

**NATIONAL INDUSTRIAL SECURITY PROGRAM  
POLICY ADVISORY COMMITTEE**

**MINUTES OF THE MEETING**

**Wednesday, April 23, 2003  
(as approved by e-mail vote on June 16, 2003)**

The National Industrial Security Program Policy Advisory Committee (NISPPAC) held its 21<sup>st</sup> meeting on Wednesday, April 23, 2003, at 10 a.m., at the National Archives Building, 700 Pennsylvania Avenue, Northwest, Washington, DC. J. William Leonard, Director, Information Security Oversight Office (ISOO), chaired the meeting. The meeting was open to the public.

**I. Welcome, Announcements and Introductions.**

After welcoming those in attendance and the self-introductions, the Chair suggested that approval of the September 25, 2002 minutes be deferred until the end of the meeting to allow the membership time to review the extensive revisions submitted by the Department of Defense. Not all of the members had the opportunity to offer their comments because the revisions were circulated while some of the members were en route to the meeting. Accordingly, the membership agreed with the Chair's suggestion.

**II. Administrative Matters.**

**A. Department of Homeland Security to Join the NISPPAC.**

Pursuant to Executive Order 12829, as Amended, "National Industrial Security Program," the Chair announced that he will ask the Department of Homeland Security to become a member of the NISPPAC. Accordingly, the Chair moved that the pertinent paragraphs in Articles 3, 4 and 9, of the NISPPAC By-laws be amended to accommodate this addition to the membership. (A copy of the motion is attached to these minutes.) The motion was seconded and passed unanimously by the NISPPAC members.

**B. Nominations for Two Industry Members.**

The Chair then announced that the terms of two industry members, Michael Nicholson and Maynard Anderson, are due to expire in September 2003. He requested that the members submit the names of potential candidates to him by Friday, July 11.

**III. Old Business.**

**A. Update on the Amendment to Executive Order 12958, "Classified National Security Information."**

On March 25, 2003, the President signed Executive Order 13293, "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." After giving a brief overview of the principle purpose of the Amendment, the Chair pointed out that the Amendment does not substantially change what can be classified. He clearly pointed out that information ineligible for classification prior to March 24, 2003, remains ineligible for

classification on March 26, 2003. However, there is one narrow exception to this rule. The Order permits the reclassification of permanently valuable historical records that are 25 years old or older under limited circumstances. He emphasized that industry should report to the Information Security Oversight Office any instances of requests to classify information that was ineligible for classification prior to the Amendment. As he concluded his remarks on this issue, he added that what could be classified on March 24, 2003, can still be classified on March 26, 2003.

The Chair continued his discussion of two other issues that he expects to impact on industry. The first concerned the changes in marking requirements for classified documents. He informed the membership that the new marking requirements would become effective on September 22, 2003. The ISOO staff has already begun the process for drafting the Order's implementing directive that will include the new marking requirements. Agencies should expect to receive the draft for comment by June 25.

The second issue concerned the automatic declassification of records in non-Government repositories. This issue will be addressed in the implementing directive and ISOO will be seeking industry's views for handling classified records that are 25 years old or older that are held by contractors.

#### **B. Update on the Financial Disclosure Agreement Form.**

Emily R. Hickey, Senior Program Analyst, Information Security Oversight Office, reported that the package for the Financial Disclosure Form is on its way to the Office of Management and Budget. She explained that the approval process takes approximately six months. This includes a 60-day comment period.

Ms. Hickey further explained that ISOO did not convene a working group to develop procedures to ensure the confidentiality of financial disclosure reports, because subsequent to the September 2002 meeting, the Executive Agent suggested that this could be achieved by amending the NISPOM. Therefore, ISOO decided that it is unnecessary to convene a working group, at this time. The change to the NISPOM concerning financial disclosure reports will be coordinated with Industry and Government when it is developed. The expectation is that this change to the NISPOM will be completed and become part of the package that includes the approved Financial Disclosure Agreement Form forwarded to the President for his final approval, probably by the end of 2003.

Following the report, the members briefly discussed other issues relating to the financial disclosure reports. As the discussion concluded, the Chair and the NSC representative emphasized that agencies are expected to practice total reciprocity and that individuals should not be required to repeatedly submit information for the Financial Disclosure Agreement Form. Both the Chair and the NSC representative asked to be notified if anyone experiences a failure to observe total reciprocity.

#### **C. Industrial Security Clearance Processing Delays.**

In response to the NISPPAC's concerns about processing delays for security clearances, the Chair reported that the Deputy Assistant Secretary of Defense for Security and Information

Operations (S&IO) has agreed to collaborate with ISOO and the NISPPAC to seek near-term solutions to this problem. The Deputy Assistant Secretary of Defense for S&IO has already identified “mission critical clearances” as a near-term solution and Industry has begun submitting “mission critical clearances” that are being prioritized by the Defense Security Service and the Defense Office of Hearing and Appeals.

To continue this effort, the Deputy Assistant Secretary of Defense for SIO has requested that ISOO chair a small working group to seek additional near-term solutions for the security clearance processing delays. The Chair asked that those members interested in serving on the working group to provide their names to Laura Kimberly, Associate Director for Policy, ISOO, by May 2. The Chair would like volunteers from Industry and Government and particularly the Personnel Security Working Group. The working group is expected to meet during the month of May.

#### **D. Sensitive Homeland Security Information and Sensitive But Unclassified Information.**

The Chair reported that a Delegation Memorandum, which is under consideration within the Executive Office of the President, has deferred the effort on the issuance of guidance for Sensitive Homeland Security Information. In the meantime, Industry is looking at its internal procedures for protecting Sensitive But Unclassified (SBU) Information. At the request of the NSC staff, Industry will provide examples of the problems that it is experiencing with protecting SBU information. The Chair recognized that these issues are of particular concern to Industry and assured the NISPPAC members that he would keep them apprised of the actions taken to address these matters.

#### **IV. New Business.**

##### **A. Executive Agent’s Update.**

The Deputy Director for Industrial Security, Office of the Assistant Secretary of Defense reported the following:

- (1) The Department of Education (ED) has entered into an agreement with the Department of Defense to become the newest User Agency under the National Industrial Security Program. Under this Agreement, which is required by Executive Order 12829, as Amended, “National Industrial Security Program,” the Defense Security Service will serve as the Cognizant Security Office for ED contractor facilities requiring access to classified information.
- (2) The Department of Homeland Security has requested to be a User Agency under the National Industrial Security Program.
- (3) The Department of Defense continues to provide support to those entities that were transferred by operation of law to the Department of Homeland Security.
- (4) Under the “Transforming Government” Initiative, it has been recognized that the Personnel Security Investigations Program requires transformation. In Fiscal Year 2004, the Defense Security Service will be divested of its investigative mission and obtain investigative support from the Office of Personnel Management. The Department of Defense will continue to operate its Joint Personnel Adjudication System, otherwise known as JPAS.

## V. Defense Security Service (DSS) Update.

The Deputy Director for Industrial Security, Defense Security Service (DSS), updated the membership on the use of the Electronic Personnel Security Questionnaire (EPSQ) as the front end process for security clearances requests.

In his concluding remarks, he commented that the EPSQ will be replaced by electronic Questionnaires for Investigations Processing or e-QIP. E-QIP is an automated version of the Questionnaire for National Security Positions (Standard Form 86) that will be used by all Government agencies. E-QIP will reduce the wait time for clearances because e-QIP automates the SF 86 and makes it electronically transmittable. More importantly, individuals needing to make subsequent submissions will have access to a new form that contains the previously submitted data. Automation of the form will reduce the completion time to fill it out from hours to minutes and the processing time from days or weeks to a few hours. Benefits will also be gained in the scheduling process of background investigations. DSS will let its customers in the DOD and its contractors know when they may use e-QIP to process Standard Form 86.

As the discussion turned to DSS's Personnel Security Investigation (PSI) Production, the Deputy Director for Personnel Security Investigations reported that the DSS's PSI Production remains very high and that DSS consistently exceeds its production goals. The Deputy Director noted that the input of cases is exceeding customer projections by more than 40%. Despite the high input, Interim Secret clearances are being issued within three to five days.

DSS has established the following priority to handle cases that are pending:

- (1) Priority cases (submitted in accordance with the DOD Priority). This is approximately 2,000 cases.
- (2) Identified industry mission critical cases. Initially, DSS asked industry to identify 5% of its mission critical cases. DSS has raised the percentage to 10%. Industry should identify the missions critical cases regardless of age up to an additional 10% of requests pending. On the initial round, over 2,000 cases were identified. Of that, DSS has only 400 investigations pending.
- (3) Old cases. These are cases submitted prior to March 2002. Currently, there are 17,000 industry cases pending. The goal is to have the cases closed by the end of Fiscal Year 2003.
- (4) New Single-Scope Background Investigations (SSBI) received since March 2002.
- (5) New issue National Agency Check, Local Agency Check (NAC/LAC). The non-issue NAC/LACs will flow through the automated processes.
- (6) New Periodic Reinvestigations (PR).

Currently, three contractors, DYNCORP, OMNISEC and ISJV, are actively working on DSS investigations. The contractors have been tasked with SSBI's with a particular emphasis on high volume areas such as the National Capital region, Southern California, Fayetteville, Seattle and the Tidewater region. The Deputy Director remarked that it is really critical that the DSS receive releases on cases as soon as possible. The releases should not be mailed. The membership was requested to scan releases and attach them to the e-mail transmitting the EPSQ or to fax the

releases. The fax number is 866-369-2812. A lack of releases can significantly impact the time it takes an agent to complete cases.

The discussion concluded with an overview of DSS lapse time on cases received since March 2002: (1) NAC/LACs averaged 70 days overall, non-issue NAC/LACs average less than 40 days due to the automation capability; (2) SSBI's averaged 157 days, and (3) Top Secret PRs averaged 160 days overall.

**VI. The Director of Central Intelligence's (DCI) Special Security Center.**

The Director, Special Security Center, informed the NISPPAC members that the Special Security Center is in operation. It is not a CIA organization in its office of security. The Director of the Special Security Center reports directly to the Special Assistant to the DCI for Security. Ultimately, the Special Security Center will consist of 63 positions. Recruits for the Special Security Center are sought from every area of the Federal Government. To ensure this, vacancy positions are posted on the Office of Personnel Management "USAJobs" web site.

The purpose of the organization is to ensure the proper handling and maintenance of classified intelligence information. Before 9/11, the Director of Central Intelligence had concerns about the intelligence community's handling of such information and asked senior officials to conduct a self-inspection of their programs. The self-inspections revealed that the DCI's directives were not being uniformly applied. The DCI's solution to this problem was to form the Special Security Center. Oversight and compliance has become even more critical, now that the intelligence community provides actionable operational information on a daily basis to individuals in the Government who have never had access to Sensitive Compartment Information or intelligence information. The Special Security Center will be providing assistance and guidance in the handling of classified intelligence information to the intelligence, defense, law enforcement and foreign affairs communities, as well as industry.

**VII. 2003 Update on Industry's Five Security Issues.**

The Director of Sector Security, Northrop Grumman Corporation, updated industry's five security issues, which were identified in the fall of 2000. They were Meaningful Clearance Reform, Reciprocity, Fee for Service, Sensitive But Unclassified Information Protection and Chapter Eight Issues. The response or action taken to address these security issues is listed in the chart below.

Industry's Five Issues	Response/Action Taken
<p>(1) <b>Meaningful clearance reform</b> – The clearance process is a strain on industry resources, particularly since 9/11, because it impacts on industry's ability to move people and effects the periodic reinvestigation process. Industry is conducting a study.</p>	<ul style="list-style-type: none"> <li>• In Spring 2001, DSS initiated the transfer of all special access clearance processing to OPM for a period of one year to provide Industry more timely processing for these critical clearances.</li> <li>• OSD and DSS also requested that Industry estimate the number of clearances to be required in FY 2002 to judge manpower needs.</li> </ul>

- At the Spring 2002 NISPPAC mtg., Industry requested that an IPT be formed to address the current Clearance Issues and examine best practices.
- By the Fall of 2002, the NISPPAC meeting had an entirely different tone: (1) DSS brought back the OPM clearance work and had focused on the acceleration of new clearance processing, (2) The old clearances (pre-March 2002) would sit until resources were available to address them, (3) The DOHA backlog was also intolerable. Although Industry's submittal of proposed clearance needs for 2003 had provided additional manpower for DOHA, the learning curve would be great.
- At the Fall 2002 NISPPAC mtg., industry announced its five new issues: clearances. The members voted to have the Chair send a letter to the SecDef asking for a review of resources.
- At the October AIA/NDIA mtg., the MOU/NISPPAC demanded dialogue and assistance. Critical programs in Operation Enduring Freedom, as well as Homeland Security, could not perform because of the Personnel Clearance quagmire.
- At the AIA/NDIA meeting, the Deputy Assistant SecDef for Security & Info Operations agreed to a system where FSO's could identify 5% of their Mission Critical clearances and send these to OSD, where they would be parceled to DSS, OPM, and DOHA, as appropriate.
- January 2003, the MOU/NISPPAC distributed the request for Mission Critical Clearances that were lost or lagging in the DSS, OPM and DOHA systems.
- DSS reps and five of the six organizations (except ASIS whose defense industry reps are in other organizations) distributed the request forms.
- Late February 2003: (1) 300 contractor facilities responded; (2) 2072 investigations were identified as lost or lagging; and (3) 228 had already been issued, 1194 were

	<p>still in DSS, 154 were at OPM and 484 were at DOHA, 12 had been terminated.</p> <ul style="list-style-type: none"> <li>On Feb.13, 2003, MOU/NISPPAC reps met with the DA SecDef for SIO. DSS transferred its DSS investigations to OPM. They discussed changes in the clearance processing and systems access.</li> </ul>
<p>(2) <b>Reciprocity</b> – The biggest issue for the NISPPAC because of its actual take on what industry believes to be the value of the NISP--a cost-effective system. The two areas of concern are: (i) personnel clearance, and (ii) physical and cyber security. Industry is proposing a working group to address this issue.</p>	<ul style="list-style-type: none"> <li>ISOO would create a survey on reciprocity and call on various participating companies to discuss their experiences and concerns with <u>reciprocity</u> in both the clearance process and other areas such as cyber security and sensitive but unclassified information handling.</li> <li>Industry requested that an IPT be formed to address the current Clearance Issues and examine best practices.</li> </ul>
<p>(3) <b>Fee-for-Service</b> – This is a bad idea for business. Industry will wait for DOD’s resolution.</p>	<ul style="list-style-type: none"> <li>In the Spring of 2001, industry reps worked with AIA’s Security and Procurement Committees on correspondence to the OSD Comptroller.</li> <li>A logical and practical argument was presented that demonstrated the lack of value in charging industry for standard clearance processing service.</li> <li>The letter campaign by AIA Industrial Security and Procurement groups shelved the issue of Fee for Service for Contractors.</li> </ul>
<p>(4) <b>Sensitive but unclassified information (SBU) protection</b> – Questions about reciprocity and the development of a fourth classification level. NDIA* has offered to conduct a study and provide a white paper from industry.</p>	<ul style="list-style-type: none"> <li>At the Spring 2002 meeting in Tucson, AZ, Industry (NDIA) would provide a series of general guidelines on how industry handles its Proprietary Information, which is the closest private category to Sensitive But Unclassified.</li> <li>Industry (NDIA) provided wording that summarized the critical portions of private industry’s procedures for handling their proprietary information. The baseline protective measures for proprietary information employed by industry are: (1) data must be marked to indicate its</li> </ul>

\* National Defense Industrial Association

sensitivity and carry a distribution restriction to preclude unauthorized release or public disclosure, (2) employees must be educated to recognize the markings and their meanings so it may be efficiently protected, (3) methods for handling, transmission, and destruction must preclude the potential for unauthorized use or public disclosure of the data.

- In mid-2002, several members of the MOU/NISPPAC were approached by the Office of Homeland Security to participate in a mtg., on Critical Infrastructure.
- The meeting was a learning event for both sides. The effort later developed into a DOD initiative called the Critical Infrastructure Protection Integration Staff (CIPIS – based in the Pentagon). It includes 50 DOD agencies and reps of the Defense Industrial Base were invited to participate.
- The CIPIS meets monthly and most meetings are attended by a representative of NDIA or AIA/NISSPAC.
- In 2003, Industry provided its key points to the CIP Integration Staff: (1) Protection for the names of companies (most of which are publicly traded) on the database (and their critical subcontractors) as well as associate risk factors and vulnerabilities determined by the DOD, (2) Integration of Cyber and Physical Security Programs, Assessments and Protective Measures for Security in Depth, (3) Funding, Responsibility and Compliance initiatives for additional security measures required by DOD based on their assessments of our vulnerability and current security practices, (4) Handling and Protection Criteria for SBU information produced in conjunction with these assessments, (5) Protection from FOIA and Release to Competitors for Industry's Proprietary and Competition Sensitive Information

<p>(5) <b>Chapter Eight</b> – Propose an industry study to enhance communication and interpretation. Will work with the CSAs and Information System Security Programs (ISSP).</p>	<ul style="list-style-type: none"> <li>• In the late Spring of 2001, the MOU/NISPPAC reps met with the authors of Chapter Eight to discuss industry’s concerns on the significant impact to industry in meeting Chapter Eight’s compliance.</li> <li>• Of significant interest was the DOD’s use of the Chapter Eight verbiage for collateral Confidential and Secret level systems. Industry felt the requirements were onerous and cost-prohibitive.</li> <li>• Industry was not successful in obtaining changes to Chapter Eight’s wording.</li> <li>• They agreed to accept a directive to work with the DSS on the implementation and identify solutions to Chapter Eight.</li> <li>• A general agreement that DSS could provide exemptions when the fix was cost-prohibitive or the technology was not sufficiently robust to address this issue.</li> </ul>
---	--

Following the presentation, the Director of Sector Security, Northrop Grumman Cooperation emphasized that Industry’s primary issue is coping with personnel security clearance delays. Processing security clearances continues to be a major roadblock to Industry’s efforts to fulfill its responsibilities to the Government. As the discussion continued, it was expressed that even at wartime, Industry is unable to deploy personnel to the battlefield to support a war fighter because of delays in the security clearance process.

As the discussion concluded, the Chair emphasized the need for reciprocity and that reciprocity is an issue that must be addressed. He added that the Information Security Oversight Office intends to draft an implementing directive for Executive Order 12829, as Amended, “National Industrial Security Program,” that will contain provisions on reciprocity.

**VIII. Update on the National Industrial Security Program Survey.**

The Chair reported that a draft report of the NISP survey is in circulation and that ISOO expects to have it issued by the end of May. The Chair expressed concern that the findings in the report indicate that ISOO has not fully exercised its oversight role for the NISP. In that view, the Chair announced that ISOO intends to fully assume its oversight responsibilities by (1) drafting an implementing directive for the National Industrial Security Program, (2) ensuring reciprocity and (3) reviewing agencies’ implementing regulations for the NISP. ISOO fully intends to work with both Industry and Government to ensure that the tenets of the National Industrial Security Program, to safeguard classified information in the Industrial community and to promote and preserve the economic and technological interests of our nation are observed so that redundant, overlapping, or unnecessary requirements do not impede those interests. The Chair further indicated that the NISPPAC will play a very large role in this area.

## **IX. Approval of the September 25, 2002 Minutes.**

In keeping with the decision to defer discussion of the minutes to the end of the meeting, the Chair, in response to a question raised by an Industry representative, explained that publishing the minutes on the ISOO web site would ensure the timely release and availability of the minutes in accordance with the Federal Advisory Committee Act. Moreover, the NISPPAC should serve as a vehicle for dialogue between Industry and Government. Publication on the web site would enable a wider promotion of the NISP with other Government security managers and contractors and not just the immediate membership.

As the discussion continued, the membership suggested that a synopsis of the meetings appear on the web site without attributing the remarks to a particular NISPPAC member. Others suggested that the detailed minutes with a complete and accurate description of matters discussed and conclusions reached could appear on the DSS web site or the Extranet web site.

The Chair indicated that he would take these suggestions under consideration. The discussion then turned to the approval of the minutes of the September 25, 2002 meeting. The membership agreed to review DOD's revisions to the minutes and to submit their approval via e-mail by Friday, May 9, 2003.

## **X. Closing Remarks and Adjournment.**

The Chair invited everyone to remain, after the meeting, for cake and coffee in celebration of the NISPPAC's 10<sup>th</sup> anniversary.

There being no other business raised the Chair adjourned the meeting. The next meeting is scheduled for September 2003, in Washington, DC.

### **Attachments (6):**

- (1) Motion to amend Articles 3, 4 and 9 of the NISPPAC by-laws
- (2) Response to the Action Items from the September 25, 2002 Meeting
- (3) Summary of Action Items from the April 23, 2003 Meeting
- (4) Agenda
- (5) Attendance Rooster
- (6) Handouts Distributed at the Meeting:
  - (a) NISPPAC by-laws, as amended May 20, 1999
  - (b) Motion to amend Article 3, 4 and 9 of the NISPPAC by-laws
  - (c) Letter to Secretary of Defense, dated November 12, 2002, from J. William Leonard, NISPPAC Chair, re: Industrial Security Clearance Processing Delays
  - (d) Letter to J. William Leonard, NISPPAC Chair, dated February 10, 2003, re: Actions Taken to Address Industrial Security Clearance Processing Delays
  - (e) Revisions to Executive Order 12958 on Classified National Security Information
  - (f) Federal Register copy of Executive Order 13292-“Further Amendment to Executive Order 12958, as Amended, Classified National Security Information”
  - (g) Line In/Line Out Version of Title-3—Executive Order 13292 of March 25, 2003

## MOTION

Moved by the Chairman that the pertinent sections of Article 3. Membership, Article 4. Meetings, and Article 9. Amendment of Charter and Bylaws, of the NISPPAC bylaws be amended so that the paragraphs read as follows:

### **Article 3. Membership.**

**A. Primary Membership.** Executive Order 12829 conveys to the Chairman of the NISPPAC the authority to appoint all members. The Committee's total membership of ~~22~~ 23 shall be comprised of ~~14~~ 15 representatives from executive branch agencies (including the Chairman) and eight representatives from industry. At least one industry member shall be representative of small business concerns, and at least one shall be representative of Department of Energy/Nuclear Regulatory Commission contractors or licensees. An industry member serves as a representative of industry, not as a representative of his or her employing company or corporation.

### **Article 4. Meetings.**

**A. General.** The NISPPAC will meet at least twice each calendar year as called by the Chairman. As the situation permits, the Executive Secretary will canvass the membership in advance of the scheduling of meetings in order to facilitate attendance by the largest number of members. The Chairman will also call a meeting when so requested by a majority of the ~~14~~ Government members, and a majority of the ~~eight~~ industry members. The Chairman will set the time and place for meetings and will publish notice in the Federal Register at least 5 calendar days prior to each meeting.

**B. Quorum.** NISPPAC meetings will be held only when a quorum is present. For this purpose, a quorum is defined as a simple majority of the ~~14~~ Government members or alternates and a simple majority of the ~~eight~~ industry members or alternates

### **Article 9. Amendment of Charter and Bylaws.**

Amendments to the Charter and Bylaws of the Committee must conform to the requirements of the FACA and E.O. 12829, and be agreed to by two-thirds of the ~~14~~ Government members or alternates and two-thirds of the ~~eight~~ industry members or alternates. Confirmed receipt of notification to all Committee members must be completed before any vote is taken to amend either the Charter or bylaws.

**Response to Action Items from the September 25, 2002 Meeting**

ACTION ITEM	WHO	TIME FRAME
1. Submit names to Chair to serve on the Financial Disclosure Working Group to draft procedures for implementing the standardized disclosure form in industry.	All NISPPAC Members	Tabled – the Executive Agent suggested that a simple amendment to the NISPOM could take care of this.
2. Submit recommendations for amending the NISPOM to Rosalind Baybutt.	All NISPPAC Members	DOE responded.
3. Inform the Memorandum of Understanding Group and the NISPPAC of the release of the Industrial Security Regulation.	Rosalind Baybutt	As soon as the Regulation is released.
4. Submit (via e-mail) suggestions to Chair for letter to SecDef re: the clearance delays.	All NISPPAC Members	Completed – the Ass't SecDef for Sec & Oper has identified a system where industry can identify its Mission Critical clearances.
5. Send draft letter to NISPPAC members for comment.	J. William Leonard, Chair	Completed. See above.
6. Inform Gerald A. Schroeder, Chair, Personnel Security Working Group of any instances of the lack of reciprocity in the collateral world.	All NISPPAC Members	On-going activity.
7. Suggestions/comments to OMB re: draft guidance paper on Sensitive Homeland Security Information are to be referred to Laura L. S. Kimberly, ISOO.	All NISPPAC Members	No submissions were received. OMB no longer has this task.

## Summary of Action Items from the April 23, 2003 Meeting

ACTION ITEM	WHO	TIME FRAME
1. Approve the September 25, 2002 minutes. Submit to Dorothy Cephas.	All NISPPAC Members	By Friday, May 9, 2003.
2. Draft ISOO Implementing Directive for circulation.	ISOO staff	By Wednesday, June 25, 2003.
3. Provide the Chair and the NSC representative with significant examples of how delays in the security clearance process has hampered industry.	All NISPPAC Members	By the end of May 2003.
4. Industry is to provide the Chair and NSC member with some examples of problems it incurs as it protects Sensitive But Unclassified information and specific examples of requirements.	All Industry members	In process-Lonnie Buckels has put out a call to industry via the NCMS for examples.
5. Submit names to Laura L. S. Kimberly for the establishment of a working group to develop near-term solutions to address the delays in the security clearance process.	All NISPPAC Members	By May 2, 2003.
6. Submit nominations for industry representatives to the NISPPAC to the Chair.	All NISPPAC Members	By Friday, July 11, 2003.
7. Amendment to the NISPOM. Re: Confidentiality of Financial Disclosure Reports	Executive Agent	By mid-November 2003. Must be ready for inclusion in the package that will go to the President by the end of 2003.

# National Industrial Security Program Policy Advisory Committee

Meeting-Wednesday, April 23, 2003  
10:00 PM – 12:00 PM  
National Archives Building, Room 105  
Washington, DC  
Agenda

- |             |   |   |
|-------------|---|---|
| <b>I.</b>   | <b>Welcome and Introductions</b>  | <b>(5 minutes)</b>  |
| <b>II.</b>  | <b>Administrative Matters</b><br>J. William Leonard, Director<br>Information Security Oversight Office  | <b>(15 minutes)</b>   |
| <b>III.</b> | <b>Old Business</b> <ul style="list-style-type: none"><li>• Executive Order Update</li><li>• Financial Disclosure Form Update</li><li>• Industrial Security Clearance Processing Delays</li><li>• Sensitive Homeland Security Information/Sensitive But Unclassified</li></ul>  | <b>(20 minutes)</b>   |
| <b>IV.</b>  | <b>New Business</b> <ul style="list-style-type: none"><li>• <b>Executive Agent's Update</b><br/>Rosalind Baybutt, Deputy Director for Industrial Security<br/>OASD (C3I)/ODASD (S&amp;IO)</li><li>• <b>Defense Security Service Update</b><br/>Ronald W. Iverson<br/>Deputy Director for Industrial Security</li><li>• <b>Central Intelligence Agency Update</b><br/>Edward S. Wilkinson, Director<br/>DCI Special Security Center</li><li>• <b>Industry Update</b><br/>Patricia B. Tomaselli, Director of Sector Security<br/>Northrop Grumman Corporation</li><li>• <b>NISP Survey Discussion</b></li></ul> | <b>(10 minutes)</b><br><b>(15 minutes)</b><br><b>(15 minutes)</b><br><b>(15 minutes)</b><br><b>(15 minutes)</b> |
| <b>V.</b>   | <b>Open Forum</b>   | <b>(5 minutes)</b>  |
| <b>VI.</b>  | <b>Closing Remarks and Adjournment</b>  | <b>(5 minutes)</b>  |

**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**

**Daniel Green**

Department of the Air Force

**Katherine H. Darby**

Department of the Army

**Alyn C. Hulse**

Central Intelligence Agency

**Rosalind Baybutt**

Department of Defense

**Ronald W. Iverson**

Defense Security Service

**Judith Hughes**

Defense Security Service

**Lynn Gebrowsky**

Department of Energy

**Mary Gallion**

Department of Energy

**Geralyn Praskievicz**

Department of Energy

**D. Jerry Rubino**

Department of Justice

**Jeffery A. Moon**

National Security Agency

**Ralph Wheaton**

Department of the Navy

**Thomas O. Martin**

Nuclear Regulatory Commission

**Kimberly Baugher**

Department of State

**Edward S. Wilkinson**

DCI Special Security Center

**William H. Leary**

National Security Council

**J. William Leonard, Chair**

Information Security Oversight Office

**Industry**

**James P. Linn**

Science Applications International Corp.

**Thomas J. Langer**

BAE SYSTEMS North America, Inc.

**Maynard C. Anderson**

ARCARDIA GROUP WORLDWIDE, INC.

**Patricia B. Tomaselli**

Northrop Grumman Corporation

**P. Steven Wheeler**

Lockhead Martin Aeronautics Company

**Michael S. Nicholson**

Washington Group International Government

**Dianne Raynor**

MCA Engineers, Inc.

**ISOO Support Staff**

Laura L. S. Kimberly

Dorothy L. Cephas

Emily R. Hickey

Bernard S. Boyd

Philip A. Calabrese

Margaret L. Rose

Rudolph H. Waddy

Matthew W. Stephan

Lamont K. Taylor

Neil C. Carmichael

Robert L. Tringali

**Observers**

Virginia Hall

Teresa Knott

Gary Weber

Peter R. Nelson