**NATIONAL INDUSTRIAL SECURITY PROGRAM**
**POLICY ADVISORY COMMITTEE (NISPPAC)**

**MINUTES OF THE MEETING**
**(Finalized February 6, 2007)**

The NISPPAC held its 27th meeting on Thursday, November 2, 2006, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, N.W., Washington, D.C. J. William Leonard, Director, Information Security Oversight Office (ISOO) chaired the meeting. The meeting was open to the public.

1. **Welcome, Introductions and Administrative Matters** – The Chair greeted the membership and attendees. Two new NISPPAC industry members, Lee Richard Engel and Vincent Jarvie, were acknowledged. The participation of Ms. Carol Bales (Office of Management and Budget [OMB]) was recognized.

2. **Sensitive But Unclassified (SBU) and Federal Information Security Management Act (FISMA) Update** – The Chair introduced these topics as Old Business from the May 10, 2006 NISPPAC meeting and also provided an update on current related issues. With regard to SBU, in December 2005, the President provided guidelines to the Executive Agencies for implementation of the Information Sharing Environment (ISE) from a terrorism prevention and response viewpoint. One of the guidelines addressed the question of SBU. Under the direction of the Office of the Director for National Intelligence (DNI), the Program Manager for the ISE established an Inter-agency Coordinating Group to address the specifics of the guideline calling for increased standardization in the handling of SBU to meet the goal set forth by the President by the end of the calendar year. The NISPPAC Chair has been asked to serve in an advisory capacity to this inter-agency group and in this role will help represent the perspective of cleared industry supporting the Department of Defense (DoD), Intelligence Community (IC), and Department of Energy (DOE). The overall goal is to create a framework that can be applied to all categories of SBU information. Regarding FISMA, the impact of the legislation on industry was also raised during the last NISPPAC meeting. The NISPPAC industry representatives were to prepare a white paper on this topic. Mr. Tom Langer (Industry) stated that an initial FISMA paper was prepared earlier in the year, but unfortunately further work was not accomplished. As evidenced in contracts, however, there still remains confusion whether FISMA applies to a direct connection by a contractor into a government database or to the holding of any government data by a contractor. There are still issues regarding Personnel Security Clearance (PCL) requirements necessary for Information Technology (IT) 1, 2, and 3 levels, which are still not understood within industry organizations. The Chair recalled that at an April 2006 meeting sponsored by ISOO between the NISPPAC industry representatives and Mr. Glen Schlarman (OMB), the latter requested a paper from industry that would explain

inconsistencies encountered in contracting with agencies. Langer stated that the NISPPAC industry representatives would reinitiate their efforts and produce a final FISMA white paper by December. In connection with this discussion, Mr. Ray Musser (Industry) raised a question concerning the DoD Instruction 5239 that is under draft, which deals with Critical Program Information (CPI). According to Mr. Musser, the instruction may entail the accreditation of systems, including those of contractors which store the latter information, and thus may also be related to FISMA requirements. Discussions are ongoing between industry and DoD (AT&L) on framing the instruction.
**ACTION:** Industry will reinitiate the effort on the FISMA Industry White Paper by December, 2006 The NISPPAC Chair will forward a copy to Mr. Glen Schlarman (OMB).

3. **Combined Industry Presentation (Attachment 1) –** The combined industry presentation was made by Mr. Musser.

   a. **SIPRNET Access –** Industry requests a partnership with US Government agencies to obtain sponsorship for SIPRNET connections to receive threat data. DSS had planned a pilot program, but funding problems prevented its implementation. Several industry partners are willing to explore means of paying for installation of SIPRNET systems into contractor facilities. The driving reason is the asymmetrical counter-intelligence threat that is being faced by industry and government. Government agencies are willing to provide threat information, but lack a means to provide the latter to the field in a timely fashion. In discussion, Mr. Musser stated that funding issues centered on connectivity and initial start-up. Mr. Richard Engel (Industry) stated that there is precedence for industry providing funding for installation. Mr. William Fairweather (DSS) stated that there have been discussions with industry regarding possible funding, but with no substantial results at this time. Mr. Langer stated that the process for industry obtaining SIPRNET access is long and complex. Mr. Musser stated that potential partners for sharing threat data with industry also include the Office of the National Counterintelligence Executive (NCIX) and Federal Bureau of Investigation (FBI).
   **ACTION:** 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.

   b. **Access to Threat Data –** Industry reports that the issues regarding threat data concern whether the right information is being shared with industry and the timeliness with which industry is receiving such information. As an example, Mr. Musser recalled a briefing presented at Aerospace Industries Association (AIA) which communicated outdated information that dealt more with a "brick and mortar Russian threat" vice a more up-to-date asymmetrical threat, which is presently being observed by industry. Mr. Philip Bounds (NASA)

stated that sharing threat information with industry has resulted in useful exchanges that effectively deal with intrusions into information systems. In the ensuing discussion, industry representatives stated that contractors have provided intrusion information such as the signatures of intruders and other indicators to Government customers, only to discover that the information was already known, and that there was no timely regular channel for a mutually beneficial exchange of threat data. The Government's sharing of threat information is often on an *ad hoc* basis and not from centralized points. Mr. Timothy McQuiggan (Industry) emphasized that useful threat data would not only include intrusion information to prevent industry from being penetrated, but also relevant threat information that deals with the increasing trend of companies outsourcing back-office data off-shore. Although data such as travel information and the use of American Express is unclassified, there is a need to provide company decision makers appropriate threat information to deal the effects of such outsourcing.

**c. Fee For Service –** Industry reports that it is necessary that this issue obtain some final resolution in order that the question no longer remains a distraction. The Chair queried Ms. Rosalind Baybutt (DoD) whether there was an active discussion within the Department on the question of charging industry for Personnel Security Clearances (PCL). Ms. Baybutt stated that there was no active discussion of this issue at present.

**d. Joint Personnel Adjudication System (JPAS) –** Industry has concerns regarding funding and resources. Very recently there have been serious issues concerning system availability and operational output. Industry has made JPAS a cornerstone of its operations and now seeks assurances as well as a forward outlook regarding the viability of the system in future years. Mr. Fairweather stated that these concerns would be addressed during his remarks later in the meeting. Mr. Musser raised the following specific issues: data integrity; mandating a system hierarchy and validating the systems inputting data; improvement and updating of training; and addressing recent questions regarding electronic fingerprints and signatures. In addressing questions regarding connectivity between the Clearance Verification System (CVS) and JPAS, Mr. Mark Pekrul (Office of Personnel Management [OPM]) stated that OPM is working with DoD to bring about greater efficiency and described the link between the two systems established through the Personnel Investigations Processing System (PIPS) database. In order to load a PCL into the CVS, there has to be a ping against PIPS, which means, for example, that should an agency wish to load a Top Secret PCL into CVS before the system would accept the latter; the CVS searches the PIPS database for a Single Scope Background Investigation (SSBI) on record. If there is an investigation on record, the PCL will be successfully loaded; if not, it will be rejected back to the agency as an error. Most of the error rejections occur because the agency that performed the investigation upon which the PCL was based (which is not necessarily the agency submitting the clearance) either did not report the

information for inclusion into the database, or reported it under a different term or acronym that was not "SSBI" (so that it did not read). OPM is working towards a next generation CVS which will break the link between CVS and PIPS, making the former much more like a Scattered Castles system, by more purely relying upon the input data received from the agencies and not checked against a database. Agencies will be held to accuracy of the data provided. OPM has stood up a robust well-staffed agency liaison group regarding the need to submit data to CVS. Mr. Fairweather stated that DSS and OPM are working closely together on connectivity issues.

**e. Reciprocity –** Industry understands the Navy's culture wherein the Base Commander's establishes policy for the security of their operations on his installation. Nevertheless, industry wishes to create a dialogue with the Navy aimed at fixing some of the basic issues regarding base access for cleared contractors. Different locations report that cleared contractor personnel are being refused access thus resulting in wasted time and resources. Mr. Ralph Wheaton (Navy) stated that he would address this issue in a separate presentation.

**f. Foreign Ownership, Control and Influence (FOCI) –** Industry reports that there is a trend to solicit SF 328 information when it does not appear appropriate. The Chair stated that this is an agenda item that Joann Saunders (FBI) will be addressing.

**g. Reciprocity, SBU –** As multiple caveats for SBU proliferate, industry is seeking guidance on their simplification and handling requirements.

**h. Chapter Eight –** Industry has made the DSS implementation of the Office of the Designated Approving Authority (ODAA) contained in the newest chapter eight of the National Industrial Security Program Operating Manual (NISPOM), a cornerstone of its operations. Consequently, assurances are now sought regarding funding/resources, which could have a potential affect on company operations. Mr. Fairweather stated that this point would be addressed in the DSS presentation.

**i. PCLs –** Industry continues to work with the Government in order to develop a plan for processing collateral clearances more efficiently and effectively. Industry members participate in many working groups dedicated to clearance problems. Industry participated in the DNI-Special Security Center (SSC) survey and anticipates the results. The Chair noted a special presentation by Kenneth Zawodny (DHS), which was sponsored by ISOO and made the day before the NISPPAC meeting. The meeting underscored that industry needs a clearer understanding of what the requirements are, especially in view of the fact the latter tend to vary from component to component within DHS and are not necessarily consistent. If requirements were known up front, industry would be better equipped to meet them. It also highlights that security

clearance reciprocity is meaningless when there are a myriad of suitability issues, which require 100% completion of forms and conducting investigations to determine staff-like access to buildings, systems, etc.

**j.** The Chair raised the issue of whether OPM exercises a similar oversight role regarding industry as it does with respect to agency suitability determinations for Federal employees. Mr. Pekrul stated that a number of issues are raised by this question including the fact that absent the need for a PCL, there is no mandate in the Code of Federal Regulations or Executive Orders to investigate contractors at all. However, ost agencies do conduct such investigations on contractor employees who have staff-like access. Further, from a security standpoint, it makes sense that similar access necessitates similar investigative requirements. However, this is being done by agencies on a voluntary basis because there is nothing mandating such actions. Mr. Pekrul then added that he is chairing a process at OPM that is reexamining the various policies and regulations that underpin personnel security actions in order to broaden the mandate to include contractors in the non-national security environment, i.e., the same requirements for vetting should be extended to a contractor with staff-like access and identical job positions as a Federal employee. OPM is examining what types of investigations are required and what future suitability criteria should be used across the board. Presently there is a void in policy because when these regulatory documents were framed contractor employees were not embedded into federal organizations to the degree that they are now. Policy is just now catching up to the present environment.

**k.** Mr. Musser reported on metrics gathered for the month of September 2006 by industry independently and immediately prior to the release of the General Accountability Office (GAO) Report (*DoD Personnel Clearances, Additional OMB Actions are Needed to Improve the Security Clearance Proc*ess, September 2006). Industry's internal metrics were consistent within days of the GAO numbers. The industry metrics indicated that for the month of September 83.7% of final Secret clearances were completed outside the goal (on average 332 days to complete), and 96% of Top Secret initial cases did not meet the goal range (on average 478 days to complete). These findings are consistent with the GAO report that showed a period of over one year for initial industry Top Secret clearances. The GAO report was for clearances adjudicated in January and February 2006, and thus covered cases completed in 2005, or early in 2006.

**4. Homeland Security Presidential Directive (HSPD)-12** – The Chair initiated discussion on this topic by introducing Ms. Carol Bales (OMB). The Chair stated that his intention was to ensure a venue for a dialogue as industry experiences implementation issues such as inconsistencies from agency to agency. Such a dialogue is intended to surface issues and obtain their resolution. Ms. Bales stated that OMB chairs an executive steering committee for HSPD-12 which includes

representatives from seven different Federal agencies and addresses various issues such as ensuring interoperability across the Federal Government and working out issues regarding the security clearance process. The Chair offered to consolidate any questions provided by the NISPPAC members and forward them to Ms. Bales. Among the latest policy developments regarding HSPD-12, Ms. Bales stated that OMB will be issuing policy to cover foreign nationals with access to Federal facilities or information systems.

**a.** Mr. Gerry Schroeder (Department of Justice [DOJ]) raised the issue of limited investigative resources available for HSPD-12 and suitability requirements. Mr. Schroeder stated that OMB needs to plan for the impact of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2002 as agencies increasingly devote resources to statutory requirements. Ms. Bales stated that OMB has collected metrics from the agencies on projections for how many additional investigations [National Agency Check and Inquiries (NACI)] will be required for Federal employees and contractors. This information covers the next two years and was provided to the FBI and OPM. The response received from FBI was that based on the metrics provided no negative impact was anticipated. According to Ms. Bales, OPM is in the process of determining of whether additional resources are required. Mr. Pekrul stated that most of the investigations submitted due to HSPD-12, which otherwise would not have been requested, will be on uncleared contractors. As a result, most of these will be almost exclusively NACI investigations, which are field-work neutral investigations and are done by automation. There should be little impact on OPM workload. The Chair pointed out that even though the investigations are automated, the results will have to be adjudicated.

**b.** Mr. Wheaton stated that the following questions need to be addressed in connection with HSPD-12: Who is going to request the investigations for industry and military? Who is going to investigate? Who is going to adjudicate and by what standard? Who is going to provide resources? Who is going to document? Are these decisions going to be reciprocally accepted by all agencies?

**c.** Mr. Langer raised issues of duplicative investigations and the lack of an interim clause under HSPD-12 until a final adjudication, with the potential effect in "sidelining personnel." Ms. Bales stated that if a contractor has already been cleared with a Secret PCL or a NACI, another investigation should not take place. The Chair stated that in examining these issues it was important to make a distinction between three inter-related but separate matters: security clearances to access classified National Security Information (NSI), investigations for Personal Identity Verification (PIV) cards to access facilities or Information Systems (IS), and a suitability investigation that is related to the duties of the position, which can be position-unique.

**d.** Mr. Pekrul stated that the investigation completed for HSPD-12 is investigation for suitability, usually a NACI, but can be higher if an agency so decides. It should be adjudicated according to the suitability criteria (5 CFR 731). As is the case for security clearances, there are different levels of suitability. Each of these levels has its own prescribed investigative requirements, a NACI being the minimal. In any case, it is within the discretion of an agency to determine whether a higher level of suitability, and consequently a higher investigative requirement, is necessitated. Thus, if a contractor with only a NACI needs to work at an agency which requires a higher level of suitability, the additional requirements should be initiated after employment. Mr. Pekrul and Ms. Bales concurred that a current Secret PCL is valid for PIV card issuance.

**e.** The Chair raised the question of whether a Secret cleared contractor employee with a fourteen-year old in scope investigation would require a NACI and/or additional investigations/adjudications if moving to agencies/offices with higher suitability standards. Mr. Pekrul stated that although for government employees the fourteen-year old investigation should be accepted absent a break of more than two years in service (and without any report of significant derogatory information in the case of a break in service of less than two years), the application of this principle to the contractor community is not mandated. Mr. Schroeder stated that there should be consistency between the scopes for clearance and suitability requirements. As an example, Mr. Schroeder stated that it makes no sense to allow someone a Secret PCL for fifteen years without reinvestigation and to access Secret information, the unauthorized disclosure of which could cause serious damages to the national interest, but require additional investigations for entrance into a building.

**f.** **ACTION:** The NISPPAC membership will forward general questions and issues regarding implementation of HSPD-12 to the ISOO staff (patrick.viscuso@nara.gov), which in turn will consolidate and forward the latter to OMB. These questions and issues should be submitted by December 15th.

5. **OPM Update –** The OPM presentation was made by Mr. Pekrul. The following metrics were provided for industry cases; processing times for initial Top Secret SSBIs from date of receipt by OPM to the date of closure were 297 days (February 2004), 258 days (February 2005), 177 days (February 2006), and 198 days (September 2006). Mr. Pekrul stated that the increased number of days in September was associated with additional work load due to the expenditure of "end of the year" fiscal money. For National Agency Check Local Agency Check (NACLC) investigations, processing times were 110 days (February 2004), 167 (February 2005), 141 (February 2006), and 170 days (September 2006). The Chair raised the question of the consistency between the OPM metrics and those of industry. Mr. Pekrul stated that Ms. Kathy Dillaman (Director, OPM) is preparing a response to the GAO report. The GAO metrics account for other periods and activities in addition to

metrics which cover the time from the reception and closure of a case by OPM. Other time periods and activities may include the date that the Subject provides case papers to the processing office, which adds time. The Chair made the recommendation that OPM, DSS, and a designated Industry representative meet to analyze the investigative metrics gathered by industry. The recommendation was accepted by Mr. Musser and Mr. Pekrul.
**ACTION:** The Industry NISPPAC membership will designate a representative to meet with OPM and DSS in order to review clearance completion time statistics compiled by industry. This group will, in turn, report by December 15th to the NISPPAC on any additional insights gained.

**a.** Regarding Periodic Reinvestigations (PR), Mr. Pekrul stated that OPM is striving to meet the mandate of the IRTPA. While the ultimate goals have not yet been met, the decreasing initial investigative times reveal positive trends. Nevertheless, as a result of the issues as discussed earlier by Mr. Schroeder, reinvestigation times are not decreasing at the same rate as initial ones, e.g., while in February of 2004 SSBI PRs were at 303 days, the metric was at 352 days in September 2006. Further, it should be noted that 180 Phased PRs (PPR) were closed in September 2006 at an average of 60 days for completion, and that there are presently 4,961 investigators and record searchers through five companies under contract to OPM.

**b.** With the support contract at Boyers, PA, there are approximately 7,000 contract employees total. The Federal agent staff is currently at 1,435, which includes 90 Special Agents in Charge (SAC) and 90 Investigative Assistants (IA). The remaining personnel are street level investigators. The number of Federal staff is expected to be increased to 1,700 by the end of FY07. Ms. Dillaman intends to continue increasing staff in order to meet workload requirements. The point should be made that OPM is working the issues as strongly as possible, with positive results in some areas, and continuously moving towards meeting the IRTPA requirements.

**c.** Mr. Musser stated that "the delta" being seen from both Industry's and OPM's metrics indicates that there is a process and systems issue that is not related to the application of additional investigative resources. The Chair responded that the meeting of the OPM, DSS, and Industry representatives will prove useful in examining such an issue. Mr. Pekrul stated that while there are issues related to process and systems, there is still a need to obtain investigative resources because of workload considerations; and that both Ms. Dillaman and OPM are committed to meeting the goals mandated by the IRTPA.

**d.** Mr. Pekrul reported that suitability issues are currently being examined by the Security and Suitability Investigations Working Group (SSIWG) which he chairs. There are regulations mandated for Federal Agencies which govern the eight criteria for suitability determinations contained in 5 CFR 731. The

SSIWG is addressing the issue of agency-specific suitability criteria. For example, complete lack of prior drug use is used as a suitability criterion for hiring agents by the Drug Enforcement Agency (DEA), but is not a criterion for other agencies. Such criteria should be taken out of the realm of suitability and segregated into the category of qualifications with the idea of promoting reciprocity among agencies regarding suitability. The working group is seeking to engage Chief Human Capital Officers with the aim of having such issues resolved as qualifications before the stage of an investigation for suitability. In addition, the SSIWG is making draft revisions to 5 CFR 731 that clarify the suitability criteria and make appropriate additions, e.g., financial responsibility, loyalty, etc. The goal of the SSIWG's work is to bring suitability and national security considerations into closer alignment, so that there are similar levels in each and investigations are more clearly "passable" between the two. The SSIWG is working in harmony with the DNI-sponsored Research Working Group and National Research Advisory Group which are examining the national security investigative process and standards.

**e.** The Chair noted that regarding suitability there is tremendous value to be derived from transparency so that even if there is a diversity of criteria being applied, industry's knowledge of such requirements in advance would promote a greater capability of more efficiently supporting government agencies. In response to the Chair's question concerning available resources to learn such requirements, Mr. Pekrul stated that he would be willing to discuss the issue personally with industry and suggested a survey of basic documents such as 5 CFR 731 which sets forth the Government's suitability program. A training course dealing with suitability adjudication is available through the Graduate School of the US Department of Agriculture. Mr. Pekrul also suggested that industry representatives visit OPM's facility at Boyers, PA to discuss suitability with personnel who specialize in the subject. The Chair recommended as an action item that OPM provide sources and products to be posted on the National Industrial Security Program (NISP) section of the ISOO website. The recommendation was accepted by Mr. Pekrul.
**ACTION:** OPM will identify resources, websites, products, etc. to ISOO staff (patrick.viscuso@nara.gov) regarding suitability issues and guidance appropriate for industry in order that these are posted to the NISP section of the ISOO website as a reference for industry.

**f.** Discussion took place regarding contractors who do not require a PCL, but strictly a suitability determination to access an installation, e.g., a trucker or gardener, who meets the industry standard for driving or lawn care. Ms. Shannon Morrison-Walters (OPM) stated that such a determination would be an agency risk-based decision, e.g., the issuance of PIV cards to drivers. The same process would be followed as for other contractors and Federal employees. The Chair stated that the adjudication of issues would be different

from agency to agency and position to position. Ms. Pekrul stated that there is a provision in HSPD-12 implementation guidance that mirrors the suitability guidance in that if the Subject is in a low risk position and the access is going to take place for six months or less, then there is no obligation to investigate or issue a PIV credential.

**g.** Regarding the employment of electronic releases, Mr. Pekrul discussed the potential difficulties for field agents using electronic signatures to obtain cooperation from entities until the latter technology obtains public recognition. In terms of electronic fingerprint cards, many agencies are moving to live-scan electronic submission. At present, when they are received in mailed hard copy, there is a match-up procedure and often attachments arrive well in advance of the e-QIP submission, particularly since the former are undergoing checks through the submitting agency before coming to OPM. The mailed materials will be held in abeyance for a stipulated period and in turn, OPM will contact the agency involved before returning fingerprint cards or releases. In other cases, eQIP submissions will be received in advance of the fingerprint cards and releases, which will set up another delay in the process. The best solution is complete electronic submission where releases can be scanned and attached, with submissions taking place all at once. In answer to the question as to why fingerprints need to be resubmitted, Mr. Pekrul stated that the latter are actually not required for the SSBI-PR by the national investigative standards, even though agencies still continue to collect them as part of the PR process. The Chair inquired what can be done presently to improve the process (particularly since industry is now using eQIP) with regard to attachments, releases, and fingerprint cards. Mr. Pekrul stated that OPM is willing to work this issue with the concerned parties to make the process more efficient. The Chair recommended that the issue be worked by DSS and OPM regarding the attachment of releases by industry when submitting using eQIP.
**ACTION:** OPM and DSS will provide feedback on the electronic attachment of releases by November 14th to the NISPPAC, and on options and alternatives regarding fingerprints, including the use of US General Services Administration (GSA) service centers or other alternative sources, by the end of the calendar year.

6. **Submission of the SF 328 –** An overview of the FBI risk management process in relation to the submission of the SF 328 was presented by Ms. Joann Saunders (FBI). In March 2005, a Director of Central Intelligence Directive (DCID) 7/6 was issued that required the Intelligence Community (IC) to employ a common methodology for conducting risk assessment on contractors who do business with the community. In October 2005, the FBI began implementing the DCID through contractual standards. The FBI made the decision that the largest threats were associated with access to classified information and critical assets. Thus, it was determined that FBI's contractual standards would be applicable to services that required access to classified information or the procurement of critical assets, which were identified information

technology hardware, software, telecommunications, and audiovisual equipment. Consequently, from October 2005, FBI began to place risk assessment clauses into contracts dealing with the latter. The clauses stipulate that the Bureau will conduct risk assessments on vendors to determine whether such contracts are in the best interest of the IC. Two items required for submittal by contractors in the risk assessment process are the Standard Form (SF) 328 and the Key Management Personnel (KMP) listing. If the SF 328 is not dated within one year of the procurement, then there is language within the standard which offers an option for the corporate official authorized to certify the SF 328 to submit a letter attesting that the information contained in the latter form remains accurate. The information being submitted is used for a whole contract review including such elements as FOCI, criminal, financial, personnel, counterintelligence, and performance aspects of that particular vendor. This submission and review is based on an IC requirement. Within the standards, a recent revision is that if the contractor has already provided a SF 328 and there are no changes, the authorized official can submit a letter stating that the form has already been forwarded in conjunction with a previous procurement. In consequent discussion, Ms. Saunders stated that this is a common methodology in the community and may be characterized as "centrally located." When the FBI conducts a risk assessment, an evaluation is stored in a database utilized by the rest of the IC. Ms. Saunders stated that this database is queried for current reviews. Mr. Musser stated that a FBI contracting officer is requiring the resubmission of forms under all circumstances including those in which information on the SF 328 has not changed, but was unable to provide specifics regarding the cases in question. Ms. Saunders stated that this process did not imply that the DoD FOCI adjudication was insufficient, but rather that FBI was seeking information versus FOCI adjudication or eligibility. Ms. Baybutt stated that the SF 328 is a government form designed for a specific purpose and use by the four Cognizant Security Agencies (CSA). The Chair stated that the issues involved concerning companies appear to mirror discussions regarding personnel suitability. The company may be cleared, but the determination is being made whether it is suitable for a particular procurement.
**ACTION:** The NISPPAC Chair will hold discussions with the Special Security Center (SSC) to determine the impacts on the NISP of Intelligence Community requirements associated with DCID 7/6, especially the submission of SF 328s for threat assessments associated with classified procurements. The NISPPAC Chair will provide assessments and recommendations to the NISPPAC membership within the next few months.

7. **I-9 Issue Briefing (Attachment 2) –** A briefing was presented by Mr. Ralph Wheaton (Navy) on the submission of the Form I-9, Employment Eligibility Verification, for Navy facility access. Mr. Wheaton stated that an issue was raised in June 2006 regarding the requirement. There is nothing in official Navy security policy that requires the viewing of such forms before the granting of access to a facility. A Commander Fleet Forces Command (COMFLTFORCOM) message issued in January 2006 stated that a significant increase in illegal aliens/undocumented workers being granted access to sensitive facilities was raising force protection/anti-terrorism issues and resulting in a need for a common approach.

In this message, the Form I-9 was viewed as a tool to verify that visitors had been screened for citizenship or legal residence. The on-site verification of the I-9 was to be required before issuing access documents. Contractors were already required by law to complete the Form I-9. Mr. Wheaton stated that the I-9 procedure does not require the creation of new processes/documents. In response to complaints, an email was sent out the same commands that received the fleet forces message, which stated that a valid visitor certification or JPAS clearance verification was also acceptable. There are 2.3 million visitors to Navy facilities on a weekly basis, and although there may have been some misunderstandings, only a small percentage is being denied access. Also, in response to these kinds of problems, guidance was posted on the Navy security website (www.navysecurity.navy.mil). The commands are operating under Title 50, USC, Internal Security Act Requirements and DoD Instruction 5200.8 (Security of DoD Installations and Facilities). COMFLTFORCOM and the Navy Judge Advocate General (JAG) determined that there are no prohibitions against using the Form I-9 for screening personnel. The tool standardizes command policies. Other solutions and tools are solicited.
**ACTION:** Specific US Navy base access (Form I-9) issues should be forwarded directly to Mr. Ralph Wheaton, Head, Industrial and Technical Security Branch, Office of the Chief of Naval Operations (N09N2), Washington Navy Yard, Building 111, Washington, DC 20388-5380, email: ralph.wheaton@navy.mil , telephone: (202) 433-8860, fax: (202) 433-8849. Mr. Wheaton will in turn update Ms. Rosalind Baybutt, Deputy Director for Industrial Security (OUSD[I]/ODUSD [CI&S]). Broader issues and questions should be provided to the NISPPAC Chair, which will then be consolidated and provided Federal agencies, as appropriate.

8. **DSS Update –** *The following remarks were read by Mr. William Fairweather, (Acting Deputy Director, DSS):* **"**Good morning and thank you for the kind introduction. I'd like to thank the NISPPAC and the ISOO for the opportunity to speak this morning. I'm Bill Fairweather, Acting Deputy Director of the Defense Security Service, DSS. The Acting Director of DSS, Kathy Watson, wanted to be here this morning, but she has been called to another meeting so I am here in her place. But you should know that the NISPPAC is very important to Kathy Watson and she views the NISPPAC as an important partner in national security. As you know, our mission at DSS is to oversee and ensure the protection of national security assets in industry. We take our mission very seriously because we know that the security of the United States depends on it. I'd like to share with you some of what Kathy Watson and I have been doing since our arrival at DSS last spring. We have been assessing how well DSS is meeting its missions and spending much of our time on the agency's budget and finances. DSS is facing many challenges and we're committed to finding both short and long term solutions as we look toward future improvements. In the past six months, DSS has developed a six point plan for improvement. That plan is ongoing and I'd like to tell you about it:

***Organizational Structure.*** Historically, DSS has not had the human or financial resources to properly conduct its mission. To accommodate critical short-term needs, we augmented our staff with 18 personnel from throughout the DoD intelligence

community for six months. The Director commissioned a manpower survey to determine the appropriate number and mix of personnel for DSS and I expect to receive the results of that study in November. The Director plans to act according to the recommendations in the study.

***The FY06 Budget.*** DSS had a successful fiscal year-end close out. Due to funding shortfalls in FY06, DSS received $80 million supplemental funding in support of the DSS PSI mission for industry.

***The FY07 Budget.*** DSS has worked closely with the Under Secretary of Defense (Intelligence) and the DoD Comptroller to resolve the issues surrounding the DSS budget for FY07 and we have received tremendous support from both offices.

***Personnel Security Program Improvement Plan.*** DSS has coordinated with the Under Secretary of Defense (Intelligence) to develop a *Personnel Security Program Plan*. This plan will completely overhaul the PSI process.

The operational imperatives of the new program will be quality assurance, responsiveness, reliability and reciprocity.

The plan includes:

Training for security managers on JPAS; Establishing standardized training and certification for investigators and adjudicators.

The establishment of a clearance oversight office to oversee and analyze PSI projections, link requirements with funding, audit and resolve billing issues and conduct liaison with DoD components;

Complete electronic requests for investigations. DSS will be able to send release forms electronically in November. I anticipate receiving funding to purchase and deploy fingerprint equipment and modify JPAS to accommodate this;

Staffing the DSS Clearance Liaison Office. This office will coordinate and sponsor overseas investigative requirements, maintain the investigative files repository and identify and coordinate unique critical requirements for DoD.

Establishing a case tracking system for adjudicators to use.

Working with the community and NSC to update the national investigative standards to support issue-tailored investigations and integrate emerging technologies into the personnel security process.

Standardizing CAF functionality to all DoD CAFs can grant and deny clearances and make SCI determinations;

Implementing electronic screening and adjudication for DoD PSIs; and
Amending the national investigative standards for periodic reinvestigations so that these can be accomplished aperiodically and be driven by events, using an automated records check tool.

We have spent a lot of time and energy on this plan. We are very proud of it and happy to report that we have the full support of Dr. Cambone, the Under Secretary of Defense for Intelligence. We are currently working with our DoD colleagues as well as our business partners in the intelligence community, OMB, OPM and the Hill to obtain support and funding for this program. We will keep the NISPPAC and the ISOO fully informed as our implementation plan unfolds.

***Realistic Expectations.*** Having said that, DSS must manage expectations within DoD, the 23 non-DoD federal agencies that use DSS' industrial security services, and the defense industry as to what DSS – at its current size and budget - can realistically achieve. It will take time and considerable resources to fix systemic problems that have taken so long to develop. Be fully assured however that we are taking very deliberate steps to improve the PSI process end to end.

***DoD Inspector General (IG) Requested Audit.*** DSS requested that the DoD IG conduct an audit of DSS to determine what business practices and procedures may have led to the current financial situation. This audit is in process and I expect to receive the report in December.

In addition to the six point plan, I want to tell you some more about what we are doing to improve the PSI process. DSS has developed a renewed and reinvigorated relationship with the Office of Personnel Management (OPM). The DSS-OPM Partnership Plan for Dialogue, Innovation, and Progress brings DSS and OPM teams together on many fronts with the overall goal of improving the PSI process. This partnership has proved most critical in technological and financial improvements to the PSI process. For example, a DSS/OPM team worked closely to ensure that OPM's eQIP form was made compatible with the DSS JPAS and DISS systems for information sharing DoD-wide.

DSS has also teamed with OPM and the DoD adjudicative community to gather and analyze metrics that reflect whether or not desired quality is being obtained in the PSI process. I plan to oversee this effort closely to ensure we receive the investigative products we need to make informed adjudicative decisions.

I realize that improvements have been promised in the past. I know that those improvements have been slow to materialize if they materialized at all. But I can assure you that the Department is committed to making necessary changes to improve the PSI system. The senior management positions at DSS are now open as permanent executive billets and having stable leadership will ensure that there is accountability for the state of DSS. I feel confident that we will have a better system than we've had in the past.

DSS and the Department recognizes that the time for change is now, and we are working to make that happen.

We will look to the NISSPAC and to ISOO to help us. We certainly value your input and I trust that it will continue. Thank you for your kind attention, and again for the invitation to speak this morning."

8. **DoD Update –** Ms. Rosalind Baybutt (DoD) stated that fee for service is being explored in a preliminary manner regarding non-DoD agencies paying for Industrial Security investigations. Any decision will have to be based on sufficient study and coordination with all agencies involved. Regarding the SF 328s, productive discussions occurred between the DoD and the Department of Energy with the aim of sharing the same database. In addition, Ms. Baybutt stated that the utility of the NISPOM Supplement, DoD 5220.22 M Sup 1, (which is the addendum to the NISPOM dealing with SAP, SCI, and Restricted Data [RD]) is under study, and requested the assistance of the Chair in obtaining feedback from the NISPPAC membership regarding whether the document has value to agency members and whether industry members observe the Supplement in contractual documents. **ACTION:** Ms. Baybutt requested that the NISPPAC government membership provide input on the utility of the NISPOM Supplement (DoD 5220.22 M Sup 1) to the NISPPAC Chair (patrick.viscuso@nara.gov). She also similarly requested that NISPPAC industry membership provide input on whether the latter document is referenced in government contracts.

9. **NISP Signatories Update –** Ms. Gerayln Praskievicz (DOE) stated that a reorganization has taken placed within DOE merging the Office of Security with Office of the Departmental Representative to the Defense Nuclear Facilities Board and the Office of Environmental Health and Safety. The new organization is the Office of Health, Safety, and Security. Mr. Brian Dunbar (CIA) stated that the new management of the Agency is extremely supportive of security. Information Security functions have been combined into the Agency's Industrial Security division with the result that facility accreditations as well as Information Security certifications and accreditations are handled jointly.

10. **Closing Remarks and Adjournment –** The Chair acknowledged the service of two departing NISPPAC members, Thomas Langer (Industry) and P. Steve Wheeler (Industry).

11. **Summary of Action Items:**

    **a.** Industry will reinitiate the effort on the FISMA Industry White Paper. The NISPPAC will pass a copy to Mr. Glenn Schlarman (OMB).

    **b.** The Chair, on behalf of NISPPAC, will explore options with the DISA regarding the extension of SIPRNET access to industry partners, and report back to the

NISPPAC membership.

**c.** The NISPPAC membership will forward general questions and issues regarding implementation of HSPD-12 to the ISOO staff (patrick.viscuso@nara.gov), which in turn will consolidate and forward the latter to OMB. These questions and issues should be submitted by December 15th.

**d.** The Industry NISPPAC membership will designate a representative to meet with OPM and DSS in order to review clearance completion time statistics compiled by industry. This group will, in turn, report by December 15th to the NISPPAC on any additional insights gained.

**e.** OPM will identify resources, websites, products, etc. to ISOO staff (patrick.viscuso@nara.gov) regarding suitability issues and guidance appropriate for industry in order that these are posted to the NISP section of the ISOO website as a reference for industry.

**f.** OPM and DSS will provide feedback on the electronic attachment of releases by November 14th to the NISPPAC, and on options and alternatives regarding fingerprints, including the use of US GSA service centers or other alternative sources, by the end of the calendar year.

**g.** The NISPPAC Chair will hold discussions with the SSC to determine the impacts on the NISP of IC requirements associated with DCID 7/6, especially the submission of SF 328s for threat assessments associated with classified procurements. The NISPPAC Chair will provide assessments and recommendations to the NISPPAC membership within the next few months.

**h.** Specific US Navy base access (Form I-9) issues should be forwarded directly to Mr. Ralph Wheaton, Head, Industrial and Technical Security Branch, Office of the Chief of Naval Operations (N09N2), Washington Navy Yard, Building 111, Washington, DC 20388-5380, email: ralph.wheaton@navy.mil , telephone: (202) 433-8860, fax: (202) 433-8849. Mr. Wheaton will in turn update Ms. Rosalind Baybutt, Deputy Director for Industrial Security (OUSD[I]/ODUSD [CI&S]). Broader issues and questions should be provided to the NISPPAC Chair, which will then be consolidated and provided Federal agencies, as appropriate.

**i.** Ms. Baybutt requested that the NISPPAC government membership provide input on the utility of the NISPOM Supplement (DoD 5220.22 M Sup 1) to the NISPPAC Chair (patrick.viscuso@nara.gov). She also similarly requested that NISPPAC industry membership provide input on whether the latter document is referenced in government contracts.