NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE

MINUTES OF THE MEETING

Friday, March 12, 2004

The National Industrial Security Program Policy Advisory Committee (NISPPAC) held its 22nd meeting on Friday, March 12, 2004, at 10 a.m., at the National Archives Building, 700 Pennsylvania Avenue, NW, Washington, DC. J. William Leonard, Director, Information Security Oversight Office (ISOO), chaired the meeting. The meeting was open to the public.

I. Welcome, Announcements, Introductions and Administrative Matters.

After welcoming the NISPPAC members and others in attendance, the Chair noted that one of its members, Lonnie Ray Buckels, passed away on December 30, 2003. By letter, on behalf of the NISPPAC members, the Chair expressed condolences to Lonnie's wife and family. In paying tribute to Lonnie, the Chair commented on Lonnie's distinguished military service and his dedication to the NISPPAC and the National Industrial Security Program (NISP). The Chair and the attendees honored Lonnie Ray Buckels by observing a moment of silence.

Following a short pause, the Chair started the introductions by introducing the new members. The two new industry representatives are Raymond H. Musser, General Dynamics Corporation and Donna E. Nichols, Washington Group International, Inc. The Chair then noted that the membership of the NISPPAC had been expanded to include two additional Government agencies: the Department of Homeland Security (DHS) as a member and the Office of Personnel Management (OPM) as an observer. Ora L. Smith represented DHS and Winoa H. Varnon represented OPM.

Following these introductions, the Chair extended his deep appreciation on behalf of the NISPPAC to outgoing members Michael S. Nicholson and Maynard C. Anderson for their four years of distinguished service to the NISPPAC. The Chair stated that he hoped that they would maintain an ongoing dialogue with the NISPPAC and its members.

After the other NISPPAC members and attendees introduced themselves, the Chair noted that the representatives from the Department of Defense (DOD) and the Defense Security Service (DSS) were not able to attend the meeting due to a scheduling conflict.

At the conclusion of the introductions, the Chair reminded the members that the minutes from the last NISPPAC meeting were approved via e-mail on June 6, 2003, and a copy had been placed in their folders.

The Chair concluded his administrative remarks by inviting the attendees to remain after the meeting for a guided tour of the renovated Rotunda, which houses the Declaration of Independence and the U.S. Constitution to include the Bill of Rights.

II. New Business.

A. Department of Homeland Security.

The Deputy Chief, Personnel Security Division, DHS, reported that DHS entered into an agreement with the Department of Defense to become a User Agency under the NISP on

August 22, 2003. Currently, DHS is in the process of assimilating into its Security Office all of the security responsibilities and duties of the 22 organizations that were transferred to it by operation of law. To ease the transition for industrial security policy and procedures, DHS has an interim internal management directive for its national industrial security program.

The Deputy Chief also reported that every state governor and selected members (a limit of five) of their staff have been cleared to receive classified national security information. Each state will have operation centers to store classified information. These centers will be supported by the DHS Security Office and the Information Analysis and Infrastructure Protection Directorate.

Following the discussion, the Chair reminded the NISPPAC members of the amendment to Executive Order 12958, which permits the sharing of classified information with state and local officials in the event of an immediate need to respond to a threat. The National Security Council (NSC) representative followed up on this point by adding that the Administration is undertaking initiatives for sharing information that is now identified as "Sensitive Homeland Security Information" (SHSI). Both the Chair and the NSC representative pointed out that this controlled information already existed and that it is not a new category of national security information but rather a means to share it outside the Federal Government. They added that even though the protection of SHSI does not rise to the level of protection required for classified information, there are safeguarding mechanisms including access restrictions. To ensure that the safeguarding measures and access restrictions are applied systematically, the Administration is developing policies and procedures for sharing SHSI with state and local officials. The NSC representative indicated that he expects the policy for sharing such information will be issued by the end of this year.

B. Office of Personnel Management.

The Assistant Director for Operations, Center for Federal Investigative Services, OPM, reported that since 9/11, the number of clearance requests increased dramatically. As a result, the rising demand for investigations is straining the resources for the investigatory process. Consequently, OPM developed a strategic plan to address the resource needs for handling investigations for the security clearance process. The strategic plan includes Government-wide initiatives to encourage information sharing throughout the security clearance process. The plan includes: (1) increasing the number of vendors for conducting investigations to expand OPM's investigatory capability; (2) the use of E-QUIP as a web-based system and as a stand alone CD-ROM to eliminate the drudgery and redundancy of filing out the SF 86, Questionnaire for National Security Positions; (3) the use of an electronic SF 85, Questionnaire for Non-Sensitive Positions will complete the circle for E-QUIP and is expected to be online in August of this year; and (4) the use of the Clearance Verification System (CVS) with DOD's Joint Personnel Adjudication System (JPAS) so that information flows between the two systems.

Following the report, the members discussed the status of the transfer of the industrial security clearance investigatory function from DSS to OPM. The OPM representative commented that the transition is pending and that OPM and DOD have entered into a "strategic partnership" and that the DSS resources for investigations still remain with DOD.

As the discussion continued, the OPM representative noted that the absence of DOD and DSS prevented an informed discussion of the investigatory process for industrial security clearances and suggested that OPM, DOD, DSS, and industry meet to discuss these matters at another time. The membership agreed to table the discussion until they could meet in a more appropriate forum.

As the discussion concluded, the Chair offered to assist OPM in making the arrangements for the meeting.

C. Personnel Security Issues.

Industry's update on the industrial security clearance process revealed that the current measures for improving the system are not producing the desired results. Industry reported that: (1) the interim clearance helps approximately 80% of the programs and employees in industry, however, it does not assist the personnel assigned to Special Programs due to policy prohibitions against using interim clearances; (2) the transition to OPM for Contractor Clearance Processing did not occur smoothly and it appears that less than 10,000 Contractor cases have been opened since October 1; and (3) industry typically processes between 14,000 and 20,000 cases into the system each month, 25% of these cases will be Periodic Re-Investigations.

In order for the NISPPAC members to ascertain the "state" of the industrial security clearance process, an illustration of one company's metrics was provided. The company's metrics appear in the tables below:

Current Average Government Cycle Times for Cases Closed in February 2004

- Average Cycle Time for Final Secret and Confidential ------ 420 days. This time frame is somewhat mitigated by interim Secret and Confidential clearances (65-75%).
- Average Cycle Time for Final Top Secret was 495 days. While interim Top Secret clearances are granted, they are generally useless.

The Impact of Interim Security Clearances

- On Average 75% of the Secret Clearances submitted to DSS for processing received interim clearances.
- The 25% without an interim clearance could not work a classified program (and therefore charge a program) for a total of 360 days until the employees received their final clearance.
- 114 cases were reflected in the 25%
- 90 days were subtracted for the typical processing time
- 114 employees were unable to work for 270 days (194 actual work days)
- 194 days at an average of $800 per day
- The delay in just the processing of 114 Secret clearances with no interim clearance provided cost the company $17.7 million, in 2003.

The Cost Impact for Top Secret Security Clearance Processing

- The Top Secret Clearance Process is less clear and difficult to determine because these costs are often soft or indirect costs.
- The employee may be able to work at the Secret level (and charge a contract) but he or she cannot work for the program for which he or she was hired.
- The hiring of another person, who is already cleared at the Top Secret level, at a premium above the typical salary plus a signing bonus.
- The program misses a milestone while the company recruits a new employee.
- The circle begins again when the periodic re-investigation is required and the new employee cannot be placed on a new program.

The Memorandum of Understanding Signatories made the following recommendations at the end of their presentations:

SHORT-TERM OPTIONS

- Lighten the load of clearances in process to address possible problems with investigative capability.
- Apply a Risk-Management philosophy that may provide options to the current Periodic Re-Investigation Process and remove 25% of the contractor clearance load to OPM.

LONG-TERM OPTIONS

- Modify Executive Order 12968, "Access to Classified Information" to delete those portions of the required background investigative elements that do not add value to the process and delay case completion.
- Provide funding to improve automated completion of critical path investigative processes.
- Fund and field a capability for the Automated Continuing Evaluation System (ACES) to augment and eventually replace the current Periodic Re-Investigation Process.
- Ingrain with Government a more Risk-Management approach to the process.
- Continue to work with industry to address reciprocity concerns.

The Security Affairs Support Association representative's presentation contained the following recommendations:

- Define reciprocity or crossover as "immediate conditional reinstatement" within agencies between different contracts, and between agencies for equivalent clearance levels and access to Sensitive Compartmented Information.
- Grant a 30-day grace period for individuals who change employer/sponsor while they are in the process of being reinvestigated.
- Establish and achieve a goal of completing the entire end-to-end personnel security clearance process (to include polygraph) in 90 days. Task agencies to develop a plan to meet this goal.
- Institute a "fast-track" approach to issue-free cases.
- Allow companies to build "bench strength" to promote flexibility and rapid response to changing or new requirements.
- Resolve the issue of unreasonable Single Scope Background Investigations (SSBI) timelines by either fully staffing DSS/OPM or by increasing the utilization of contract investigators and adjudicators to complete investigations and adjudicate cases.
- Implement the transfer of the personnel security investigations program from DOD to OPM immediately, with adequate resources that will ensure the success of the program within OPM.
- Deploy the DOD Joint Personnel Adjudication System (JPAS), in accordance with the President's e-Government/e-Clearance initiatives, to every cleared company that desires access to the system by December 31, 2004, or sooner.
- Support fully and accelerate OPM's e-Government/e-Clearance initiative, which speeds the investigation process for an employee's security clearance, saves money and promotes reciprocity among Federal agencies.
- Evaluate the feasibility of permitting employees, with an outdated SSBI (up to seven years old), to maintain their access to classified information provided that (i) the Periodic Re-investigation has been submitted and (ii) the SF 86 is entirely clean.

In sum, both presentations emphasized that the delays in the security clearance process stall the completion of missions and have a negative impact on contractor performance and unnecessarily add costs for the taxpayer to bear.

The follow on discussion between the NISPPAC members revealed that both Government and industry have the same frustrations with the longstanding hurdles for processing security clearances and agree that there is a crisis that needs to be addressed. The Air Force representative indicated that he would present these issues to OSD at the Security Managers Conference in Colorado Springs, next week.

As the members concluded the discussion all agreed on the importance of ensuring a continuing and effective dialogue between Government and industry on the subject of personnel security clearances. Many opined that this would be useful in ascertaining industry's viewpoints as well as the Government's perspective as initiatives are being developed for improving reciprocity, adjudication back-logs, and the requirement for the five-year periodic reinvestigations.

In highlighting the significant points of the discussion the Chair outlined the next steps towards resolving the delays in the security clearance process. These steps include: (i) a meeting with OPM, OSD and industry representatives as suggested by the OPM representative to discuss the status of pending industry requests for personnel security clearances; (ii) providing industry's concerns and recommendations to the Government's current working groups addressing personnel security clearances, especially the Personnel Security Working Group under the auspices of the NSC's Policy Coordinating Committee as well as a similar working group under the auspices of the DCI's Special Security Center, with the objective of establishing an ongoing dialogue to ensure industry's unique circumstances are taken into account; and (iii) an immediate an renewed effort by the NISP signatories to examine current business practices for the security clearance process so that immediate solutions can be applied to reduce the delays in the process, with particular emphasis placed on reciprocity.

The NSC representative reminded the members that he had asked for suggestions for policy changes that might remove some of the impediments in the security clearance system. The Chair asked the members to forward their suggestions through ISOO for presentation to the NSC representative.

III. Information Security Oversight Office Updates.

A. Financial Disclosure Form.

The Chair reported that the Financial Disclosure Form is winding its way through the Office of Management and Budget process and that it is near completion.

B. The Implementing Directive for Executive Order 12829, as amended, "National Industrial Security Program."

The Security Oversight Office has drafted an implementing directive and it is had been presented to the NISP signatories for review and comment. As soon as the comment stage is completed, the draft will be circulated to the NISPPAC members for comment.

C. The NISP Metrics in the Security Clearance Arena.

The Chair reported that a draft for tracking the trends and the amount of time it takes to receive a security clearance has been sent to the NISP signatories for review and comment. ISOO will use this tool in the NISP program as soon as it finalizes the metrics.

IV. Closing Remarks and Adjournment.

The Chair invited those who were interested to remain for a tour of the Rotunda.

There being no other business raised, the Chair adjourned the meeting. The next meeting is scheduled for September 2004, in Washington, DC.

Attachments (4):

(1) Summary of Action Items from the March 12, 2004 Meeting
(2) Agenda
(3) Roster of Attendees at the March 12, 2004 meeting
(4) Handouts (6):

- Minutes of the April 23, 2003 NISPPAC Meeting
- NISPPAC Address List
- NISPPAC Bylaws, as amended April 23, 2003
- *Federal Register* copy of Classified National Security Information (Directive No. 1); Final Rule
- Update on Industrial Security Issues for Industry, Spring 2004
- Security Clearance Process-Recommendations for Improvement

Summary of Action Items from the March 12, 2004 Meeting

ACTION ITEM	WHO	TIME FRAME
1. Meeting between OPM, OSD and industry.	The Chair and ISOO staff (Subsequently, OSD offered to organize and host this meeting.)	Early April 2004
2. Nominations for two industry members	All NISPPAC Members	Due to Chair by May 31, 2004
3. Brief OSD on issues surfaced by industry concerning the security clearance process	William A. Davidson, Air Force	Present at the DOD Security Managers Conference in Colorado Springs, March 2004
4. Suggestions for amending Executive Order 12968	All NISPPAC members	Due to Bill Leary, through ISOO, by May 31, 2004
5. Meeting with Personnel Security Working Group, DCI Special Security Center and industry	The Chair and ISOO staff to coordinate with the Chair of the PSWG and SSC	Mid-April 2004
6. Meeting with NISP signatories to develop common approach to reciprocity practices in the near-term	The Chair and ISOO staff	Mid-April
7. Follow up with NISPPAC members to report on outcome of the meetings mentioned in action items nos. 5, 6, and 7	The Chair and ISOO staff	Mid-May ----- early June 2004

National Industrial Security Program Policy Advisory Committee

Meeting-Friday, March 12, 2004
10:00 AM – 12:00 PM
National Archives Building, Jefferson Room
Washington, DC

Agenda

I. Welcome, Introductions and Administrative Matters **(10 minutes)**
J. William Leonard, Director
Information Security Oversight Office

II. New Business

- **Department of Homeland Security** **(10 minutes)**
  Ora L. Smith
  Deputy Chief, Personnel Security Division

- **Office of Personnel Management** **(15 minutes)**
  Winona Varnon
  Assistant Director for Operations
  Center for Federal Investigative Services

- **Personnel Security Issues** **(70 minutes)**

  - Patricia B. Tomaselli, Director of Sector Security **(35 minutes)**
    Northrop Grumman Corporation

  - Frank F. Blanco, Executive President **(15 minutes)**
    Security Affairs Support Association

  - Open Discussion on Clearance Related Issues **(20 minutes)**

III. ISOO Updates **(5 minutes)**

IV. Old Business **(5 minutes)**

V. General Open Forum **(5 minutes)**

VI. Closing Remarks and Adjournment **(5 minutes)**

National Industrial Security Program Policy Advisory Committee
Meeting-Wednesday, April 23, 2003
10 a.m. – noon
National Archives Building, Room 105

Roster of Attendees

Government

William A. Davidson
Department of the Air Force
Walter L. Bishop
Department of the Army
Karl Schilling
Central Intelligence Agency
Geralyn Praskievicz
Department of Energy
Ora L. Smith
Department of Homeland Security
Charles Alliman
Department of Justice
Will Morrison
National Aeronautics and Space Administration
Winoa H. Varnon
Office of Personnel Managment
Ralph Wheaton
Department of the Navy
Thomas O. Martin
Nuclear Regulatory Commission
Andrea G. Jones
Department of State
William H. Leary
National Security Council
J. William Leonard, Chair
Information Security Oversight Office

Industry

Dianne Raynor
Boeing Company
Thomas J. Langer
BAE SYSTEMS North America, Inc.
Maynard C. Anderson
ARCARDIA GROUP WORLDWIDE, IN
Patricia B. Tomaselli
Northrop Grumman Corporation
P. Steven Wheeler
Lockhead Martin Aeronautics Company
Donna E. Nichols
Washington Group International Government
Raymond H. Musser
General Dynamics Corporation

ISOO Support Staff

Laura L. S. Kimberly
Dorothy L. Cephas
Emily R. Hickey
Jason P. Hicks
Philip A. Calabrese
Margaret L. Rose
Rudolph H. Waddy
Matthew W. Stephan
Lamont K. Taylor
Jorg J. Wetzel
Robert L. Tringali
William J. Bosanko

Observers

Kent Hamilton
Michael Allen
Daniel Bishop
Richard Ernau
Don Strout
Doug Hudson
Edward J. Halibozek
Michael L. Yawn
Sheri Portee
Linda Creel
Frank F. Blanco