NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE

MINUTES OF THE MEETING

Tuesday, May 10th, 2005

The National Industrial Security Program Policy Advisory Committee (NISPPAC) held its 24th meeting on Tuesday, May 10th, 2005, 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, Introductions and Administrative Matters

As part of regular introductions, the Chair introduced the newest NISPPAC member, Mary Griggs, Deputy Director for Industrial Security, Defense Security Service (DSS). ..

II. Old Business

- **Approval of September 15, 2004 NISPPAC Minutes**

The Chair asked the NISPPAC members if they were ready to approve the September 15th, 2004 NISPPAC Minutes. There were no objections and the minutes were approved.

- **Status of the Implementation of the Declaration of Principles**

The NISPPAC promulgated the Declaration of Principles with respect to clearance reciprocity after the September 15, 2004 meeting and took a leadership role in working with the Cognizant Security Authorities (CSA) to develop a working framework of specifying and defining what reciprocity is. The Declaration of Principles became the foundation for the Personnel Security Working Group (PSWG) proposed reciprocity principles for government. This will result in one set of principles for both government and industry. The Chair noted that after attending many conferences and speaking engagements for security professionals, there is still not a lot of familiarity with the Declaration of Principles and that he has only received two complaints so far concerning reciprocity. The Chair opined that there probably have been more than two incidents concerning this issue since the Declaration of Principles was promulgated.

The Chair also noted the passing of The Intelligence Reform Act in December, 2004 and that a portion of the Act addresses personnel security clearance issues and reciprocity. The Office of Management and Budget (OMB) has a major role in overseeing the implementation of these provisions.

The Chair is optimistic about the National Industrial Security Program (NISP) Implementing Directive. The Order, which was signed in 1995, called for a NISP Implementing Directive. The Directive is in draft form and is pending at the National

Security Council (NSC). The Chair will provide more information about the status of the Directive at the next NISPPAC meeting.

III. New Business

- **Combined Industry Presentation**

Mr. Thomas Langer, NISPPAC Industry representative, gave an Industry Update on behalf of all his fellow industry members which provoked considerable discussion. (Refer to Attachment (5): NISPPAC Industry Update Presentation). Mr. Langer emphasized the following:

- Reciprocity at the working level is still a problem.
- Access has been denied at the 4 to 5 year mark for Top Secret and at the 9 to 10 mark for Secret, while a new investigation was pending.
- Agencies frequently request up to date paperwork when an employee moves from one employer to another.
- These issues have had to be resolved at a very high level, for example at the corporate level of a large contractor to an agency senior security official.

- **Discussion**

The Chair asked if contractors continue to see the same problem from agencies once a clearance problem has been resolved at a high level.

Tom Langer advised that there is still resistance at the working level of an agency to make the same kind of decisions. There have been problems with access to public trust positions at DHS for example. There is a lack of reciprocity which makes it difficult to staff some positions. These positions involve access to sensitive but unclassified information. Active DoD security clearances are not enough at the Department of Health and Human Services (HHS) for example and HHS has been asking contractors to submit HHS paperwork so that the clearances can be readjudicated. The clearances are also reinvestigated which forces the contractor to wait long periods of time for the position to be filled.

The Chair asked about personnel who have security clearances but need access to hazardous materials or sensitive chemical or biological information. He asked about this issue from a DHS perspective. John Young, DHS, stated that he had little information on the issue, but that there are a number of screening programs for truck drivers or personnel who handle hazardous material. The Homeland Security Presidential Directive (HSPD) 12 ”Policy for a Common Identification Standard for Federal Employees and Contractors” is currently at the working group level.

Rosalind Baybutt, DoD, asked if public trust positions were investigated by OPM and how does one check to see if an individual is already being investigated. Tom DelPozzo, OPM, provided that a person would not be reinvestigated if the previous investigation

met certain criteria. He added that OPM will review security clearance paperwork and conduct another investigation if it takes too long to obtain a person's security file from another agency. He further commented that this depends on the customer and OPM only does this if it is necessary. Tom Langer added that there is concern that duplicate investigations will only clog up the system more.

The Chair noted that the Order does not address eligibility for a clearance for other categories besides access to classified information, for example Public Trust positions. Tom Langer stated this issue is of significant concern to industry; specifically, requirements associated with new categories of information like Sensitive But Unclassified (SBU) are starting to appear in the comments section of DD-254's with unique and differing requirements for storage of sensitive information. He continued that the scope of SBU is enormous and appears to be everything that is below Confidential. He specified that there is limited industry research on this issue and the February 2004 Congressional Research Service (CRS) report on this issue clearly captures the wide range of data in government that falls in this category. Mr. Langer provided that Industry recommends two working groups: one for the requirements for clearances in public trust positions requiring access to sensitive unclassified information and proposed solutions to the current stovepipes where a number of agencies have different ways of doing business. The second working group would address SBU requirements being levied as part of the DD Form 254, security classification guidance process.

Tom Martin, NRC, noted that he has found 21 categories of information that fall under the category of SBU. He commented that they include DOE categories, Law Enforcement Sensitive (LES), DHS etc. He added that SBU vetting process needs to be simplified.

Tom Langer provided an update on the following National Industrial Security Program Manual (NISPOM) issues.

- First a Chapter 8, NISPOM white paper on computer security issues. He noted that Industry proposed a white paper and the Defense Security Service (DSS) accepted and proposed two working groups and that may meet by the end of May 2005. One will focus on system accreditation cycle time and the other on the Information Security System Manager (ISSM) self-certification authority. DSS has appointed a lead and industry has been asked to appoint a counterpart. A request for names has been made and there has been a large response.

- Another issue is the 2012 deadline for sub-standard containers to comply with the NISPOM. This issue is moving forward and updates will be provided.

- A third issue which the National Classification Management Society had the lead on is alarm response. Guards must respond to all alarms and the

NISPOM does not allow for cleared employees to respond. Employee response to alarms is a last option. In some cases this has delayed accreditation due to the costs of a guard force response. Most local police departments will not respond to alarms and as a result, contractors have to coordinate a guard force response to alarms. A dialogue with the Office of the Secretary of Defense and DSS on this issue has begun and an update will be provided at a future meeting.

The Chair asked if the sub-standard container issue required a modification to the safeguarding directive. Rosalind Baybutt stated that the 2012 deadline has been in the NISPOM for some time and DoD has already met the standard. The 2012 deadline is for the entire Federal government.

- Tom Langer noted another issue is DHS's Immigration and Customs Enforcement (ICE) office and its the verification of alien status. It is difficult for industry to verify Green Cards or proof of residency as there are many high quality forgeries. Currently it can only be done through ICE. Many non-US citizens are employed as knowledge workers by industry, often by sub-contractors. These companies sometimes employ workers who are in the United States illegally.

  Pat Tomaselli, NISPPAC Industry Observer advised that there have been a number of articles in the press on this issue. These employees have not accessed classified information but are in close proximity to it. They have access to facilities and sometimes have access to International Traffic in Arms Regulations (ITAR) or other regulated information. Contractors do not have access to government immigration data and there needs to be a way to vet personnel. Industry can do this. It is a growing problem. Ms. Tomaselli asked if personnel have used forged documents to gain access to sensitive technology.

  A member of the audience commented in the affirmative, adding that there have been a number of cases of personnel with forged documents gaining access to sensitive areas.

  Tom Langer added that prime contractors are liable for civil or criminal penalties for the actions of their sub-contractors, citing WalMart as a recent example.

  The Chair asked if there have been cases where illegal aliens gained access to sensitive technology. Tom Langer responded that there have been cases and they have been turned over to ICE and the FBI. It is a growing problem.

- Mr. Langer advised that the last item is the MOU agreement revision which has been commented on and involved many industry groups. It was signed in 1993 and not revised after that. Industry asked all groups that were involved to see if they still wanted to participate. The goal of industry is to reach as many sources of information as possible. The draft agreement is in final revision now and calls for the election of a director for the MOU NISPPAC group from a signatory group or a current NISPPAC member. It is the best way to reach out to all of industry, especially for smaller companies who are reluctant to raise these issues themselves.

The Chair commented that the NISPPAC could outline some next steps on the SBU/Public Trust Position issue, perhaps with the two working groups mentioned earlier. The Chair then asked for any additional comments from the government NISPPAC members on the issues raised from the presentation.

Ms. Baybutt proffered that the Personnel Security Working Group (PSWG) should be looking at this issue as they have personnel who represent the clearance entities within their agency. The Chair commented that there is not an appropriate place within government to raise these issues. As a result, many well intentioned government managers have had to decide what to do on their own which has lead to some of the consequences discussed earlier.

The Chair added that he has been contacted by Hill staffers who wanted to know more about SBU access problems. They asked about personnel who already have security clearances having problems gaining access to certain types of unclassified information. As a result, specific language covering this issue was put into draft legislation to ensure that personnel who have security clearances will have access to sensitive unclassified information.

The Chair stated that the NISPPAC could help articulate the issue and put together a small working group of government and industry. The results can be given to the HSPD 12 working group under the Homeland Security Council PCC and other appropriate fora.

John Young, DHS, stated that the plan is to be submitted in June and it will start in October 2005.

Tom Martin, NRC, added that SBU could be an addendum to the Declaration of Principles on Reciprocity. A security clearance should cover all SBU categories. Currently, there is not a document that ties all these types of unclassified information together. Could this be added to the Declaration of Principles?

The Chair noted that the Reciprocity Principles are not meant to craft new policies, but to give existing policies more substance. Most SBU categories are based on statutes and this limits what agencies can do even if they want to. A policy document on this issue may not have much value.

Tom DelPozzo, OPM, advised that OPM has responsibility for the regulations that cover Public Trust positions: 5 CFR 71. Suitability is entirely OPM's responsibility. 5 CFR 71 is in the process of being revised by a working group in OPM. For Public Trust positions, the level of investigation depends upon the employee's level of responsibility. For example usually a NAC, LAC and credit check are conducted for lower level government employees in Public Trust positions. For higher level positions, a background investigation may be needed.

The Chair commented that ISOO is willing to chair a working group on this issue in order to draft a reciprocity white paper to articulate this problem. The Chair asked for a response from those wanting to participate through e-mail by Friday, May 20th, 2005 or at the end of today's NISPPAC meeting.

The Chair also noted that SBU is outside of the scope of the NISP. However, government requirements for protection, handling and storage of SBU are being put in DD-254's. The chair asked the NISPPAC members about the implications of this.

Ms. Baybutt interceded and stated that government requirements for DoD For Official Use Only (FOUO) have always been in DD-254's.

An unidentified audience member stated that private sector security personnel do not know what to do with DD-254's that cover SBU because there is not a clear definition of what SBU is. Who do you report a security violation to? How do you prevent future violations? What are the identification and marking requirements? Protection usually is limited to locking the material in a locked container.

Tom Langer advised that industry recommends a working group to define what the problem is and what industry's position is. This could be done, even though it is outside of the NISPPAC charter.

The Chair stated that ISOO is willing to pull the interested parties together to promulgate this issue. Reciprocity must be tackled first as it is the most immediate issue and then this issue could be handled in a few months at the next NISPPAC meeting.

Mary Griggs, DSS stated that this could be an action item for the MOU. Dissemination of information on this issue is important and anyone interested in this issue could be directed to an internet link

Tom Langer suggested a hyperlink on the DSS website as it is where contractors go for information anyway.

An unidentified audience member commented that this problem is either a bureaucratic problem or a post-adjudicative problem. Even if clearances are adjudicated properly, another agency may want to readjudicate and reinvestigate as two or three years may have passed by since the last investigation and the employee concerned may have a new

issue that has emerged that could affect the clearance which was not present when the clearance was previously adjudicated.

The Chair stated that this is a risk that exists irrespective of the person's status. The system is designed for five year reinvestigations and changing employment does not change the level of risk. He referred to the PERSEREC study in which it was noted that agencies are loath to inherit risk from another agency. The Chair commented that from a national security perspective it is the same risk. National security is not enhanced by agencies refusing to inherit risks. This situation leads to more demands on the investigative process that cannot keep up, thus creating new risks.

- **PSWG Update**

Greg Pannoni, Associate Director for Policy, ISOO gave a brief update on the PSWG.. Copies of "Reciprocity of Access Eligibility Determination" and "Summary of Most Significant Changes" to the "Proposed Adjudicative Guidelines" were distributed.

The "Reciprocity of Access Eligibility Determination" was developed after the last PSWG meeting and is similar to the Declaration of Principles except for a change under Collateral Security Clearances to the amount of time between Periodic Reviews (PR). The PSWG members agreed to 7 years for Top Secret, 10 years for Secret and 15 years for Confidential. Employees shall immediately be granted a security clearance by the gaining activity if the investigation falls within those timeframes. Also, gaining activities may accept investigations greater than those ages on a case-by-case basis.

The Chair gave a brief explanation for that change. Many employees are out of scope for their PR, through no fault of their own. If an employee moves to another company, their clearance will still be honored as it is no fault of their own that they have not been reinvestigated.

Mr. Pannoni advised that the changes are still considered to be a pre-decisional draft, but they should be formally approved by the PSWG soon and will then be sent to the Policy Coordinating Committee for approval.

Mr. Pannoni continued with an update on the proposed New Adjudicative Guidelines and advised that there has been at least one proposed change to each of the 13 adjudicative guidelines. The guidelines have been expanded to provide more detailed guidance.

Also, assistance to the background investigation process was discussed at the most recent PSWG meeting. The DCI Special Security Center has been in discussions with Choice Point and Lexus-Nexus with regard to potential means of garnering data on prospective candidates for a security clearance. The Center intends to conduct a study which will compare data collected through traditional government methods of investigation versus what private sector data providers may provide through other methods such as using various databases. Subsequent to this comparison, the Center intends to evaluate the two data collection methods to determine which is cheaper, faster, more reliable and

concomitantly not subject to exploitation. They expect that the results will provide that some data collected will be the same, some different and some similar.

- **Director of National Intelligence (DNI) Update**

A brief update on the recently created Director of National Intelligence (DNI) was provided by Ms. Mary Rose McCaffrey. The DNI is Ambassador John D. Negroponte and the Principal Deputy Director of National Intelligence is General Michael V. Hayden. An organizational table is not available yet, but they will have four major deputies: (1) Collection, (2) Analysis (3) Management and (4) Customer Outcomes. There will also be a Chief of Staff. So far only the Management position has been filled by Patrick Kennedy, who was Ambassador Negroponte's chief of Staff in New York and in Iraq. Currently, the DNI has the authority to hire up to 500 personnel and many of these personnel will be from other government agencies. He and his staff are currently working on the WMD recommendations and on staffing functions, led by General Hayden. An organizational chart should be available in the next week. The creation of the Office of the Director of National Intelligence is based on the recommendations from the WMD report.

Designation of an oversight entity is being developed. There is an Executive Order covering this issue that is under development. Ms. McCaffrey also referred to the Intelligence Reform and Terrorism Prevention Act of 2004 which requires that a plan be in place for a 120 day clearance cycle. The legislation states that this is resource dependent.

The Chair asked about Director of Central Intelligence Directives (DCID). Ms. McCaffrey explained that they will continue to be in effect until new regulations are written and implemented. The new regulations will be called Intelligence Community Directives. The first seven DNI Directives have been issued and cover the organization of the Office of the Director of National Intelligence. The NISP has not been addressed yet.

- **Sharing of Information with State, Local and Private Sector**

Mr. Paul Hightower, Deputy Director, Infrastructure and Coordination Division, Directorate of Information Analysis and Infrastructure Protection, Department of Homeland Security gave a comprehensive presentation on the Information Protection and Infrastructure Analysis Division Infrastructure Coordination Division. (Refer to Attachment (6): Information Analysis and Infrastructure Protection Directorate, Infrastructure Coordination Division Presentation).

Mr. Hightower made the following comments with regard to his presentation:
He stated that information sharing is critical with new categories of sensitive but still unclassified information being created at DHS and with that information being pushed out to other agencies and the private sector. He highlighted that there are four resource areas and 13 critical infrastructure sectors as laid out in Homeland Security Presidential

Directive No. 7. The Infrastructure and Coordination Division, Directorate of Information Analysis and Infrastructure Protection, Department of Homeland Security is working closely with intelligence offices within Information Analysis (IA) and Infrastructure Protection (IP) depending on the information needed and then determining what can or needs to be shared with the private sector. It is the hub for information sharing and has a close relationship with the private sector and with sector specific agencies. It also has a 24 hour watch center. The final rule for Protected Critical Infrastructure Information (PCII) is still being finalized. Mr. Hightower mentioned that situational awareness is critical and the Infrastructure and Coordination Division works closely with IA/IP intelligence analysts. Sector Coordinating Councils are also being developed for each private industry sector. They are created and run by the private sector and are comprised of representatives of owners/operators. There is also cross-sector coordination in both the private and government. A Homeland Security Information Network (HSIN) is also being created that will have access to SBU information, which will enable both government and the private sector to be informed about critical infrastructure issues that affect them. Information sharing is conducted between the following entities: public to private and private to private. The National Infrastructure Coordination Center (NICC) collects reports of suspicious activity within each sector, which is then reported to the Homeland Security Operations Center (HSOC). Mr. Hightower highlighted the keys to success at the end of his presentation:
(1) Building bridges between DHS and the private sector and between DHS and state and local government;
(2) Share useful and actionable information and;
(3) Communication and coordination with various sectors, for example, the financial sector is in close contact with the Department of the Treasury.

Questions?

Question: Critical Infrastructure Information (CII) guidelines were released by DHS about 18 months ago. How does Sensitive Homeland Security Information (SHSI) interact with CII?

Mr. Hightower: Public Critical Infrastructure Information (PCII) addresses *voluntary* submissions from the private sector that concern critical infrastructure. This information is protected under the Freedom of Information Act (FOIA) and the Critical Infrastructure Act of 2002. The final rule for PCII is still in coordination and has not been approved yet. Industry is concerned about protecting critical infrastructure information. There have been some voluntary submissions, but not very many.

John Young, DHS advised that SHSI is information developed by DHS, state and local or the private sector that concerns terrorism issues and is similar to FOUO. In contrast, PCII is a voluntary submission to government by industry. Much information is shared via secure e-mail.

Question: What methodology are you using to share information with the private sector?

Mr. Hightower: DHS is moving to a Homeland Security Information Network (HSIN) process supported by IA. It is mostly in the form of e-mails and security related bulletins that are sent out to a vetted community.

Critical Infrastructure is a large part of the HSIN. It is the responsibility of the Infrastructure Coordination Division to distribute information to whoever needs it. Often, a recipient may receive the same information from several different sources.

Question: How is classified or sensitive information shared with uncleared individuals in an emergency?

Mr. Hightower: A tear line is needed for release and DHS relies on IA and other members of the intelligence community to do that. The Infrastructure Coordination Division will rely on the sector specialists to determine who needs to be contacted within the sectors. For example, there were terrorist threats to the banking sector last summer. The proper personnel were notified through teleconferences and other means before an official notification to the public was made.

John Young: DHS has procedures for emergency release of classified information. There are designated senior officials within DHS that are authorized to make the decision to release classified information to uncleared personnel.

IV. General Open Forum

Mr. DelPozzo, OPM, mentioned that OPM has five contractors conducting investigations and these contractors are up and running. DSS investigators were also transferred to OPM in February, 2005. The situation is looking good and the necessary resources are mostly available.

Ms. Tomaselli, Industry Observer, asked how many investigators are currently working for OPM?

Mr. DelPozzo stated between 4000-5000 investigators plus support staff. This is a rough estimate. Some contractors are still hiring personnel and others are fully staffed.

V. Closing Remarks and Adjournment

The Chair mentioned that there will be a NISP panel at the American Society for Industrial Security Conference in Orlando, Florida in September 2005. The Chair will be on that panel. The essence of the presentation will be on how the NISP can be made more national. The Chair will coordinate with other panel members, some of whom are on the NISPPAC as well as other government agencies. The Chair would like input and comments from NISPPAC members for this panel. The central theme of the panel will be that the NISP makes more sense now than ever.

The meeting was adjourned at 12.00.

Attachments (6):

(1) Summary of Action Items from the September 15, 2004 Meeting.
(2) Summary of Action Items from the May 10, 2005 Meeting
(3) Agenda.
(4) Attendance Roster.
(5) NISPPAC Industry Update Power Point Presentation
(6) Information Analysis and Infrastructure Protection Directorate, Infrastructure Coordination Division Power Point Presentation

Attachment 1

Summary of Action Items from the September 15, 2004 Meeting

ACTION ITEM	WHO	STATUS
Implementation of the Declaration of Principles *Includes POC at DoD, CIA, DOE and NRC for reciprocity issues on agency website*	J. William Leonard, ISOO	ISOO formally promulgated a "Declaration of Principles" on August 17th, 2004. The "Declaration of Principles" and agency point of contact list have been posted to the ISOO website. ISOO has included the "Declaration of Principles" as an appendix to the draft NISP Implementing Directive. None of the NISP signatories have posted the "Declaration of Principles" and a POC on their website. DoD states that questions pertinent to personnel security clearances may be answered by calling the DSS Customer Support Desk number which is posted on the DSS website. DOE advises that they are in the process of updating their HQ Office of Security website which will link the Declaration of Principles throughout the DOE complex websites. CIA provided that they will look into posting it on their internal and external websites. NRC has taken no action.
Draft change to the NISPOM posted on DoD website	Rosalind Baybutt, DoD representative and Executive agent to the NISPPAC	As of May 10, 2005, the NISPOM change is under review at the DoD Office of General Council.
Sponsorship of industry's initiative to re-engineer the personnel security clearance process. (p.16) *Ms. Baybutt, DoD recommended that industry's proposal be put into a more concrete from and then be presented to the PSWG.*	Mr. Tom Langer, NISPPAC Industry representative.	Mr. Langer advised that he had spoken to Mr. William Leary, NSC, and decided to 'stand down' on this matter due to the enactment of the National Intelligence Act.
Draft NISP Implementing Directive. Comments from NISPPAC members have been reviewed.	J. William Leonard, ISOO	The PCC will convene a group of interested parties (NISP signatories) to come to a consensus on outstanding issues.

Attachment 2

Summary of Action Items from the May 10, 2005 Meeting

ACTION ITEM	WHO	STATUS
NISP Panel at the September 12-15, 2005 ASIS Conference in Orlando, Florida. The Chair requested input and comments from the NISPPAC members.	J. William Leonard, ISOO	Due date for requested input and comments is August 1, 2005.
NISPPAC Issue White Paper on background checks, investigations and adjudications for purposes other than access to classified information.	Greg Pannoni, ISOO	Proposed Terms of Reference on this issue e-mailed to NISPPAC members on June 6, 2005. Response due from NISPPAC members by June 15, 2005 for comments/suggested changes, volunteers and recommendations. Due date was originally May 20, 2005.
NIISPPAC issue white paper on increasing use of DD Form 254 to promulgate requirements to protect SBU	Greg Pannoni, ISOO	Action to occur after reciprocity issue above is addressed.
Draft NISP Implementing Directive	J. William Leonard, ISOO	The PCC will convene a group of interested parties (NISP signatories) to come to a consensus on outstanding issues.

Attachment 3

National Industrial Security Program Policy Advisory Committee Meeting

Tuesday, May 10, 2005
10:00 AM – 12:00 Noon
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. Old Business

- **Approval of September 15, 2004 NISPPAC Minutes** **(5 minutes)**

- **Status of the Implementation of the Declaration of Principles** **(5 minutes)**
  J. William Leonard, Director
  Information Security Oversight Office

III. New Business

- **Combined Industry Presentations** **(30 minutes)**
  Thomas J. Langer
  Industry Representative
  -Summary of MOU Revision
  -Controlled but Unclassified Information
  -Clearance Reciprocity Issues
  -Positions of Trust Investigations
  -NISPOM Chapter 8 Issues

- **Discussion** **(15 minutes)**

- **PSWG Update** **(10 minutes)**
  Gregory Pannoni, Associate Director for Policy
  Information Security Oversight Office

- **Director of National Intelligence (DNI) Update** **(15 minutes)**

- **Sharing of Information with State, Local and Private Sector** **(20 minutes)**
  Paul Hightower, Deputy Director, Infrastructure and Coordination Division
  Department of Homeland Security

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

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

Attachment 4

National Industrial Security Program Policy Advisory Committee

Meeting-Tuesday, May 10, 2005

10 a.m. – noon
National Archives Building

Roster of Attendees

Government

Danny Green
Air Force
Karl Schilling
Central Intelligence Agency
Mary Griggs
Defense Security Service
Geralyn Praskievicz
Department of Energy
John J. Young
Department of Homeland Security
James L. Dunlap
Department of Justice
Thomas O. Martin
Nuclear Regulatory Commission
Andrea G. Jones
Department of State
Tom DelPozzo
Office of Personnel Management
Rosalind Baybutt
Department of Defense
J. William Leonard, Chair
Information Security Oversight Office

ISOO Support Staff

Gregory Pannoni
Philip Calabrese
Jason Hicks
Bruce I Campbell
Jorg J. Wetzel

Industry

Thomas J. Langer
BAE SYSTEMS North America, Inc.
Kent Hamilton
Northrop Grumman
P. Steven Wheeler
Lockheed Martin Aeronautics Company
Donna E. Nichols
Washington Group International
Raymond H. Musser
General Dynamics Corporation
Dan Schlehr
Raytheon
Dianne Raynor
Boeing
James P. Linn
SAIC

Observers

Dave Davis, Industry, ASIS
Kathleen Branch, DoD
Anna Harrison, DOJ
Kirsten Koepsel, AIA
Ed Halibozek, Industry
Michael Yawn, Industry
Dr. Jim Hickok**,** NCMS President
Mary Rose McCaffrey, DSSC
George Ladner, DSSC
Kathy Bevington, CIA
Paul Hightower, DHS/IP/ICD
Stephen Lewis, DSS
Joyce Weymouth, Industry, MOU ISWG Chair