NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

MINUTES OF THE MEETING
(Finalized/Approved January 6, 2006)

The NISPPAC held its 25th meeting on Tuesday, November 15, 2005, 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 is open to the public.

1. **Welcome Introductions and Administrative Matters –** The Chair acknowledged the service of departing NISPPAC members Jim Linn and Diane Raynor. The participation of Keith Backman (ODNI) in the meeting was also recognized.

2. **The membership officially approved the May 10, 2005 NISPPAC Minutes**.

3. **National Industrial Security Program (NISP) Directive Update –** Greg Pannoni (Associate Director, ISOO) presented a NISP update based on an outline and presentation distributed to the membership (Attachment 1). The Directive clarifies NISP roles and responsibilities. Its publication in the Federal Register for a thirty-day public comment period is expected shortly, with ultimate finalization most likely by the end of the year. The main points presented included: delineation of the ISOO Director's responsibilities, ISOO review of Agency implementing regulations, ISOO monitoring of the NISP, the coordination process for changes including deviations from national safeguarding requirements, CSA responsibilities for oversight, DoD responsibilities as the Executive Agent, and agency inclusion of security classification requirements in classified contracts as well as ensuring agency personnel receive appropriate education/training.

4. **Reciprocity –** Based on recommendations from the Reciprocity Working Group to obtain high level data from industry on how well reciprocity is being honored, J. William Leonard introduced a discussion on draft procedures for submitting such information to ISOO (Attachment 2, "Reporting Perceived Unauthorized Exceptions to Reciprocity"). The Working Group recommendations are still subject to change since they have not been officially finalized. The NISPPAC helped develop principles for reciprocity in summer 2004, which were eventually expanded government-wide, after having been approved by the Policy Coordinating Committee (PCC) that is responsible for personnel security issues under the National Security Council (NSC). Those principles are now official government-wide to include industry. The principles, statutory language of Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) that address security clearance issues, and Executive Order 13381 are being used as a base-

line by the Working Group to measure how well the government is honoring reciprocity. The specific proposal is to ask industry to track how often they are requested to submit personnel security questionnaires and whether there is a perception that the reciprocity standards are being violated. It should be emphasized that these are perceptions and there may be "false positives." For example, subjects may be unaware of waivers/exceptions upon which SCI access has been granted; and thus, this may result in an incorrect perception that reciprocity is not being honored when another agency, which is not obligated to accept the same risk, does not allow the clearance transfer to occur. Although granted that the data may be imperfect due to such perceptions, the information will be useful in tracking high level trends and in understanding the degree of policy implementation. Rosalind Baybutt (DoD) questioned why the survey does not include information on which government agencies are perceived as not implementing reciprocity. Mr. Leonard responded that the intent is to keep the survey simplified and not a substitute for processes to seek relief on transactional issues, e.g., those resolved between contractor and government agency. The aim is to obtain a broad view of trends, rather than the granularity of fixing individual transactions. Mr. Leonard proposed that the industry associations determine who will be the reportees and consolidate the reports. The data could be reported to ISOO or OPM. Thomas Langer (NISPPAC) proposed that six or seven large contractor users of SAPs and SCI provide the information on a monthly basis to ISOO and report trends at the next NISPPAC meeting based on the data. Mr. Leonard emphasized that the key to the data collection is that it can be defended as a representative sample. It was decided that government and industry would communicate with ISOO by the end of the week on whether to proceed with the survey, to include the suggestion of other metrics.

5. **Databases -** During the ensuing discussion, Rick Hohman (SSC) stated that Scattered Castles currently includes waiver/exceptions from some IC agencies and will eventually contain JPAS waivers/exceptions. William Marosy (OPM) stated that the consolidated database is being built based on inputs from the Intelligence and collateral communities to include such information as types of polygraph, waivers, and other data fields. Steve Wheeler (NISPPAC) stated that there should be a tracking mechanism for the SAP environment, which records accesses and allows individuals to have their clearance transfer from one program to another, similar to the SCI community. From a Reciprocity Working Group perspective, Mr. Leonard, stated that it was acknowledged that there are some sensitivities involved in recording all of the programs that an individual might have had access to. Consequently, the focus of the Reciprocity Working Group was on the attributes that programs tend to consider, namely, the polygraph and non-U.S. citizen immediate family members. Whether the individual was read into a SAP or not, these two data fields will be centrally available. In this way, if a SAP had these access requirements, this information could be obtained and a determination rendered, without new forms or investigations. This is similar to what DoD has been doing by designating individuals as "SCI eligible."

6. **Combined Industry Presentation (Attachment 3):**
   - Mr. Langer reported progress in the work of the "Chapter 8" Working Group, which has concentrated on issues surrounding accreditation timelines with the Defense Security Service (DSS), the Cognizant Security Agency for DoD programs, and has produced an approved implementation scheme.
   - Regarding the Sensitive But Unclassified (SBU) question, Mr. Langer stated that a letter from the NISPPAC Industry representatives was sent on November 10, 2005 to Mr. John Russack (Program Manger for the Information Sharing Environment, ODNI). The letter requests a dialogue with his office for the aim of establishing one national standard on handling and marking SBU; designation of personnel by agency who can establish requirements; and training for those designated officials (Attachment 4). Mr. Langer reported that the number of designations and requirements for SBU continue to multiply and that these are becoming burdensome, particularly since they are inconsistent and appear arbitrary. The largest part of OPM's background investigations are unrelated to access for national security information, and are in fact drawing scarce and stretched resources away in order to make suitability determinations for a variety of programs established at individual agencies for SBU. Further problems with security clearance processing by OPM will be seen if SBU and Federal Information Security Management Act (FISMA) standards are not rationalized; and Position of Trust/Suitability Determinations continue to increase.
   - Mr. Wheeler reported on a concern raised during the May 10, 2005 NISPPAC meeting concerning the lack of a means to verify status and background for immigrants employed at contractor facilities. Since this meeting, the NISPPAC Industry members learned of an employment verification pilot program under the Systematic Alien Verification for Entitlements (SAVE) Program being operated by DHS. This pilot program allows participating employers access to a Verification Information System (VIS) database in order to verify employment authorization for all newly hired employees. There are restrictions associated with the program: no verification prior to hiring or completion of the I-9 process; no use for pre-screening; and no use for re-verification of employment eligibility. U.S. Immigration and Customs Enforcement (ICE) is active in apprehending illegal workers at contractor facilities, most of whom are themselves independent contractors. Significant numbers of independent contractors are performing construction and maintenance work at sensitive critical infrastructure and defense industrial base facilities. Resident aliens ("green card" status) are being used as knowledge workers by industry. The VIS assists industry, but does not address the preponderance of the problem. Industry is proposing to work proactively and open a dialogue with DHS to help expand the automated resources available to validate the authenticity of alien documentation for all immigrants directly employed or working as independent contractors within contractor facilities.
   - Mr. Langer reported on the FISMA interim rule to the Federal Acquisition Regulation (FAR) that was effective September 30, 2005 with comments due

November 29, 2005. The rule requires agencies to implement IT security rules and consult with IT security professionals on purchase of information system products. The rule also requires that contractors are held to the same information system security standards as government employees. The main industry concerns are centered on agency definitions of IT security standards, agency definitions of SBU, and the extent of agency authority over contractor proprietary systems housing government information. Problems are already developing with additional burdensome government inspections of contractor information systems based on inconsistent standards. There are a variety of authorities cited including contract modifications. Industry is coordinating comments for submission by the November due date.

7. Discussion and Action Items:

- SBU – Mr. Keith Backman (DNI) outlined the responsibilities of the Program Manager to create an Information Sharing Environment. The DNI has been working across the government with the White House and the Homeland Security Council to create guidelines on information sharing, to include SBU. Last week, DHS initiated a working group to also examine SBU. John Young (DHS) reported that this working group under Sigal Mandelker is examining the question at the federal level and has taken an initial step of a data call regarding the designations for this information, the protections required, and their statutory/regulatory basis. Mr. Langer reiterated industry's concerns regarding the volume of SBU designations and lack of consistent standards. Mr. Leonard emphasized that the issue can be framed in terms of information approved for public release and that which is not. Gerry Schroeder (DOJ) responded that this may oversimplify the question and that markings are being added to information to prevent mandatory disclosure. Consequently, there is a need for a national standard to prevent such abuse. ACTION: Mr. Backman proposed that the NISPPAC direct an email to him which frames its proposed representation to the DHS working group, and that his office will coordinate with the latter. Mr.Young stated that he will work with the DHS working group leadership to determine its timelines on the inclusion of the private sector as well as States and local governments.
- Position of Trust Suitability Determination – Ms. Baybutt stated that DoD will reject suitability determination background checks within the Department for individuals already granted DoD Personnel Security Clearances (PCL). Mr. Marosy stated that when OPM established their staffing numbers, these took into account suitability and national security workloads. As reported to Congress, 8,000 investigative FTEs were estimated to meet the latter requirements. This number has been met in order to reach the time limit goals of IRTPA, which mandates that by December 2006 OPM must complete 80% of security clearance granting investigations within 90 days. OPM expects to meet this timeliness requirement. Efficiencies are being realized with the combination of former DSS resources. CFR 731, 732 cover in extensive detail what constitutes a security vs. suitability investigation. Mr. Schroeder responded that a better match between suitability and access to classified

information would be helpful for the purpose of extending reciprocity beyond the confines of the security clearance world. The chair of the PCC has asked the Personnel Security Working Group (PSWG) to examine this issue. Recognizing the OPM equities that OPM has in the suitability process, the PSWG will be creating a working group to address such questions, which OPM has already agreed to chair. Mr. Leonard stated that one of recommendations of the Reciprocity Working Group (in terms of the instructions and guidelines that OMB will be promulgating pursuant to EO 13381, "Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information," with respect to reciprocity) is to try addressing this issue in part, and in essence inform agencies that while we need to acknowledge agencies' prerogatives and authorities to implement unique suitability requirements, to make certain when agencies issue their additional but not duplicative suitability requirements that they are not going back and revisiting any of the underlying issues, which have been already addressed from a security clearance point of view.

ACTION: As a follow-up to OMB's issuances on vetting for SBU positions, Mr. Leonard proposed sending an ISOO letter to all agency heads reminding them of the NISP as well as the investigations conducted and the clearances granted to contractors under the latter program, which may satisfy any additional requirements. The letter will also recommend that before initiating an investigation on a contractor, who claims one has already been conducted under the NISP (including also IC and DOE programs), the agency will verify this information. The letter will provide sources where the verification can be obtained.

- DHS/ICE – **ACTION**: Mr. Young offered to coordinate with the NISPPAC Industry members on this issue.
- FISMA Interim Rule – Industry and government members expressed concerns regarding potentially numerous, inconsistent, costly and burdensome requirements being levied by various government activities on unaccredited systems used at contractor facilities for unclassified information. These requirements imposed on the electronic environment are connected with those also being levied on content (SBU) and personnel (suitability determinations). There is confusion and uncertainty regarding how the FISMA provisions will be imposed.

  ACTION: Mr. Leonard proposed to broker a meeting between NISPPAC representatives and OMB to promote understanding and initiate dialogue.

8. **Access to Government Facilities and Information Systems –** Kimberly Baugher (DOS) introduced discussion of the issuance of Personal Identity Verification (PIV) credentials and Interim Secret PCLs (Attachment 5). FIPS-201 and OMB M-05-24 require that favorable fingerprint checks be completed prior to the issuance of PIV credentials. This presents a problem since personnel are granted Interim Secret clearances by DISCO while their fingerprint results pending. The problem for DOS is that they do not wish to initiate a duplicative fingerprint check for Interim Secret-

cleared contractors working on-site or deny badges for Interim Secret-cleared contractors. Mr. Marosy stated that the Requirements Working Group for Clearance Verification System can consider the inclusion of a data field for fingerprint checks of investigations in process and that DOS personnel are members of this group. Ms. Baybutt and Thomas Martin (NRC) discussed technical and process improvements that are expected to improve fingerprint check times.

9. **OPM Update –** Mr. Marosy stated that the use of eQIP has been a success in substantially reducing the number of rejected PCL questionnaires, but benefits still need to be realized because attachments are being submitted in hardcopy form by fax or mail (and afterwards have to be matched manually with the electronic form). The attachments should be scanned and submitted electronically. At the same time, OPM is also being delayed by waiting for fingerprint cards, a problem that could be resolved by using Live Scan. Another problem being encountered is the submission of attachments without a request for investigation. In the case of DoD due to volume, OPM will hold the attachments for thirty days, rather than fifteen, periodically reviewing for a case opened in eQIP, before returning them to a submitting office, which in most instances is the Defense Industrial Security Clearance Office (DISCO). Consequently, this means most of the cases involved are from industry. Scanning would bring about a substantial improvement (Ms. Baybutt requested information on scanning attachments from Mr. Marosy. Mr. Marosy stated that he would provide this information, which he stated was previously made available to DoD). However, there is also an issue concerning JPAS. eQIP cases are bridged from JPAS into eQIP. JPAS does not have a mechanism to identify to OPM the attachments being sent. This is a known technical issue that is being worked by OPM and DoD. Mr. Langer stated that industry has received clear direction from DSS/DoD on using eQIP and that these instructions are being followed. With the increase in workload on OPM from 400 to 4,000 cases submitted weekly from DoD, Mr. Langer believes that the problems are not coming from industry. The problem of matching attachments is not going to be solved simply by submitting them electronically. Industry is concerned by the losses in overhead being incurred as a result. Other industry and government NISPPAC representatives noted that rejections were taking place on items that do not have bearing on the investigative process, such as middle initials of former employers. Mr. Schroeder observed that OMB/OPM metrics will measure returns in terms of whether due to the agency or OPM. Mr. Marosy agreed that this will be part of the metric standards. In response to questions on process, Mr. Marosy stated that industry normally submits electronically to DISCO, which in turn releases the case to OPM. If attachments were received without a request for investigation, OPM is unable to provide notifications because of the volume, but does return the attachments. Ms. Baybutt suggested that if all materials are submitted and DISCO issues an interim clearance, this means that case should have been sent to OPM. If after fifteen days a case has not been opened, the DISCO help desk should be contacted, which in turn will work with OPM.

10. **NISP Signatories Update –** Ms. Baybutt stated that NISPOM changes are in the final stages of editing having already been coordinated with DoD OGC and are expected to

be signed by Dr. Stephen A. Cambone, Under Secretary of Defense for Intelligence. Carol Haave, Deputy Under Secretary of Defense (DUSD) for Counterintelligence and Security, announced her resignation. Robert W. Rogalski, who is Director of Security, is now the acting DUSD. Kim Housman (CIA) announced that her agency in the future will be represented by Ruth Olsen, who is Acting Chief of Security Policy. Lynn Gebrowsky (DOE) announced several organizational changes and the consolidation of the twenty-seven Safeguards and Security Directives. Sharon Stewart (NRC) is the new Director of Facilities and Security. Mary Griggs (DSS) announced that Heather Anderson's last day as Director, DSS will be November 18, 2005. Janice Haith will be the Acting Director, DSS.

11. **Closing Remarks and Adjournment –** The Chair thanked and made presentations to outgoing NISPPAC members Jim Linn and Diane Raynor.