-QIP is released to DISCO
Initiation date until the date Subject begins e-QIP
Date Subject begins e-QIP until Subject signs e-QIP
Date Subject signs e-QIP until e-QIP is released to DISCO

Defense Industrial Security Clearance Office (DISCO) Front End Time – date e-QIP was released to DISCO until e-QIP released to OPM (an average 1.6 days – data provided by DSS)

OPM Received Package – date e-QIP released to OPM until required forms are received (fingerprints, releases, etc)

OPM Investigation Process – date the investigation request was received until the completed investigation was mailed out

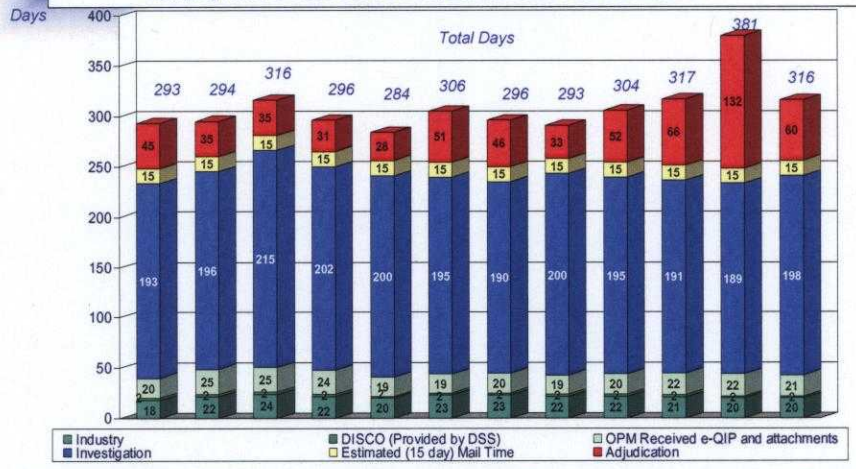
DISCO Adjudication Process – Federal Investigative Service Division (FISD) mailed out date until date of adjudication minus 15 days for estimated mail time

NOTE: DISCO Adjudication time includes any additional investigation required

d. The following metric data was presented:

Industry's End-To-End Metrics
Initial Top Secret (SSBI) Security Clearance Decisions

*Sampling limited to those actions with required data fields -e-QIP submissions

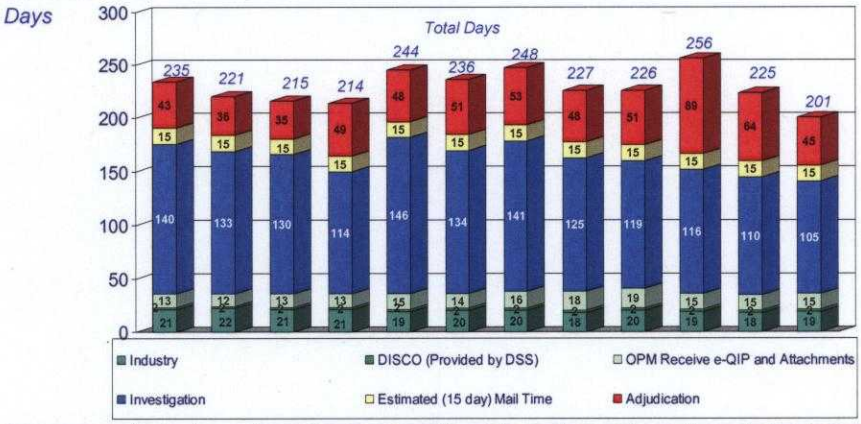


*Sampling	Oct 06	Nov 06	Dec 06	Jan 07	Feb 07	Mar 07	Apr 07	May 07	Jun 07	Jul 07	Aug 07	Sept 07
e-QIP submissions	488	655	637	641	618	1,372	1,115	1,462	1,729	1,393	1,376	1,591

Please note: DISCO Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested

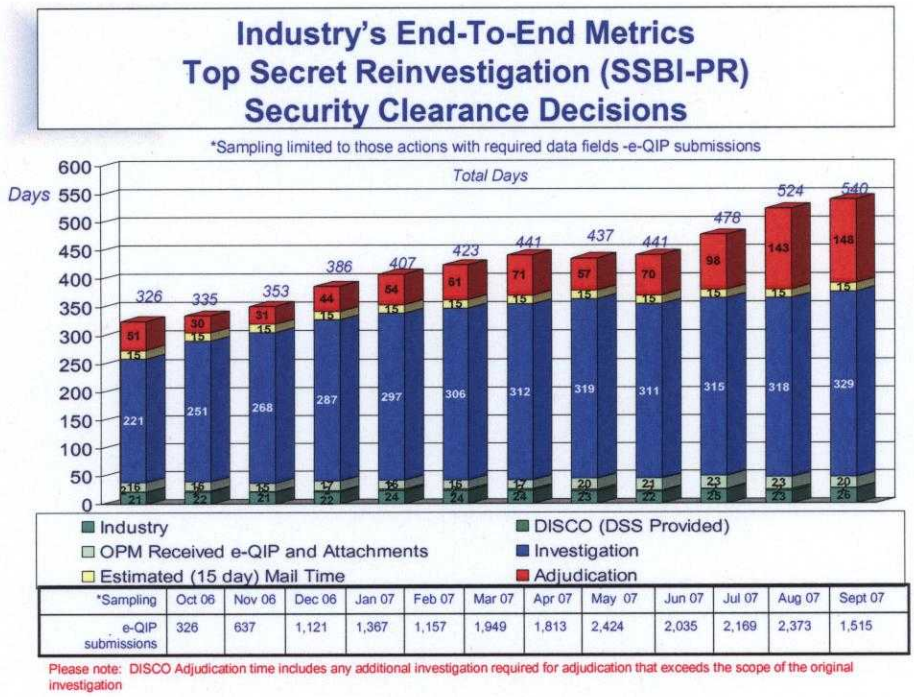
Industry's End-To-End Metrics
Secret (NACLC) Security Clearance Decisions

*Sampling limited to those actions with required data fields -e-QIP submissions



*Sampling	Oct 06	Nov 06	Dec 06	Jan 07	Feb 07	Mar 07	Apr 07	May 07	Jun 07	Jul 07	Aug 07	Sept 07
e-QIP submissions	4,289	6,356	5,672	9,095	5,790	8,060	6,023	5,846	5,520	10,348	14,089	11,232

Please note: DISCO Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested



*Sampling	Oct 06	Nov 06	Dec 06	Jan 07	Feb 07	Mar 07	Apr 07	May 07	Jun 07	Jul 07	Aug 07	Sept 07
e-QIP submissions	326	637	1,121	1,367	1,157	1,949	1,813	2,424	2,035	2,169	2,373	1,515

Please note: DISCO Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation

e. Ms. Smith observed that the increasing times for adjudications of initial SSBIs reflect OPM's work on the old inventory cases. As the inventory is reduced, the impact is increased workloads for adjudications and challenges for the continued timeliness of the latter. Mr. John Fitzpatrick (Office of the Director of National Intelligence [DNI]) observed that if the sample only includes those cases that were adjudicated then the selection mechanisms used by the adjudicative facilities will influence the total sample. For example, if the Central Adjudication Facilities (CAF) are closing out the oldest cases, then this would present an end-to-end view of the contribution of investigations to closing out the old cases and their matching adjudications. However, if this is not the case, then not too many conclusions can be drawn regarding what makes up the investigative timeline since the latter is driven by which cases were closed. Ms. Dillaman stated that this correctly identifies a problem in measuring progress; and observed that the better OPM performs in closing old cases, the worse the agency appears statistically since the average age of the cases being processed will increase. In summary, last year OPM closed 150,000 more investigations than were received. These closings represented a collapsing of the backlog. Consequently, the current average age of the clearances granted throughout the entire year does not reflect timelines for new cases entering the process. Average end-to-end timeliness measured from the date the Subject certified his or her data until the adjudication date, if started during the first half of fiscal year 2006, for new TOP SECRET SSBI cases was 352 days; and if started in the first half of 2007, was 195 days, which represents an improvement of 45%. Similarly for SECRET cases, the average end-to-end time was 230 days in 2006 and 138 in 2007. Hence, the metric data presented in PCL Ad Hoc Working Group slides does not fully represent the progress being made. The Chair stated that the slides in the presentation represent what Industry is experiencing today and inquired regarding the possibility of making projections for the next six months. Ms. Dillaman stated that most likely, by January 2008, OPM will work down the old case load and will be at a "steady state" or

currency with incoming traffic, which is based on working from a ninety day deadline. At the point of "steady state," the majority of older cases will be shuffled out of the system.

f. Ms. Smith stated that a survey is being distributed to further identify opportunities for process improvements. Mr. Scott Conway (Industry) stated that the survey is already designed and will be distributed to practitioners in Industry, OPM, and DSS to elicit what should be improved about the clearance process. Ms. Smith stated that OPM has already distributed 150 surveys to the agency's investigators and operations personnel.

g. Mr. Haberkern observed that e-QIP cases are received at OPM without fingerprint cards and release forms, and a large number of e-QIP files received within the last 30 days were waiting for the related paper documents to arrive. Similarly, numerous mail bins at OPM were observed containing paper fingerprint cards and release forms for which no e-QIP file yet exists. The scanning/printing of completed reports of investigation and daily mail dispatch is resource and time intensive for OPM. The group believes this issue can be largely resolved by the implementation of electronic reports transmittal and on-screen adjudication of cases. Mr. Haberkern observed that OPM has begun a program in which completed background investigations are electronically transferred to the U.S. Army Central Personnel Security Clearance Facility (CCF) for adjudication of clearances under its jurisdiction. The program enables the CCF to process cases electronically through their Clearance Adjudication Tracking System (CATS). Mr. Haberkern stated that the working group also identified two Joint Personnel Adjudication System (JPAS) issues. The first was that JPAS cannot access the Agency Use Block (AUB) of e-QIP with the impact that DISCO cannot enter special/extra coverage codes, thus hindering transmission of e-fingerprints. According to Mr. Haberkern, DSS is currently addressing this problem by recoding JPAS to allow access to the AUB. Mr. Pannoni observed that if there was a method to code such coverage initially then the additional work could be accomplished at the same time as the investigation is being run. The second JPAS issue concerned the current use of a single Security Office Indicator (SOI) for DISCO, which results in the delayed mailing of cases to the appropriate CAF for SCI decisions. Mr. Haberkern stated that the problem of such delays will be resolved when DISCO receives SCI authority.

h. Ms. Smith presented several working group observations on third-party issues. The group observed that the National Law Enforcement Telecommunications System (NLETS) successfully provides OPM with an automated direct-check capability to criminal databases in systems from fifteen states and Canada. The remaining 35 states are in various stages of increasing the quality and coverage of their databases to convert to a direct-check capability. Regarding the FBI name-check process, the working group observed that it is a widely dispersed file retention system; only 20% of name checks produced potential hits; the hits themselves indicate little as to what the hit may be and never guarantee an investigation subject match; and geographically separated files may be on the same Subject, but the process for retrieval and review is uneven and time-consuming. Ms. Smith stated that there is an initiative to centralize and automate military records within two years. In general, the

group observed that OPM has found a varying degree of responsiveness by State Bureaus of Vital Statistics. There are different procedures and varying stages of automation, which contribute to delays in obtaining information for investigations. In this regard, there is a potential NLET-type system in planning, but no short-term improvement actions are being taken.

i. A review of ongoing personnel clearance actions was presented by Ms. Smith and Mr. Haberkern on behalf of the working group:

i. Electronic Transmittal of Fingerprints – the process of a contractor submitting fingerprint cards (and/or e-QIP) directly to OPM remains an issue. The working group believes electronic transmittal of fingerprint cards from Industry to OPM is critical to reduction of case completion time. Mr. Haberkern observed that the DSS is committed to resolving this problem. Ms. Kathy Watson stated that OPM and DSS will be forming a team to move forward on the issue.

ii. Electronic reports of investigations – Ms. Smith stated that OPM is making the capability for an electronic report of investigation available to agencies in order to pilot electronic delivery of investigative results. On November 7, 2007, DoD visited the Army CAF to review/evaluate Army's automated case management/adjudication system. Results appear promising and efforts are underway to take advantage of Army's experience in order to develop a common DoD system. Ms. Dillaman stated that electronic delivery will not only shorten transmission times, but also allow for triaging of work through electronic adjudication so that more complex cases can be handled by experienced personnel; and those easily resolved to be more quickly adjudicated. The electronic investigation will be a combination file of data and electronic images. The data or text format elements will be the credit report, the FBI fingerprint report, reports of investigation, and the data from the SF-86. Hard copy reports or inquiries received will be in Portable Document Format (PDF). However, there will be data recorded that will indicate issues cases, which agencies can use in building their electronic adjudication schemes.

iii. Survey of Industry and Government to identify problems/solutions for process improvement – the working group has distributed a survey questionnaire to a representative sample of "participants in the clearance process" (investigators, adjudicators, management staff, and Facility Security Officers). ISOO will receive and collate responses. The working group will analyze completed surveys and make process improvement recommendations to the NISPPAC Chair by January 2008.

iv. An end-to-end metric that reflects the combined fastest 80% of Industry cases (SSBI and NACLC) consistent with the Intelligence Reform and Terrorism Prevention Act (IRTPA) requirement and an

annual Fiscal Year average end-to-end timeliness for all industry cases – the working group will continue to produce these data metrics.

v. JPAS status update regarding the capability for DISCO to enter codes requesting special investigative needs upon case initiation – the working group will continue to monitor progress on resolving this issue.

vi. Clarify and confirm the percentage of initial e-QIP Industry submissions that are rejected by DISCO – if the percentage is found to be greater than 5%, the working group will produce an analysis of the primary causes for the rejections.

j. The Chair commended the members of the working group and the supporting agencies for their efforts. The Chair observed the value of learning what customers are experiencing and the replacement of anecdotes with empirical data; and requested that the working group make a projection for the next six months taking into account accomplishments already made in the investigative arena, the current inventory of cases awaiting adjudications, and initiatives already underway. This projection will be evaluated at the time of the next NISPPAC meeting.

k. ACTION: As briefed to the NISPPAC membership, the Personnel Security Clearance (PCL) Ad Hoc Working Group will analyze survey results obtained from a representative sample of participants in the clearance process and make specific process improvement recommendations to the NISPPAC Chair by January, 2008. Recommendations should identify current and desired states as well as approaches, plans, and timelines for achieving results. The working group will continue to analyze key data points that measure end-to-end clearance processing for industry. In addition, the group will produce a six-month projection for clearance processing timeliness of Industry cases taking into account the current state, progress already achieved in the investigatory arena, and the current inventory of cases awaiting adjudication.

2. **ODAA Ad Hoc Working Group Report** – Mr. Pannoni stated that the Director, DSS, and Director, ISOO, agreed to establish a working group to develop metrics for measuring the timeliness of the end-to-end Certification and Accreditation (C&A) process. The objectives of the group are to bring transparency to the process so that Industry and DSS understand the requirements and responsibilities necessary for the C&A of information systems; and to maximize efficiencies by leveraging Industry's and Government's knowledge and expertise. The work of the group was the subject of a joint presentation by Mr. Stephen Abounader (Industry) and Mr. David Cole (DSS).

a. Mr. Abounader stated that the creation of the group has promoted open dialogue between DSS and Industry. The work of the group provided a catalyst for the resolution of the self-certification issue, the definition of which was promulgated in the October 2007 Industrial Security Letter. In addition, the group has made progress in the creation of a mechanism for data collection that provides insight into the C&A

process.

b. Mr. Cole presented data received from the data collection instrument developed to measure the timeliness of the end-to-end C&A process. Two aspects of the C&A process were presented; (1) plan review and (2) on-site validation of systems against submitted plans. The metrics are a snapshot in time of the end-to-end process from September 1st to October 31st 2007, during which period 174 plans were received, reviewed, and processed nationally. The average time from plan received date until the issuance of an Interim Approval to Operate/Approval to Operate (IATO/ATO) was approximately 50 days nationally across DSS. This may be broken down into the following average times: plan submittal (received by DSS) to plan review – 28 days (Mr. Cole stated that this time needs to be improved and lowered to under one week); time to perform initial review – 13 days; contractor response to comments/questions – 7.5 days (these are responses to DSS queries that arise from the plan's review); and time for decision and issuance of IATO/ATO – 2.5 days. Regarding the 174 plans in question, by October 31st, 50% required changes from Industry and 20% were denied IATO. Mr. Cole stated that the 20% rejection rate is not good, but that DSS is working on areas to dramatically decrease the latter, including the development of plan templates that will promote standardization, which hopefully should be available at the start of the year. The second half of the C&A process is onsite validation, where DSS touches the systems and compares them to the plans submitted. In September, there were approximately 128 visits. 45% of the visits resulted in an ATO granted with no issues. The remaining 55% required some type of comment, change, deviation, or work with Industry onsite. Within this 55%, an ATO was not recommended for 20%. Mr. Cole stated that this percentage is not good and should ideally be under 5%. The remaining 35% involved DSS working with Industry onsite to make corrections and to have an ATO granted.

c. Mr. Abounader stated that the working group will continue to resolve issues and develop process improvements. The maintenance of communications through the working group as a conduit between Industry and DSS is crucial to success in this area. Some of the ongoing action items include the following: DSS will update the ODAA Process Guide to be consistent with the definition of self-certification; DSS will create security plan templates (in this connection, Industry has delivered templates for Master Systems Security Plans (MSSP) and Profiles for security plan template development); DSS will issue additional tools; Industry will evaluate the tools and provide feedback; and the group will work on standard configurations to standardize and thus speed up the C&A process during onsite visits.

d. Mr. Cole covered three additional items in connection with the ODAA. First, in response to Industry queries regarding who would be contacted if there are differences of interpretation, the DSS chain of command should be utilized. The first step in addressing issues should be the Regional Designated Approving Authority (RDAA). An issue raised to the RDAAs is also communicated to Mr. Cole. The issues are then "tabled" within the ODAA to promote consistency. All four of the RDAA positions have been filled. Second, Mr. Cole stated that, through the NISPPAC, DSS requested Industry's assistance in assessing the Electronic Feedback and Automated Plan Template (eFAST), an online system developed by DSS for

submission of security plans. During October, DSS asked Industry to request system accounts in order to interact and develop plans. 167 contractors expressed interest. 137 submitted requests for system accounts. 106 security plan templates were made. About 40 comments were received from Industry. Mr. Cole stated that Industry participation was low in the assessment of the eFAST tool; and that it will be difficult to draw conclusions on the tool due to the low participation. Third, the DSS ODAA has received approval and funding for 25 full time positions, the majority of which will be in the Field as Information Systems Security Professionals (ISSP).

e. Mr. Musser asked Mr. Cole whether DSS would be meeting with contractor security personnel to promote better understandings of the C&A process and thus reduce the number of rejections. Mr. Cole responded that the proper forum would be through the NISPPAC Ad Hoc working group, and stated that he was open to conducting workshops through the group. Once templates, configuration standards, and supporting tools are developed, Mr. Cole stated that DSS staff will be conducting demonstrations for contractors in the future. In the long term, Mr. Cole stated that a training course will be "revamped" that will walk the student through the end-to-end C&A process.

f. **ACTION: The Office of the Designated Approving Authority (ODAA) Ad Hoc Working Group will continue to resolve issues, develop process improvements, and promote communication between Industry and the Defense Security Service (DSS) on the certification and accreditation process for information systems. At the next meeting of the NISPPAC, the group will present a report on specific measurements and improvement of the overall timeliness of the certification and accreditation process, revisions of the ODAA process guide, training efforts, the reduction of deficient System Security Plans (SSP), and the reduction of denials for Interim Approval to Operation/Approval to Operation (IATO/ATO).**

3. **Combined Industry Presentation** – The combined Industry presentation was made by Mr. Musser. Mr. Musser stated that within the last three years substantial change has taken place in the NISPPAC, particularly with the creation of the ad hoc working groups. Mr. Musser expressed his hopes that these positive changes would continue in the future. Mr. Musser welcomed the two new Industry members, Ms. Porter and Mr. Beals.

   a. The presentation focused on the following main areas: JPAS, Personnel Security Clearance Processing, and DIB IA.

   b. JPAS – Mr. Musser stated that in order to amplify the earlier presentation touching upon JPAS, emphasis should be placed on Industry's concern that focus is maintained on this system, even if other systems come online hopefully in the future. JPAS must continue to be maintained and remain viable. Industry desires to enter into the dialogue on solutions regarding electronic fingerprinting and signatures. As the metrics reveal, fingerprinting problems are a major factor affecting turn-around times and causing confusion. Industry welcomes Ms. Watson's recent efforts to resolve the fingerprinting issue and offers assistance. Mr. John Skudlarek (DSS) introduced himself as the DSS Chief Information Officer and responsible for JPAS. Mr. Skudlarek stated that JPAS is fully funded and concerns about JPAS failing are

unfounded. Mr. Skudlarek stated that DSS was successful in obtaining additional funding to ensure its organizational baseline was stable, and that the necessary operational and maintenance funds exist to sustain JPAS. He also stated that, DSS is working aggressively to keep JPAS running and viable. He observed that problems are rapidly addressed, including one which occurred between JPAS and e-QIP several weeks previously. Mr. Skudlarek stated that the decision was made at the Deputy Secretary of Defense level that the new system formerly known as System X, and now as the Defense Information System for Security (DISS), would be developed by the Business Transformation Agency (BTA) under Acquisition, Technology and Logistics (AT&L); and that "DSS will work with BTA as your advocate, as the security community's advocate, to try to make sure that BTA gets DISS right." Mr. Skudlarek stated that he understood that "there will be a series of demonstrations in the next year and that BTA hopes to roll out the first version of the new DISS, probably in '09." He stated that DSS will completely support the BTA effort. Mr. Skudlarek does not anticipate that JPAS will be replaced in the first spiral. Currently, he expects "that JPAS will be in the Field for at least another 4-5 years." Mr. Skudlarek stated that DSS is "working now to make enhancements to JPAS." Some enhancements will support reciprocity. DSS is also working with the DNI Special Security Center to establish an interface with Scattered Castles. He also stated that DSS is working "on the Agency Use Block to enable the coding of the submissions for electronic fingerprints, as well as INS checks and other special coverage codes." Mr. Skudlarek stated that DSS is doing its best to make the JPAS "as viable as it can be while understanding there is a future system to be developed and certain enhancements will not be done until the future system is stood up." Regarding electronic signature, a capability was implemented earlier in the year that allows all applicants "to fax in their signed release forms to marry them up with their submitted e-QIP submission or to scan and upload them." Mr. Skudlarek stated that the acceptance rate for scanning and uploading signed release forms is "over 99%." Mr. Musser asked whether in recent months anyone from Industry had been involved in any of the new processes either with JPAS or with the new system. Mr. Skudlarek stated that the last few months have been "one of flux" with the transfer of the mission from DSS to BTA, and that "we also have a strong advocate on the Personnel Security side, Mr. Haberkern" and "your strong advocates led by Mary Griggs." Mr. Skudlarek stated that "there has been no attempt to exclude Industry." Mr. Skudlarek stated that "the enhancements" being worked by DSS "came out of things like the NISPPAC where we have been paying attention and your voice has been heard and factored in." Mr. Musser stated that previously Industry had a "solid footing into the design and implementation of JPAS" and that "this does not seem to be the case in this new system." Mr. Musser stated that an Industry observer could give some insight into Industry concerns and design criteria which "would help immensely and probably save money in the long run." Mr. Musser stated that this is a suggestion based on the discussion of transparency which has occurred throughout the present meeting and that Industry could provide Subject Matter Experts (SME) without any conflict of interest. Ms. Watson stated that the recommendation would be passed onto BTA. Regarding the fingerprint issue, the Chair suggested that before DSS and OPM come to a final agreement Industry's perspective will be taken into account through the PCL Ad Hoc Working Group. Ms. Watson agreed to the suggestion.

ACTION: DSS and OPM will assure that through the PCL Ad Hoc Working Group the Industry perspective is taken into account before finalization of a solution to the electronic transmittal of fingerprints from Industry to OPM.

c. Personnel Security Clearance Processing – Mr. Musser stated that the previous report from the PCL Ad Hoc Working group addresses Industry's concerns dealing with personnel security clearance processing. Mr. Musser stated that Industry wants the PCL Ad Hoc Working Group to continue working. It has already shown tremendous accomplishments. Although informing them of changes occurring in the PCL process, Mr. Beals stated that Corporate Executive Officers (CEO) are not observing any changes in the timeliness of clearance processing. According to Mr. Beals, if accurate trends can be projected and monitored by the working group, the CEOs may start "backing off from their constituencies." Mr. Musser stated that it is the hope of Industry that the recent personnel security breaches will be seen as aberrations and not as excuses for shying away from clearance processing reforms. The Chair stated that the essence of clearance reform has to involve all parties buying into a risk management approach.

d. DIB IA – Mr. Musser stated that Industry has serious questions whether the DIB IA will be the best solution to the threat. Regarding suitability requirements, it is unclear how personnel will be cleared, who are operating unclassified systems in an unclassified environment and protecting data, which may or may not be Controlled Unclassified Information (CUI). As currently written, a large number of such personnel, who have never held clearances, will have to be cleared. There will also be impacts on physical security involving the protection of the systems where they are located. According to Mr. Musser, Industry is hearing a definition of CUI from DoD, which differs from that being stated by the DNI. Industry hopes that there will be congruence on the definition of CUI, how it must be protected on an electronic system, and what it will cost Industry to provide such protection. Industry operates flat horizontal networks with multi-country connectivity. However, as currently written, Industry will be required to implement on the latter systems safeguarding and protecting requirements similar those for the SECRET level. Eventually when this new Federal Acquisition Regulation (FAR) clause is implemented, there will be an impact on Industry.

e. NISPPAC ODAA Working Group – Mr. Musser re-emphasized that value of the team approach and the problems that can be solved through such an approach's implementation in the NISPPAC working groups.

f. Additional DIB IA Discussion – The Chair stated that Ms. Victoria Morgan, a representative of the Office of the Assistant Secretary of Defense (Networks & Information Integration), OASD(NII), was invited to the NISPPAC meeting. Ms. Rosalind Baybutt (DoD) stated that Ms. Morgan had intended to attend if possible, but was not at the meeting. The Chair inquired whether the NISPPAC should assist in crystallizing issues. Mr. Gregory Torres (DoD) stated that it was not necessary for the NISPPAC to become engaged with DIB IA presently. From an information security perspective, Mr. Torres stated that his office will have the lead for the Department in implementing any national level policy derived from the entire effort.

Mr. Torres has heard rumors that there are concerns regarding the definition of CUI. This will be defined at the national level and implemented by Mr. Torres' office. Consequently, if anyone is hearing that a different direction is being pursued (perhaps from an Information Technology perspective); concerns should be forwarded through the NISPPAC to Mr. Torres' office, which will in turn contact NII so that clarifications can take place. Mr. Musser stated that a single focal point is needed and agreed concerns should be forwarded to Mr. Torres through the NISPPAC. According to Mr. Musser, the matter is complicated by five different working groups on DIB IA and that concise information is needed for planning purposes. Mr. Torres said that his office can examine the specifics of implementing the national decision on information security. The working groups are functioning well. However, if someone is implying what the policy of CUI will or will not be, this type of policy implementation should instead be coming from Mr. Torres' office. Mr. Torres agreed to take back and respond to issues regarding DIB IA raised by Industry during the combined presentation such as suitability; impact on personnel and physical security; as well as defining and segregating CUI.

ACTION: The Industry representatives will submit any specific concerns regarding the Defense Industrial Security Based Industrial Awareness (DIB IA) to the NISPPAC Chair, which will in turn be forwarded to Mr. Gregory Torres, Director of Security (ODUSD(CI&S)/Security Directorate). Responses will be forwarded to the Chair and, as appropriate, provided to the NISPPAC membership.

4. **The Government-wide Implementation of HSPD-12** – The topic was addressed by Mr. David Temoshok (Director, Identity Policy and Management, GSA Office of Government wide Policy).

   a. HSPD-12 has four control objectives: issuance of identity credentials based on sound criteria to verify an individual's identity; identity credentials strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation; personal identity that can be rapidly authenticated electronically; and identity credentials issued by providers whose reliability has been established by an official accreditation process.

   b. There are a number of HSPD-12 milestones. However, one of the most significant is to convert all employees to the Personnel Identity Verification (PIV) standards by October 27, 2008 through the enrollment and issuance of PIV cards to all covered employees and contractors.

   c. Mr. Temoshak stated that the focus of the briefing is on the process for enrollment and issuance of the cards. OMB provides policy and implementation guidance. The National Institute for Standards and Technology (NIST) provides HSPD-12 process and technical requirements. GSA provides government-wide implementation and acquisition assistance; coordinates agency implementation through the Federal Identity Credentialing Committee; develops and tests interface specifications for interoperability; and serves as "Executive Agent for Acquisition" for approving products and services in implementation of HSPD-12. Interoperability of HSPD-12 systems across government is required. Agency implementation is controlled through

the Approved Products List, acquisition controls, and standard interface specifications. GSA is designated to provide shared services and infrastructure for government-wide implementation.

d. More than 16 agencies are implementing their own HSPD-12 infrastructure (Department of Homeland Security, Department of Defense, Department of State, Veterans Administration, Health and Human Services, Department of Education, Department of Labor, Housing and Urban Development, National Aeronautics and Space Administration, Social Security Administration, Environmental Protection Agency, Federal Trade Commission, National Science Foundation, Small Business Administration, Executive Office of the President, and the Federal Housing Finance Board). More than 100 agencies wish to share infrastructure. Shared service providers include: DoD, through the Defense Manpower Data Center, for branches of the military; Department of State for 8 agencies which share international housing; and GSA for the remainder of the government. For GSA, the overall goal is to deploy 225 enrollment stations nationwide and enroll all Managed Service Office customers (800,000+) by October 2008.

e. HSPD-12 requires a personal enrollment encounter with every employee and contractor, where identity is verified and biometric information is recorded including fingerprint as well as facial image. The issuance of the cards requires a second personal encounter.

f. GSA infrastructure covers the enrollment stations nationwide, the establishment of identity accounts, the enrollment of individuals, and the issuance of all credentials. Personally identifiable Information is not stored locally. A complete enrollment package is sent securely to a single database (Shared Service Identity Management System [SSIMS]) and then submitted in turn to OPM. OPM handles background investigations and the FBI criminal history check. The SSIMS waits for adjudication before issuance. HSPD-12 allows issuance of the PIV cards on completion of the adjudication of the criminal history check. PIV cards are flagged for pending adjudications of National Agency Checks with Written Inquiries (NACI) and higher security clearance. The flag remains until a determination is made. A negative determination results in revoking of the account and all credentials. A positive adjudication requires a dynamic updating of the PIV certificate on the card.

g. Mr. Torres asked whether the HSPD-12 adjudicative criteria have been issued. Ms. Dillaman stated that OPM has the lead on the criteria and that their issuance is expected in the near future. Mr. Torres stated that one of the intents of HSPD-12 is to verify an individual's identity and asked whether a method had been found to accomplish this. At present, when DoD conducts background checks, the investigations are performed based on the identity claims of the Subject. Consequently, when a criminal check is conducted, the Department is attempting to find whether a criminal record exists. If the Subject's fingerprints are not on file, this does not verify identity. Internal to DoD, at the Defense Personnel Security Research Center, the Department is attempting to find a way of verifying identity over time based on history. Mr. Torres queried whether there would be a national standard for verifying identity. Mr. Temoshok stated that HSPD-12 creates a standard for identity

verification for the Federal Government which can also be adopted by other organizations. GSA grants requests from States and other entities to adopt NIST standards because such adoption assists in meeting the challenge of identity management by promoting organization around standards. Mr. Temoshok stated that HSPD-12 does not solve the issue, but rather points the way forward to more standardized identity verification and credentials. Mr. Musser asked whether GSA's Public Key Infrastructure (PKI) credential will be adopted by DoD. Mr. Temoshok stated that DoD is implementing the common policy regarding the PIV authentication certificate. Mr. Temoshok stated that he does not know DoD's decisions on the additional certificates (signing, encryption, and management keys).

h. Ms. Lisa Gearhart (Army) stated that there is an Army Working Group attempting to create Army guidance on HSPD-12. Ms. Gearhart stated that she learned that there is an appeals process for HSPD-12 provided for under Federal Information Processing Standard (FIPS) 201. As an observation, Ms. Gearhart stated that Army has not determined how such an appeals process might be handled for contractors. At present, the Army CAF does not adjudicate HSPD-12 suitability, but this is left up to security managers in the field. Ms. Gearhart inquired who will be issuing guidance regarding such an appeals process. Mr. Torres stated that this would be addressed internally within DoD. Mr. Temoshok stated that although there is a requirement in FIPS 201, this does not mean a separate HSPD-12 appeals process from existing personnel appeals. If a decision is made for non-suitability, the Subject in question is simply not enrolled in the PIV program.

5. **The Presidential Guideline 3 Report: Standardize Procedures for Sensitive But Unclassified (SBU) Information** – The topic was addressed by Dr. Josh K. Weerasinghe (Office of the Program Manager, Information Sharing Environment [ISE], ODNI).

a. On October 31, 2007, the President issued the National Strategy for Information Sharing. Dr. Weerasinghe has provided copies to the NISPPAC Chair.

b. Dr. Weerasinghe stated that the proposed CUI framework does not create another classification or a Freedom of Information Act (FOIA) exemption. The subset of information involved is unclassified, but nevertheless needs to be safeguarded. Presently, SBU information is shared according to an ungoverned body of policies and practices that confuse its producers and users. Across the Federal government, there are at least 107 unique markings and over 130 different labeling or handling processes and procedures for SBU information. Inconsistency in SBU policies greatly increases the likelihood of erroneous handling and dissemination of information. Current SBU sharing practices not only impede the timeliness, accuracy, and ready flow of terrorism information that should be shared, but often fail to control the flow of information that should not be shared.

c. The proposed CUI framework stipulates that all CUI will carry one of three markings. Each marking option signals that the material contains CUI and that both safeguarding and dissemination controls apply. There are two levels of protection, "Controlled" and "Controlled Enhanced." There are two levels of dissemination, "Standard Dissemination" and "Specified Dissemination." There are four additional

markings (PCII, CVT, SSI, and SGI) which can be applied within the CUI framework, but are not applied in isolation from the framework.

d. The recommendation made to the President is that the National Archives and Records Administration will be the CUI Executive Agent. The CUI Executive Agent will develop and issue standards based on ISE-wide CUI policy. The Executive Agent will receive the advisory support from a CUI Council, made up of senior-level department and agency representatives, State, local, and tribal officials. The CUI Council will be made up of representatives from participating cabinet-level departments and advisors from state, local and tribal government entities. In addition, the CUI Council will utilize established processes to engage private sector partners. The heads of the participating departments and agencies will be responsible for implementing the CUI Framework standards for ISE-wide CUI policy and ensuring that their agencies comply with the CUI Framework.

e. In October 2007, the CUI report and recommendations were provided to the Deputy Secretaries for concurrence. In general, there was consensus along all the major elements in the proposed framework. Meetings will be occurring to resolve issues. If the recommendations are accepted, the President will issue policy, which will then be followed by implementing regulations to address specific requirements. Mr. Kent Hamilton (Industry) queried whether there would be a suitability requirement. Dr. Weerasinghe stated that if this was requirement, then the matter would have to be addressed through the CUI governance process to include the council and executive agent; and, in such a case, would be established nationally. Mr. Gerry Schroeder (DOJ) stated that CUI markings should not be applied to information that is releasable under FOIA. Dr. Weerasinghe stated that the report precisely defines what can and cannot be CUI. The Chair stressed that the specifics are pending Deputy Secretary-level approval, and will be subject to the President's decision.

6. **Consolidation of CAFs** – The topic was addressed by Mr. Gregory Torres (Director of Security, ODUSD[CI&S])

   a. Mr. Torres stated that Mr. James R. Clapper, Jr. (Under Secretary of Defense for Intelligence) with the support of the Secretary of Defense has directed the Security Directorate to develop a plan for consolidating DoD CAFs as a means of continuing to streamline, with the end goal of obtaining greater efficiencies and consistency throughout the Department. The Security Directorate is obtaining input from those Defense agencies with CAFs and will be creating a strategy for submission to Mr. Clapper.

7. **NISP Signatories Update** – Ms. Baybutt stated that DoD intends to revise Chapter 8 of the National industrial Security Program Operating Manual (NISPOM). There is a national level effort to move the entire government towards the same C&A process, standards, etc. Ms. Baybutt has held discussions with Ms. Sharon Ehlers (ODNI) on this topic. Ms. Baybutt is seeking to start meetings with the Cognizant Security Authorities (CSA). Certain issues need to be addressed such as integrity and availability, which are not covered by Chapter 8. Ms. Baybutt stated that the CSAs will have to make a decision on whether such topics are included in a revised chapter. Ms. Baybutt requested that

such meetings occur under the auspices of ISOO. The NISPPAC Chair accepted the recommendation.

ACTION: The NISPPAC Chair will sponsor meetings between the Cognizant Security Authorities (CSA) to address issues relevant to the revision of Chapter 8 of the National Industrial Security Program Operating Manual (NISPOM). The results of these discussions will be reported to the NISPPAC membership.

8. **Proposed Amendment of the NISPPAC Bylaws and Charter** – Consistent with the Bylaws of the NISPPAC, after prior notification of all members before the present meeting, a motion was agreed unanimously by the membership to accept one amendment of the Bylaws and one amendment of the Charter. These amendments are relevant to Federal Advisory Committee requirements and specified that NISPPAC Industry members are not Special Government Employees. The amended Bylaws and Charter will be posted to the NISPPAC page on the ISOO website.

9. **General Open Forum** – The Chair informed the membership that proposed changes of ISOO Directive No. 1 (32 C.F.R. Part 2001) were being considered and may appear in the Federal Register for public comment. The proposals will not affect Industry except perhaps for a provision governing destruction procedures that will require agencies to use products approved by NSA. However, this will only apply to Industry if the NISPOM is revised to include such a requirement.

10. **Closing Remarks and Adjournment** – The Chair presented ISOO coins to Mr. Beals, Ms. Porter, and Mr. George Ladner as new members; and ISOO Key Awards to Ms. Nichols and Mr. Musser who are departing from the Committee. Mr. Pannoni presented an ISOO Key Award to the Chair in recognition of his retirement as ISOO Director. Retirement presentations to the Chair were also made by Mr. Fitzpatrick, Mr. Torres, Mr. Dennis Hanratty (NSA), Ms. Bridget Ouellette (Navy), Ms. Baugher, Ms. Watson, Mr. Daniel McGarvey (Air Force), Mr. Thomas Langer (Industry), and Ms. Dillaman.

11. **Summary of Action Items:**

    a. The NISPPAC Chair will continue to explore options with the Defense Information Systems Agency (DISA) regarding the extension of Secret Internet Protocol Router Network (SIPRNET) access to Industry partners.

    b. At the next NISPPAC session, the Office of Personnel Management (OPM) and Office of Management and Budget (OMB) will provide an update concerning current efforts to promote reciprocity for suitability determinations to include common adjudication criteria.

    c. As briefed to the NISPPAC membership, the Personnel Security Clearance (PCL) Ad Hoc Working Group will analyze survey results obtained from a representative sample of participants in the clearance process and make specific process improvement recommendations to the NISPPAC Chair by January 2008. Recommendations should identify current and desired states as well as approaches, plans, and timelines for achieving results. The working group will continue to

analyze key data points that measure end-to-end clearance processing for Industry. In addition, the group will produce a six-month projection for clearance processing timeliness of Industry cases taking into account the current state, progress already achieved in the investigatory arena, and the current inventory of cases awaiting adjudication.

d. The Office of the Designated Approving Authority (ODAA) Ad Hoc Working Group will continue to resolve issues, develop process improvements, and promote communication between Industry and the Defense Security Service (DSS) on the certification and accreditation process for information systems. At the next meeting of the NISPPAC, the group will present a report on specific measurements and improvement of the overall timeliness of the certification and accreditation process, revisions of the ODAA process guide, training efforts, the reduction of deficient System Security Plans (SSP), and the reduction of denials for Interim Approval To Operate/Approval To Operate (IATO/ATO).

e. DSS and OPM will assure that through the PCL Ad Hoc Working Group the Industry perspective is taken into account before finalization of a solution to the electronic transmittal of fingerprints from Industry to OPM.

f. The Industry representatives will submit any specific concerns regarding the Defense Industrial Base Industrial Assurance (DIB IA) to the NISPPAC Chair, which will in turn be forwarded to Mr. Gregory Torres, Director of Security (ODUSD(CI&S)/Security Directorate). Responses will be forwarded to the Chair and, as appropriate, provided to the NISPPAC membership.

g. The NISPPAC Chair will sponsor meetings between the Cognizant Security Authorities (CSA) to address issues relevant to the revision of Chapter 8 of the National Industrial Security Program Operating Manual (NISPOM). The results of these discussions will be reported to the NISPPAC membership.