NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE

MINUTES OF THE MEETING

Wednesday, September 15th, 2004

The National Industrial Security Program Policy Advisory Committee (NISPPAC) held its 23rd meeting on Wednesday, September 15, 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.

The Chair opened the meeting by presenting an ISOO coin to the current NISPPAC members in appreciation of the contributions they have made to the NISPPAC. Kent Hamilton and Dan Schlehr, both new industry members, were introduced by the Chair as was John Young, the new Department of Homeland Security (DHS) representative. The Chair also announced the appointment of five representatives to the Public Interest Declassification Board (PIDB) by the White House and discussed the history of the legislation. The Chair also mentioned that the PIDB is a legacy of the Commission on Reducing Government Secrecy, known as the Moynihan Commission after the late Senator Moynihan. There are still four members that need to be appointed by Congress and the Chair is optimistic that this will take place due to the interest that the legislature has in classification and declassification issues.

II. Briefing on Protected Critical Infrastructure Information

The Chair noted that Emily Hickey, formerly a Senior Program Analyst at ISOO, arranged to have Frederick W. Herr, Program Manager, Protected Critical Infrastructure Information (PCII) Program, Information Analysis and Infrastructure Protection (IAIP) Directorate, Department of Homeland Security (DHS), give a presentation on Protected Critical Infrastructure Information (PCII).

Mr. Herr's Power Point Presentation:

Protected Critical Infrastructure Information (PCII) Program
Fred Herr, PCII Program Manager

Critical Infrastructure

- Critical Infrastructure is the assets, systems, and industries upon which our national security, economy and public health depend.

- The Department of Homeland Security has the responsibility for coordinating the protection of our nation's critical infrastructure across all sectors.

85 % of critical infrastructure is privately held.

Perceived Barrier to Sharing Information: The Freedom of Information Act (FOIA)

"…we urge you to support legislation similar to the Y2K Information and Readiness Disclosure Act that would protect critical infrastructure protection information voluntarily shared with the Government from disclosure under FOIA and limit liability."

- Letter to President Bush from National Security Telecommunications Advisory Committee, June 28, 2001

"Companies are concerned that information voluntarily shared with the government that… concerns corporate security may be subject to FOIA… Sensitive information may fall into the hands of terrorists, criminals, and other individuals and organizations capable of exploiting vulnerabilities and harming the U.S."

— Open letter to U.S. House of Representatives from several major U.S. corporations, July 5, 2001

Critical Infrastructure Information Act of 2002 (CII Act)

- Protects voluntarily submitted critical infrastructure information from Disclosure under the Freedom of Information Act
- Use in civil legal actions
- Disclosure under state and local "sunshine" laws

Program Establishment and Implementation

Notice of Proposed Rule Making – 4/15/2003
Program Office Established – 2/11/2004
Interim Rule Published 6 CFR 29 – 2/20/2004
Final Rule Published – Q4 2004 (est)

Process for Obtaining Protection

- Submission of information must:
  - Include Express Statement requesting protection
  - Include Certification Statement
    - All information is voluntarily submitted.
    - Submitted for purposes of the CII Act.
    - Not submitted in lieu of independent compliance with a federal legal requirement.
    - Submitter understands that false representations may constitute violation of 18 U.S.C. Section 1001
  - Meet the definition of CII in the Act.

What is Critical Infrastructure Information?

Information defined by the CII Act including:

- Threats - Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation.
- Vulnerabilities - Ability to resist threats, including assessments or estimates of vulnerability.
- Operational experience - Any past operational problem or planned or past solution including repair, recovery, or extent of incapacitation.

CII meeting all requirements becomes PCII
(Protected Critical Infrastructure Information)

Validation Process for PCII

<u>Submissions from:</u>

- Private Industry
- Information Sharing and Analysis Organizations (ISAO)
- State/local governments

PCII Program Office:

- Checks for Express Statement
- Verifies receipt of required certification Reviews submitted information
- Determines if information meets definition of CII

Meets criteria?

Yes - Makes available to authorized users.
No - Submitter offers further justification. If still no:
1) Can request information be destroyed; or
2) Allow DHS to use information without CII Act protection

PCII Safeguards

PCII Program safeguards ensure that all submitted information is:

- Accessed only by authorized individuals
- Used only for allowable purposes
- Stored, handled, and disseminated only in ways specified by PCII Program Manager

Accomplishments to Date

- Program in place and operational; adjusting to changing requirements
- Partnering with DHS divisions and private sector to expand use of the PCII Program
  - National Cyber Security Division for submissions of cyber security information
  - Electric Power ISAC for outage reports
  - Trucking ISAC for incident reports
  - National Infrastructure Protection Plan
- Interest from other agencies
  - Agriculture – cattle tracking
  - EPA – Water treatment facilities; Methyl Bromide facilities

Next Steps

- Issue final rule
- Streamline recurring submission processes
- Accept electronic submissions
- Expand the PCII Program to include all Homeland Security directorates, other federal agencies and state and local governments

Contact Information

PCII Program Office
Department of Homeland Security
245 Murray Lane, SW
Building 410
Washington, DC 20528-0001

202-360-3023
www.dhs.gov/pcii
pcii-info@dhs.gov

Mr. Herr began the briefing by mentioning that PCII is part of the Homeland Security Act of 2002. The PCII Office was created on February 20, 2004. PCII is a category of government information that will be shared throughout the Federal, state and local governments for homeland security purposes. 85 percent of the information provided to the PCII Office is from the private sector, mostly from public utility companies. About 15 percent of the information is from state and local governments as well as a small percentage from other parts of the Federal government. Most of this information is business sensitive and/or trade secret information. However, the Federal government needs access to this information in order to determine vulnerabilities. Mr. Herr illustrated two hurdles to sharing this type of information with the Federal government: (1) If the information is provided, will the government be able to protect it from disclosure? For example, could this information be released through the Freedom of Information Act (FOIA)? (2) Will private sector companies that share this information be liable for fixing problems that could be identified with this type of information? Mr. Herr also pointed out that the PCII initiative was not only in response to the events of 9/11. Instead, this initiative has been necessary for some time and some work on it had already been done prior to 9/11.

Mr. Herr then continued with his presentation. If critical infrastructure information from the private sector is voluntary shared with the PCII Office the following will occur: (1) The information will be covered under a statuary exemption to the FOIA, exemption B (3), (2) the information will not be able to be used in civil litigation and (3) the information will not be subject to state or local sunshine laws which are similar to the FOIA.

Mr. Herr stated that the interim rule was issued after an open comment period. 120 comments were submitted for the interim rule and another 32 comments have been provided so far for the final rule, which is currently being prepared and is scheduled to be finished by the end of 2004.

Mr. Herr briefly explained that he was appointed by Under Secretary Libuti, IAIP, as the Program Manager for PCII. The PCII Program office is located within the Information Assurance (IA) Directorate, which is within the IAIP Directorate, DHS.

Mr. Herr then explained that for information to be validated as PCII, it must meet the following four conditions:
1. Applicants must make an explicit statement in which they must ask for protection of the information that they are submitting. However, all information provided is covered under an assumption of protection from release by the FOIA until a final determination has been made.
2. Applicants must be aware that the information is not protected from FOIA when it is sent to another Federal agency other than the PCII Office.
3. The applicant must state that the information is true. There are legal penalties attached to this requirement.
4. The information must meet the definition of critical infrastructure information.
If the information meets these four criteria, it will be certified as PCII.

The information submitted to the PCII Program office comes from a number of sources including Information Sharing and Analysis Organizations (ISAO), Critical Infrastructure Information Sharing and Analysis Centers (ISAC), state and local government as well as other agencies within the Federal government. If the information cannot be validated as PCII, there are other options: a B (4) FOIA exemption, destroying the information or withdrawing it.

If the information is validated as PCII, only authorized users from Federal, state and local agencies can have access to it. Federal employees are subject to penalties if they release PCII, other users are not. The PCII Program office will determine how PCII is stored and shared. Mr. Herr stated that there will have to be an accreditation process for PCII holders in order to ensure consistency.

There have only been 27 submissions since the PCII Program's inception in February, 2004. This number is low, but the lack of submissions has allowed the PCII Office to adjust the submission process.

There are also many pilot programs and other possible uses for PCII information. For example, the Department of Agriculture could use it to track cattle from birth to death and the Environmental Protection Agency (EPA) could use it to keep track of dangerous chemicals like bromide.

The submission process also needs to be streamlined, as it is currently not possible to submit applications electronically as a signature is a requirement under the Homeland Security Act of 2002.

Mr. Herr was asked a number of questions by NISPPAC members as well as members of the audience:

1. A question was asked about sharing information internationally.
Mr. Herr: The interim regulation is unclear on this issue and will it be clarified in the final regulation. No PCII information will be shared with foreign governments or other international requestors unless permission has been granted by the entity that provided the information to the PCII Office.

2. Are SHSI (Sensitive Homeland Security Information) and PCII the same?
Mr. Herr: No, SHSI was not provided with a statuary exemption to the FOIA, so PCII is protected more strongly than SHSI. Also, PCII is narrower in focus as it cannot be government-generated information. Finally, PCII is information that is submitted from the private sector.
Mr. John Young, DHS, stepped in and explained that SHSI is similar to FOUO (For Official Use Only), OUO (Official Use Only), LES (Law Enforcement Sensitive) etc. Its focus is mostly on terrorism and consists of information that is generated by Federal agencies.

The Chair presented Mr. Herr with an ISOO coin for his presentation and in appreciation of his efforts in establishing the PCII Program.

III. Old Business

The Chair introduced Mr. James Dunlap, Department of Justice (DOJ), as a new member of the NISPPAC.

The Chair began by mentioning old business items:
The Chair is looking for input on the Declaration of Principles, an action item from the last NISPPAC meeting in March 2004. The Chair thanked Jerry Schroeder and Laura Kimberly for their efforts in drafting the Declaration. The Chair stated that the hard part of this effort will be its implementation. The four NISP signatories (CIA, DoD, DOE and the NRC) have received a copy of the Declaration with a letter asking them to implement the principles.

- Status of Implementation of the Declaration of Principles

Department of Defense (DoD) Representative.
Ms. Rosalind Baybutt, the DoD Representative stated that she supports reciprocity and that it is not an issue within DoD. If industry has an issue with a personnel security clearance they can call the Customer Support Desk at DISCO. There are currently 9300 accounts in the new adjudication database. Industry also has access to the database to see if an individual moving from one company to another is eligible for access to classified information. This database includes SCI and SAP's as well as personnel that work at DoD intelligence agencies. DISCO is the point of contact for all clearance issues at DoD. The Chair asked about the dissemination of information. Ms. Baybutt stated that this has not been discussed so far, but that industry knows where to go. Also, the Declaration of Principles has not been posted on the DoD web site yet.

Central Intelligence Agency (CIA) Representative.
Ms. Alvina E. Jones, the CIA representative stated that CIA fully supports reciprocity as stated in the Declaration of Principles. CIA is also working to create a secure point of contact and secure channel for industry to contact CIA security. This will be the challenge and goal for the next fiscal year and indicated that she could not be more specific in an unclassified environment. It is also a challenge to protect the association that CIA has with industry, hence the need for a secure channel. Ms Jones said that she would get back to the Chair about dates and deadlines. Finally, industry can always contact the CIA clearance division if they have access problems. Also, Ms. Jones stated that Brian Dunbar is the current head of the security clearance program.

Department of Energy (DOE) Representative:
Ms. Geralyn Praskievitz, the DOE representative stated that DOE fully supports reciprocity. If industry has clearance problems they can contact the Director, Office of Security for resolution. The Declaration of Principles has not been distributed to DOE contractors yet. DOE would also like additional implementation guidance. DOE also plans to implement the Declaration of Principles throughout the agency. There will be a hyperlink to the Declaration of Principles on the DOE web site.

Nuclear Regulatory Commission (NRC) Representative:
Mr. Tom Martin, the NRC Representative stated that NRC is already implementing the Declaration of Principles. NRC does not foresee a change in how they do business. The agency is committed to reciprocity and fully supports the Declaration of Principles.

Industry Representative:
Ms. Pat Tomaselli, an industry representative stated that some companies that have classified contracts also have other business that is non-defense related. In this particular situation, the reciprocity issue would be dealt with in the defense arm of the company. A position would be created to handle reciprocity issues and the person hired for that position would work with the appropriate government point of contact to resolve reciprocity issues. Ms. Tomaselli stated that reciprocity is a major issue for industry.

The Chair asked the NISPPAC representatives if the Declaration was worth anything to industry.

Ms. Praskievitz, DOE, said yes. DOE doesn't think that reciprocity is a problem, but the Declaration of Principles is a good way to find out. An industry representative stated that the Declaration will be a focal point for these issues. Most problems are usually at a low level, for example questions about the scope of an investigation. The test will be if new issues will arise over the next year. The Chair stated that he believes that this is a fundamental issue with people not understanding what reciprocity really means. An industry representative stated that additional paperwork is not the issue, but that stating the job is. The Chair concluded that he expects more to come and for everyone to keep following these issues.

IV. New Business

The Chair mentioned an article in a special advertising section of the September 14, 2004 Washington Post Express on a Defense Technology Career Fair. The article is titled "Progress

Reported in Reform of Security Clearance Process", by Sheryl Silver on the current security clearance situation.

- **Executive Agent's Update**

Ms. Rosalind Baybutt, the Department of Defense Representative and Executive Agent to the NISPPAC, stated that the change to the NISPOM is being prepared and that it will be released in the next few days, once it has been signed by Ms. Carol Haave, Deputy Undersecretary of Defense for Counterintelligence and Security. Copies of the letter were passed out and she explained it is available on the DSS website. The letter is in a password protected part of the web site and that one must register first with DSS to gain access. Comments on the changes are expected due to DoD by November 15, 2004. No changes have been made to Chapter 8. Industry is being offered an opportunity to participate by commenting on the changes, however all comments must include a rationale. Ms. Baybutt also mentioned that the DSS to OPM transfer is still being worked out and has not occurred yet. Finally Ms. Baybutt commented on fee for services. The budget for the estimated costs of contract personnel investigations has been submitted through FY 2011. In the past those projections have been very accurate.

- **Update on Signatories' Personnel Security Clearance Program**

Mr. Stephen E. Lewis, Department of Defense/Defenses Security Service (DoD/DSS) Representative:
Mr. Lewis began by pointing out that interim determinations are being made within three days and final assessments are being made within five days at DISCO. There are 16,000 cases still pending in the DSS system. All new cases are going to OPM, even though the transfer hasn't taken place yet. DISCO is honoring cases that are from other agencies. There is not any data available yet on OPM's progress due to the short time period that OPM has been responsible for personal security investigations. DISCO does not adjudicate SCI clearances yet, but this issue is being looked at. There is not a projected date yet for this decision.

Alvina E. Jones, Central Intelligence Agency (CIA) Representative:
Ms. Jones stated that CIA would not provide any processing or metrics data as it is at a classified level. The agency has formed a panel of internal experts from personnel security and CIA's industrial program to look at initial access and crossover problems. This panel recommended several changes. Most of the changes were implemented and the cycle times for crossovers were reduced by 50%. There has also been a reduction in the cycle time for initial clearances, although not as significant as with crossovers. The Chair asked if CIA could specify the reduction in time. An industry representative responded that the crossover time has been reduced to one week from 30 days in the last six months.

Ms. Geralyn Praskievitz, Department of Energy (DOE) Representative:
Ms. Praskievitz provided a Power Point presentation.

DoE Personnel Security Program
Mr. Marshall Combs, Director, Office of Security September 2004

Secretary of Energy
Deputy Secretary of Energy

Under Secretary for Nuclear Security/Administrator, NNSA

Under Secretary for Energy, Science & Environment

Staff Offices (16)
Including:
Security and Safety
Performance Assurance
Intelligence
Counterintelligence
General Counsel
CIO
Mgmt, Budget and CFO

Personnel Security Program

"Q" and "L" access authorizations granted at 9 locations:
-Albuquerque Service Center (all NNSA cases)
-Chicago
-Idaho
-Oak Ridge
-Pittsburgh
-Schenectady
-Savannah River
-Richland
-Headquarters

Access Authorizations by Location

	Federal	Contractor	Total
Albuquerque	1,832	50,232	52,064
Chicago	167	2,323	2,490
Idaho	212	3,364	3,576
Oak Ridge	586	8,575	9,161
Pittsburgh	610	7,016	7,626
Richland	137	1,980	2,117
Savannah River	376	11,435	11,811
Schenectady	161	5,807	5,968
Headquarters	9,170 *	2,470	11,640
Total	13,251*	93,202	106,453

*Includes 6,684 OGA

NNSA Consolidation to Albquerque Service Center

- Consolidation effort to be completed in FY-2004
- Cases from Oakland, Nevada and Y-12 portion of Oak Ridge
- ALB will process these new cases plus Los Alamos, Sandia (2), Pantex, Kansas City, Rocky Flats, Mound, Carlsbad

Timelines Within DOE

Prescreening		**Adjudication**					
		clear	**all**				
FY 2002	45	46 (3101)	61 (5765)	FY 2004	45	43 (3179)	58 (6342)
FY 2004	35	68 (3522)	78 (6210)				

Investigation Completion Times

FY 2000	59
FY 2001	61
FY 2002	81
FY 2003	160
FY 2004	264 * ytd as of 6/2004

Reciprocal Grants at DOE Headquarters

- FY 2003 - 746
- FY 2004 ytd – 674
- These numbers do not include intelligence agency cases
- Approximately 3% of requests do not meet standards for reciprocal grant
- DOE has contact with 65 Other Federal Agencies

Accelerated Access Authorization Program

- Interim option available to all applicants for "Q"
- Adds Counterintelligence-scope poly; drug testing; psychological testing to NACC
- Approximately 500 cases this FY; 4000 cases since inception in 1991
- Processing time to grant less than 5 days from completion of testing elements

DOE's use of JPAS

- DOE checks DCII routinely with direct connection
- DOE accesses JPAS through OPM's PIPS system
- DoD systems checked whenever individual indicates DoD employment or clearance

Ms. Praskievitz made the following comments with regard to her presentation: Prescreening times, in other words, the amount of time that it takes to send a signed SF- 86 to OPM, are going down. The average is 65 days, although there are some cases that have thrown the average off, but seven days is considered good, and many take just a few days. Personnel security investigations are conducted by OPM or the FBI as DOE does not conduct its own personnel security investigations. The processing times for security clearances are going up at DOE as the new service center just stood up. There is a 3% rejection rate for reciprocal clearances from other agencies, usually because there is not enough information on the SF 86. It usually takes one day to determine if the clearance can be passed. DOE also conducts accelerated processing through the Accelerated Access Authorization Program (AAAP) for initial Q clearances. AAAP consists of a counterintelligence polygraph, psychological tests and a drug test. The program costs $800 per person. 500 cases have been processed so far in FY 2004 and 4000 since AAAP began in 1991. The employer pays for the travel, i.e. an overnight hotel room and flight. The most contentious issue for contractors has not been the polygraph, but liability as the applicants are usually just prospective employees.

An industry representative asked about online access and DOE's eligibility requirements. DOE Security can check the JPAS through OPM's PIPS system and can check DCII directly. DoD systems are checked when an individual indicates on their SF-86 that they have a DoD clearance.

Mr. Tom Martin, Nuclear Regulatory Commission (NRC) Representative:
Mr. Martin stated that the NRC clearance program is being expanded to include some of its 'licensees'. The volume of clearances granted by NRC to contractors is not very high, and NRC does rely on DOE clearances for some of its contractors, such as at the National Labs. NRC also is relying on DHS for clearances for state and local personnel in order to share threat and vulnerability information with them. NRC also relies on OPM for security investigations.

Winona Varnon, Office of Personnel Management (OPM) Representative:
The OPM representative indicated that there are three elements to OPM's personnel security clearance initiative.
1. OPM has signed contracts with five companies to conduct personnel security investigations and is expecting the first set of completed investigations from them in January. The contractors are Omniplex, MSM, CACI, Kroll, and Sa-Tech, as well as USIS, which has been conducting personnel security investigations for OPM. Investigations usually have deadlines of 35, 75 and 120 days depending upon the level of clearance required.
2. OPM is working with DoD to train DSS agents and support staff on the Personnel Investigations Processing System (PIPS**)** and is developing universal standards. PIPS processing has been operational since February, 2004. OPM will have statistics available in FY 2005.
3. OPM is conducting electronic data transfer with DoD to avoid multiple input of the same data on the same system. This effort will avoid duplicate data on PIPS and Electronic Questionnaires for Electronic Processing (EQIP). These initiatives should reduce processing times.

The OPM representative also informed the NISPPAC that the SF-85 and SF-85P will be available on EQIP in October, 2004; and that the SF-86 has been approved and will be available soon.

An industry representative asked OPM about contractor use of EQIP. The OPM representative responded that DoD is currently conducting beta testing and that EQIP will eventually be available to contractors.

- **Industry Update – Re-Engineering the Clearance Process**

Mr. Tom Langer, Industry Representative:
Mr. Langer provided a Power Point presentation that represented an industry consensus view of the clearance process issue.

NISPPAC Industry Proposal: Re-engineering the Clearance Process

Current System:

- The current system has a fragmented investigative process.
  - The lack of confidence in the investigative process has created myriad clearance systems (DSS, NSA, CIA, NRO, Special Access community, etc)
- What is advertised as compartmentalization is really each agency reducing the risk for access to their information.
- Millions of dollars are collectively being spent to provide up to the minute assurances that a candidate for access poses minimal risk.
  – Even with an existing clearance, any new access will require some form of reinvestigation.
- The system is broken and dated – we need to invest in a new system that everyone can have faith in.

Industry Proposal:

- Re-engineer the clearance process to create a *true* national system for access to each level and a system of continuous review.
  - Have all NISP signatories and industry involved in establishing the process.
  - Create one executive branch clearance agent.
  - Use the strides made in behavioral research, psychological profiling and online databases to improve adjudication and risk reduction.
  - Invest in access to online data bases, fund development of state databases where needed.
- Create a new system that verifies the trustworthiness of candidates, and then checks who they have become.

Benefits of Re-engineering:

- One standard of investigation for each level of classified information.
- Utilize "special adjudications" for information and programs that truly need extraordinary protection.
- Make need-to-know the core criteria for access.
- Eliminate the duplicate investigative processes and therein reciprocity issues.
- Reduce the costs associated with our current emphasis on risk avoidance.
- Enhancing the overall mission of security by eliminating endless access paperwork.

- **Discussion**

There was collective agreement on the presentation by the industry participants. Several comments were made about the presentation: There is a lack of consistency with personnel security clearances. The clearance system itself is also very fragmented**.** Agencies are trying to reduce their risk because they do not trust the existing system. Industry feels that the clearance process needs to be completely reengineered.

Industry indicated that its security personnel are overwhelmed with redundant paperwork. When industry was tasked with cleaning up Joint Personnel Adjudication System (JPAS), they became concerned with the amount of inaccurate information in the system. This led to questions about the overall quality of the data. Ms. Tomaselli, Industry pointed out that Contracting Officer Technical Representative (COTR) personnel also spend time dealing with security issues, which is very resource consuming. Most contractors no longer have the administrative staff necessary to do most of this work. A step back needs to be taken.

The Chair asked the NISPPAC members if this lack of confidence is justified.

An industry representative mentioned the JPAS clean-up again that contained large amounts of inaccurate data. The representative pointed out that many employees in the private sector frequently change jobs and companies and these actions were not tracked well in JPAS. However, industry has become better at submitting timely and accurate data but there are still lingering questions about the accuracy of the data.

The Chair asked about level of quality of the adjudications process. For example, NSA does not concur with the Declaration of Principles as it does not trust the accuracy of other agencies data on clearances.

Ms. Jones, CIA, stated that the agency recognizes the need for uniform investigator and adjudicator training. CIA believes that it is engaged in addressing the problem.

An industry representative pointed out that even cleared government personnel that enter the private sector often have to start the clearance process over again, even though they have held a security clearance for many years. The representative questioned why this is done as it is a waste of money. There is a need for standardization within the system as well as integrity and continuous checks.

Mr. Martin, NRC pointed out that a 1950's process is being used to tackle a 21st century problem. He asked if there has been any high level research on risk and vulnerability assessments in the personnel security clearance system. He also asked if there is an organization that can put together some proposals or recommendations.

Ms. Tomaselli, Industry, commented that when the National Industrial Security Program Operating Manual (NISPOM) emerged from the old ISM, there was a lot of industry input. She asked how industry should handle situations where an employee is cleared for one program, but not for another.

Ms. Baybutt, DoD mentioned the JPAS system. An individual's clearance information will be available on-line to adjudicators throughout government. As a result, adjudicators will be able to look at an individual case and see what previous adjudication decisions were made. She also told the NISPPAC members that DoD plans to have one standardized adjudication course for all of the DoD community.

The Chair asked the NISPPAC members what the next steps are.

Mr. Langer, Industry stated that industry is looking for sponsorship of their initiative to reengineer the personal security clearance process. There is a legislative push currently taking place and industry is trying to mitigate legislation that could be implemented without any input. Industry does not want to be in position where it is reacting to legislation that will not be a good solution to the problems that industry is facing. Industry wants legislation that it can buy into rather than be directed to do.

The Chair asked for input from the NISPPAC members. Specifically, what sort of committee do they want? The Chair also asked the NISPPAC members if they wanted their response to be for the record.

The OPM representative stated that there are too many any agencies involved to reengineer the entire process. The representative felt that everyone could join the efforts taking place and point them in one direction, which would standardize the process.

Mr. Ralph Wheaton, the Navy representative stated that standardization is not going to happen if agencies do not buy into the effort.

Ms. Jones, the CIA representative, noted that everyone agrees on uniform standards. However, everyone also has to agree on how to get there.

The Chair asked the NISPPAC committee what they wanted to do.

Ms. Baybutt, the DoD representative, asked that industry come up with something more concrete and for it to be brought up before the Personnel Security Working Group (PSWG). DoD is also willing to facilitate this effort. She also noted that industry will also have more of a voice in the PSWG as a result.

Discussion continued about the PSWG and what could be achieved at that forum.

The Chair stated that he would be willing to facilitate in any way for industry to have a voice at the PSWG. The chair also stated that Bill Leary at the NSC would also like input from industry and that they should pursue contact with the PSWG, PSC and PCC.

V. General Open Forum

No comments were made.

VI. Closing Remarks and Adjournment

The Chair mentioned the NISP implementing directive and the incorporation of the Declaration of Principles again. Another draft of this directive for agencies to comment on will be available soon. The Chair also thanked Ms. Pat Tomaselli for her contributions to the NISPPAC and presented her with the first ISOO award, as it is her final meeting at the NISPPAC as an industry representative. The Chair announced that the next NISPPAC meeting is tentatively scheduled for the Spring of 2005, unless a significant event requires a meeting before then. NISPPAC business will be conducted electronically in the meantime.

The meeting was adjourned at 12.10.

Attachments (5):

(1) Declaration of Principles.
(2) NARA Press Release, August 17, 2004 on the Declaration of Principles.
(3) Summary of Action Items from the September 15, 2004 Meeting.
(4) Agenda.
(5) Attendance Roster.

Attachment 1

Declaration of Principles for Reciprocity of Access Eligibility Determinations Within Industry

Delays in security clearances and in access to highly sensitive programs (Sensitive Compartment Information, Special Access Programs, Q Clearances, and similar programs) are a matter of concern from an economic, technological, and national security perspective. Failure to reciprocally honor clearance and access actions by another agency hampers industry's ability to be responsive to Government's needs. In addition, as agencies struggle to reduce processing times, mutual and reciprocal acceptance of investigations and adjudications by all agencies makes even more sense today. Duplicative actions create unnecessary delays, needlessly consume limited resources, and place national security at risk by further delaying the return of equilibrium to the personnel security clearance process.

In furtherance of Executive Order 12968, "Access to Classified Information," Section 2.4, reciprocal acceptance of access eligibility determinations by National Industrial Security Program (NISP) cognizant security authorities (CSAs) for industrial personnel will be implemented in the following manner:

Collateral Security Clearances

- An employee with an existing security clearance (not including an interim clearance) who transfers or changes employment status (e.g. contractor to contractor or government to contractor, etc.) is eligible for a security clearance at the same or lower level at the gaining activity without additional or duplicative adjudication, investigation, or reinvestigation, and without any requirement to complete or update a security questionnaire unless the gaining activity has substantial information indicating that the standards of Executive Order 12968 may not be satisfied.

  – The "substantial information" exception to reciprocity of security clearances does not authorize requesting a new security questionnaire, reviewing existing background investigations or security questionnaires, or initiating new investigative checks (such as a credit check) to determine whether such "substantial information" exists.

  – The gaining activity may request copies of background investigations and/or security questionnaires from the existing or losing activity for purposes of establishing a personnel security file, but eligibility for a reciprocal security clearance may not be delayed nor may there be additional or duplicative adjudication after the documents are received.

  – A security clearance is confirmed by the CSA of the gaining activity by verifying with the existing or losing activity or its CSA, as appropriate, the level of and basis for the security clearance. Where possible, automated data bases should be used to confirm security clearances.

- If the most recent investigation is not "current" in accordance with approved investigative standards an employee will immediately be granted a security clearance at the gaining activity provided the employee has completed and submitted all appropriate questionnaires, waivers, and fingerprints at either the losing or gaining activity.

Highly Sensitive Programs

- "Highly sensitive programs" means Sensitive Compartmented Information, Special Access Programs, Q Clearances, and other similar programs.

- The principles of reciprocity for collateral security clearances set forth above are also applicable for access to highly sensitive programs with the following exceptions:

  – Where the sensitivity level of the new highly sensitive program is not the same as the existing program to which the employee has access; or

  – Where the existing access to a highly sensitive program is based, under proper authority, on a waiver of or deviation from that program's adjudicative or investigative guidelines, or where the access is conditional, interim, or temporary.

- The sensitivity level of highly sensitive programs is determined from the investigative and adjudicative standards that are established at the time the program is approved; if programs use the same criteria for determining access, they are at the same sensitivity level.

  - If additional adjudication or investigation is necessary because a highly sensitive program is not at the same sensitivity level as the program to which the employee currently has access, only additional – not duplicative – investigative or adjudicative procedures may be pursued. Any additional investigative or adjudicative procedures will be completed in a timely manner.

Reporting of Practices Inconsistent With These Principles

- Each CSA shall designate in writing a point of contact for industry to report practices contrary to these principles, and the points of contact will be published on appropriate websites, such as sites of the Defense Security Service, the Information Security Oversight Office, and CSAs.

- Any such reports shall be submitted through the corporate security office for each cleared company/corporation and will be resolved in a timely manner. In cases where only one sector or division of a corporation is cleared, the

corporation shall establish a cleared contact in that sector or division to accept reports for the corporation.

- For the purpose of establishing statistics regarding the effectiveness of this declaration, CSA points of contact and industry shall provide copies of reports of practices contrary to these principles and their resolution to the Information Security Oversight Office.

DRAFT

Attachment 2

FOR IMMEDIATE RELEASE August 17, 2004

New Guidelines for Reciprocity of Security Clearances in Industry Issued by ISOO

Washington, D.C. . .On August 6, 2004, the Information Security Oversight Office (ISOO), took steps to address reciprocity of security clearances within industry. ISOO formally promulgated and forwarded to the Secretaries of Defense and Energy, the Acting Director of the Central Intelligence Agency and the Chairman of the Nuclear Regulatory Commission for immediate implementation, a "Declaration of Principles" that provides a clear articulation of how agencies must reciprocally honor security clearances granted by other agencies with enough specificity and substance that industry can hold Government agencies accountable for their actions. Bill Leonard, Director of ISOO, asked that these agency heads disseminate the Principles to their cleared contractors and designate an appropriate point of contact for industry to report any instances when these Principles are not being followed.

The National Industrial Security Policy Advisory Committee (NISPPAC), which is comprised of both industry and government representatives and chaired by the Director of ISOO, developed this "Declaration of Principles" concerning reciprocity of security clearances within industry. The Chair, Mr. Leonard, commented that: "While it should provide some relief to the current personal security clearance crises within industry, it is not a silver bullet. However, it should allow contractors who experience failure on the part of a Government program or contract office to honor reciprocally a clearance action by another Government agency to seek immediate redress".

Industry officials supporting the defense and intelligence agencies have repeatedly pointed out that delays in the security clearance process for its employees cause major inefficiency, which eventually leads to higher costs for the taxpayer and ultimately harm national security. The lack of reciprocity between agencies, where one agency refuses to accept the clearance of another agency, has significantly contributed to this problem. In the coming weeks, cleared industry with defense and intelligence related contracts should receive more detailed implementation guidance from their government customers.

Established in 1978, ISOO is responsible to the President for overseeing the government-wide security classification program in both Government and industry, and receives policy and program guidance from the National Security Council. ISOO's authority is found in two Executive orders, Executive Order 12958 as amended, "Classified National Security Information," and Executive Order 12829, as amended, "National Industrial Security Program." ISOO has been a component of the National Archives and Records Administration since 1995.

A copy of the Declaration of Principles can be found at:
http://www.archives.gov/isoo/industry/isoo_industry_main.html

# # #

For press information, the media should contact the National Archives Public Affairs staff at 202-501-5526.

DRAFT

Attachment 3

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	Comments were due to DoD by Nov 15, 2004. Follow-up with the Executive Agent on Feb 11, 2005 provided that the changes are awaiting a reply from one of the NISP signatories.
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.
NISP Implementing Directive. Comments from NISPPAC members have been reviewed.	J. William Leonard, ISOO	The draft NISP Implementing Directive is being coordinated with the NSC as of February, 2005.

DRAFT

Attachment 4

National Industrial Security Program Policy Advisory Committee Meeting

Wednesday, September 15, 2004
10:00 AM – 12:30 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. Briefing on Protected Critical Infrastructure Information (30 minutes)
Frederick W. Herr, Program Manager
Department of Homeland Security

III. Old Business

- **Status of Implementation of the Declaration of Principles (20 minutes)**
  Department of Defense Representative
  Central Intelligence Agency Representative
  Department of Energy Representative
  Nuclear Regulatory Commission Representative
  Industry Representative

IV. New Business

- **Executive Agent's Update (10 minutes)**
  Department of Defense Representative

- **Update on Signatories' Personnel Security Clearance Program (25 minutes)**
  Department of Defense/Defenses Security Service Representatives
  Central Intelligence Agency Representative
  Department of Energy Representative
  Nuclear Regulatory Commission Representative
  Office of Personnel Management Representative

- **Industry Update – Re-Engineering the Clearance Process (15 minutes)**
  Industry Representative

- **Discussion (30 minutes)**

V. General Open Forum (5 minutes)

VI. Closing Remarks and Adjournment (5 minutes)

DRAFT

Attachment 5

National Industrial Security Program Policy Advisory Committee

Meeting-Wednesday, September 15, 2004

10 a.m. – noon
National Archives Building

Roster of Attendees

Government

Walter L. Bishop
Department of the Army
Alvina E. Jones
Central Intelligence Agency
Steven E. Lewis
Defense Security Service
Geralyn Praskievicz
Department of Energy
John J. Young
Department of Homeland Security
James L. Dunlap
Department of Justice
Catherine Van Arsdel
National Aeronautics and Space Administration
Winona H. Varnon
Office of Personnel Management
Ralph Wheaton
Department of the Navy
Thomas O. Martin
Nuclear Regulatory Commission
Andrea G. Jones
Department of State
Rosalind Baybutt
Department of Defense
J. William Leonard, Chair
Information Security Oversight Office

Industry

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

ISOO Support Staff

Laura L. S. Kimberly
Jorg J. Wetzel
Margaret L. Rose
Kristofer L. Johnson
Linda J. Ebben
Rashad Shakir
Dorothy L. Cephas

Observers

Lynn Gebrowsky
Mary Gallion
Ken Stein
Anna Harrison
John Reidy
Neala K. Enfinger