NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

MINUTES OF THE MEETING

The NISPPAC held its thirtieth meeting on Thursday, May 15, 2008, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, N.W., Washington, D.C. William J. Bosanko, Director, Information Security Oversight Office (ISOO) chaired the meeting. The meeting was open to the public.

The following members were present:

William J. Bosanko (Chair)
William Davidson (Department of the Air Force)
Lisa Gearhart (Department of the Army)
George Ladner (Central Intelligence Agency)
Eric Dorsey (Department of Commerce)
Stephen Lewis (Department of Defense)
John Fitzpatrick (Office of the Director of National Intelligence)
Kathy Watson (Defense Security Service)
Barbara Stone (Department of Energy)
John Young (Department of Homeland Security)
Gerald Schroeder (Department of Justice)
Dennis Hanratty (National Security Agency)
Sean Carney (Department of the Navy)
John Czajkowski (Office of Personnel Management) – Observer
Kimberly Baugher (Department of State)
Chris Beals (Industry)
Richard Lee Engel (Industry)
Sheri Escobar (Industry)
Kent Hamilton (Industry)
Douglas Hudson (Industry)
Timothy McQuiggan (Industry)
Daniel E. Shlehr (Industry)

A. Welcome, Introductions, and Administrative Matters – The Chair greeted the membership and attendees. The Chair introduced himself as the new Director of ISOO and as the third Chair of the NISPPAC. He acknowledged the contributions of the prior Chairs, Industry and Government members, as well as the ISOO staff. The Chair stated his intention to promote the improvement of the NISP to the benefit of Industry and Government. In the coming months, the Chair stated that he would hold meetings with the Government and Industry members, as well as representatives from the Memorandum of Understanding (MOU) organizations, in order to hear concerns, better understand the challenges, and gather ideas with respect to the program. The participation of two new NISPPAC representatives, Stephen Lewis (Department of Defense) and Eric Dorsey (Department of Commerce) was acknowledged. Formal introductions of the Committee's membership and attendees were made. The Chair observed that the terms of two industry members will be expiring in September and that nominations should be coordinated among the NISPPAC Industry members for consideration, and then forwarded to the Chair. The Chair stated that the minutes from the November 15, 2007 meeting were finalized by e-mail on February 26, 2008. Finally, the Chair noted that Vincent Jarvie (NISPPAC Industry Spokesperson) could

not be present, and the combined Industry presentation would be delivered by Timothy McQuiggan.

B. Old Business - The Chair requested that Greg Pannoni (ISOO) lead a discussion reviewing action items from the November 15, 2007 meeting.

1. *"The NISPPAC Chair will continue to explore options with the Defense Information Systems Agency (DISA) to enable Secret Internet Protocol Router Network (SIPRNET) Access to Industry Partners so that timely threat data can be provided."*

Mr. Pannoni stated that efforts were made to address this item with DISA. The main issue concerns Department of Defense (DOD) sponsorship for SIPRNET access. Mr. Pannoni mentioned that new approaches and important developments within DOD provide a possible solution. Consequently, ISOO has set aside its efforts with DISA, but will continue to work with DOD. The Chair requested that DOD provide a formal update at the next NISPPAC meeting on efforts to improve and enhance the automated dissemination of threat information to Industry. The Chair further requested that an informal meeting occur before the next NISPPAC session for an update on DOD's efforts in this regard. Gregory Torres (DOD) agreed to the meeting.

ACTION: DOD will provide a formal update at the next NISPPAC meeting on efforts taken to improve and enhance the automated dissemination of threat information to industry. The Chair and DOD representatives will meet before the next NISPPAC session for an update on these efforts.

2. *"At the next NISPPAC meeting, the Office of Personnel Management (OPM) and Office of Management and Budget (OMB) will provide an update concerning current efforts to promote reciprocity for suitability determinations to include common adjudication criteria."*

Mr. Pannoni stated that this item would be covered under new business by John Fitzpatrick in his briefing on the work of the Joint Security and Suitability Process Reform Team.

3. *"As briefed to the NISPPAC membership, the Personnel Security Clearance (PCL) Working Group will analyze survey results obtained from a representative sample of participants in the clearance process and make specific process improvement recommendations to the NISPPAC Chair by January 2008. Recommendations should identify current and desired states as well as approaches, plans, and timelines for achieving results. The working group will continue to analyze key data points that measure end-to-end clearance processing for Industry. In addition, the group will produce a six-month projection for clearance processing, timelines of Industry cases taking into account the current*

state, progress already achieved in the investigatory area, and the current inventory of cases awaiting adjudication."

Mr. Pannoni stated that this action item would be addressed in the PCL Working Group Report. Mr. Pannoni then mentioned the results of the PCL Working Group survey of the participants in the clearance process and referenced its inclusion in the packet of the meeting materials. The survey results provide recommendations for improvement of the clearance process; specifically, in regard to reducing case rejections and other impediments to timeliness. Wide dissemination of the survey results was recommended to the NISPPAC membership in their respective organizations.

4. *"The Office of the Designated Approving Authority (ODAA) Working Group will continue to resolve issues, develop process improvements, and promote communication between Industry and the Defense Security Service (DSS) on the certification and accreditation process for information systems. At the next meeting of the NISPPAC, the group will present a report on specific measurements and improvement of the overall timeliness of the certification and accreditation process, revisions of the ODAA process guides, training efforts, the reduction of deficient System Security Plans (SSP), and the reduction of denials for Interim Approval to Operate/Approval to Operate (IATO/ATO)."*

Mr. Pannoni stated that this action item would be addressed through the report of the ODAA Working Group.

5. *"The Industry representatives will submit any specific concerns regarding the Defense Industrial Base Information Assurance to the NISPPAC Chair, which will in turn be forwarded to Mr. Torres. Responses will be forwarded to the Chair and, as appropriate, provided to the NISPPAC membership."*

The Chair did not receive any specific concerns. The action item was closed.

6. *"The NISPPAC Chair will sponsor meetings between the Cognizant Security Authorities to address issues relevant to the revision of Chapter 8 of the National Industrial Security Program Operating Manual (NISPOM). The results of these discussions will be reported to the NISPPAC membership."*

Since the last NISPPAC meeting, the DOD has determined that in light of recent initiatives by the Committee for National Security Systems on a revised Federal standard for protection of national security systems any revisions of Chapter 8 of the NISPOM would be premature. The action item was tabled.

C. Working Group Updates

1. **Personnel Security Clearance Working Group -** A report on the working group's progress was provided by Scott Conway (Industry), Deborah Smith (OPM), Valerie Heil (DSS), and John Skudlarek (DSS).
   a. Mr. Conway stated that the purpose of the group is to develop end-to-end metrics for PCL processing. The NISPPAC working group metrics are designed to capture average processing time for each segment of the clearance process in order to identify areas for improvement. From the previous NISPPAC meeting the working group was also tasked with developing projections on the elimination of the backlog and the achievement of the clearance processing goals set forth by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. However, such projections were not possible because of a variance in the methodologies between the IRTPA and working group metrics. The NISPPAC working group end-to-end metrics are different, but do not conflict with reported IRTPA performance.
   b. IRTPA metrics apply only to initial investigations opened on or after October 1, 2006. The IRTPA end-to-end metrics are measured from the date the Subject signs the e-QIP (electronic Questionnaires for Investigative Processing) to the date of final adjudication (or the date that the adjudication is placed in due process). On the other hand, the NISPPAC working group metrics include IRTPA end-to-end time plus the Industry front-end time. The working group metrics apply to all pending investigations, regardless of the case type or when the case was opened. Mr. Conway elaborated on the working group metrics and highlighted observable trends in the reported data (see attached presentation slides). For March 2008, Mr. Conway noted that Industry is observing that initial Top Secret as well as all Secret, and Confidential investigations have an average end-to-end timeframe of 218 days; Top Secret investigations are averaging 390 days; Secret/Confidential investigations are averaging 181 days; and Top Secret periodic reinvestigations (PR) for security clearances are averaging 348 days. Mr. Conway stated that the working group metrics reflect Industry's experience regarding clearance processing.
   c. Ms. Smith reported that OPM has eliminated its case backlog and made significant improvement in the average timeliness of investigations. She noted that the metrics presented in her portion of the presentation represent the second quarter of FY 2008 and include all investigations (both those initiated before and after October 1, 2006) for initial Top Secret, and all Secret, and Confidential clearances for Government and Industry. She reported that there were 147,061 initial Top Secret, and all Secret and Confidential investigation adjudication actions reported to OPM, with the average end-to-end age (end-to-end being defined here consistent with IRTPA as the date the subject signs the e-QIP to the date of final adjudication) of the fastest 80% being 119 days. There were 21,564 initial Top Secret investigation adjudications reported, with the average end-to-end age of the fastest 80% being 163 days. There were 125,497 Secret and Confidential investigation adjudications reported, with the average end-to-end age of the fastest 80% being 111 days. There were 25,583 adjudication actions reported to OPM for Top Secret PRs, with

the average end-to-end age of the fastest 80% being 230 days. Ms. Smith then reported metrics pertaining to security clearances for Industry. There were 37,253 initial Top Secret, and all Secret, and Confidential investigation adjudication actions reported to OPM with the average end-to-end age of the fastest 80% being 124 days. There were 4,371 adjudication actions reported to OPM for Top Secret initial investigations, with an average end-to-end age of the fastest 80% being 192 days. There were 32,882 adjudication actions reported to OPM for all Secret and Confidential clearances with the average end-to-end age of the fastest 80% being 116 days. There were 12,029 Top Secret PRs reported to OPM with an end-to-end average age of 271 days for the fastest 80%. Given that the metrics presented reflect all cases that can be measured end-to-end (where there is an adjudicative action reported back into the system), Mr. Fitzpatrick asked what portion of the total investigative workload do the metrics represent, i.e., whether the metrics presented reflect the entire workload. He stated that he understood that there is a need for agencies to report adjudicative timelines back to OPM. In terms of the 147,061 cases adjudicated in the second quarter of FY 2008, he asked whether these cases represent the total workload or were these only cases where an end-to-end could be measured. Ms. Smith confirmed that the metrics represent only cases where an end-to-end can be measured and that this question would be addressed in the portion of the presentation dealing with inventory.

d. Ms. Smith stated that future processing times will be impacted favorably as the old cases are completed and new cases are then adjudicated. Ms. Smith presented data on the elimination of the backlog for Single Scope Background Investigations (SSBI). She reported that in FY 2007, OPM closed an average 2,009 cases (28%) more per month than received. For FY 2008, OPM closed an average 2,415 cases (33%) more per month than received to date. Ms. Smith then reported on the backlog elimination for National Agency Check with Local Agency and Credit Check (NACLC) and Access National Agency Check and Inquiries (ANACI) cases. She reported that in FY 2007, OPM closed an average 7,837 cases (18%) more per month than received. For FY 2008, OPM closed an average 4,637 cases (10%) more than received to date. Ms. Smith presented data on backlog elimination for both full scope and phased SSBI – PRs. She reported that in FY 2007, OPM closed an average 2,623 cases (34%) more per month than received. For FY 2008, OPM closed an average 782 cases (9%) more than received to date. Ms. Smith presented metrics detailing the significant decrease in OPM's pending case inventory, which, as of April 18, 2008, was a total of 264,711 pending cases (Government and Industry combined).

e. Ms. Heil then presented metrics on the Defense Industrial Security Clearance Office (DISCO) FY 2008 adjudication inventory. Ms. Heil stated that there was an overall reduction of 57% in regards to NACLC, SSBI, PR and Phased PR case types during the first two quarters of FY 2008. She informed the Committee that this was achieved through mandatory overtime and increasing proficiency of adjudicators hired during the last 12-18 months. Ms. Heil then

noted that in regards to Industry there was an overall reduction of 18% for NACLC, SSBI, PR, and Phased PRs case types during the first two quarters of FY08. Concerning the front end processing time (the amount of time that it takes DISCO to review and process an e-QIP and then forward to OPM or the Facility Security Officer [FSO] for review), Ms. Heil stated that currently the average time period is less than two days.

f. Ms. Heil then reiterated the aforementioned differences between the IRTPA and NISSPAC working group end-to-end metrics. Ms. Heil stated that the IRTPA metrics capture the average of the fastest 80% of initial clearance submitted on or after October 1, 2006. For IRTPA, that calculation starts from the date of signature on the e-QIP to the date of the final adjudication determination, or the date it was referred to due process. The NISPPAC metrics calculate the average for each of the case categories, and not the fastest 80%, regardless of when opened. Further, NISPPAC metrics are calculated from the time of the FSO's notice to the subject to complete an e-QIP, until the date of final eligibility or the date the adjudication is referred to due process.

g. In regard to a question raised Mr. Schroeder about the difference between the two sets of metrics, Ms. Heil noted that the NISPPAC working group metrics were calculated to measure the overall performance of the security clearance process as viewed by Industry. IRTPA metrics, on the other hand, only consider data post-October 1, 2006. Following this point, Mr. Fitzpatrick noted that it was well within the scope of the governance entity responsible for overseeing the security clearance process to determine how to measure future metrics so as to avoid discrepancies. Following this, Mr. Torres asked whether there should be a standard time period for Industry to complete its front-end responsibilities. After a brief discussion on the matter, Mr. Pannoni commented that though there is no official mandate for completing the front-end responsibilities, it is in the interest of individual Industry members to complete and submit clearance questionnaires to DISCO in a timely and complete manner. This is made evident by the lower rejection rate and faster acceptance turnaround time for those entities that complete this part of the process as soon as possible.

h. Mr. Skudlarek provided the DSS Automation update. The update is a follow-up to a NISPPAC action to address the electronic fingerprint issue. DSS has awarded a contract for E-Fingerprint store and forward capabilities, which is similar to the system that already exists in the Army and some Industry partner organizations. Mr. Skudlarek stated that this has led DSS to believe that such a system is a low-risk solution to the problem. In order to analyze the new system, DSS recently conducted a workshop and will be carrying out a pilot with Industry partners and OPM for product testing. The pilot is scheduled to begin June 30, 2008 and will run during the fourth quarter of FY 2008. Evaluation of the pilot results will drive the phases for implementation. Mr. Skudlarek stated that the system will be implemented in FY 2009. DSS anticipates that the system will process both machine-scanned and card-scanned fingerprint files. Further details of this effort will be provided by

DSS prior to full deployment. DSS is striving to implement several new capabilities in the Joint Personnel Adjudication System (JPAS). In order to implement E-Fingerprint capabilities, modifications to the agency use block are required. DSS is now negotiating terms with a contractor for this modification as well as other new capabilities. The DSS Office of the Chief Information Officer is working to finalize the schedule for these upgrades.

ACTION: The PCL Working Group will continue to analyze key data points that measure end-to-end clearance processing for Industry and make recommendations for resolving processing issues. The group's work will be presented in a report at the next NISPPAC meeting. DSS will provide an update on the progress of its E-Fingerprint pilot program and the implementation of new capabilities in JPAS.

D. Controlled Unclassified Information (CUI): Update and Status - The Chair rearranged the order of presentations noted in the agenda to accommodate Dr. Josh Weerasinghe, Director for Policy and Programs, Acting (Program Manager, Information Sharing Environment), who presented this update.

1. Dr. Weerasinghe stated that the "Memorandum for the Heads of Executive Departments and Agencies: Designation and Sharing of Controlled Unclassified Information" was issued by the President on May 9, 2008. The impact of the new policy on Industry will not be immediate. Implementation will need to be coordinated at the Federal level and with Industry. The Presidential Memorandum adopts, defines, and institutes CUI as the single categorical designation for all terrorism related information previously referred to as Sensitive But Unclassified (SBU) in the Information Sharing Environment (ISE); and designates the National Archives and Records Administration as the CUI Executive Agent (EA) to oversee and implement the new CUI Framework. Dr. Weerasinghe then proceeded to discuss the definitions and application of the new markings established in the Presidential Memorandum. He noted that at the present time any entity can use any marking for SBU without uniformity. However, the Presidential Memorandum requires agencies to define and justify what they will be identifying as CUI to the EA. The Memorandum is also very clear on what cannot be marked as CUI and that there are to be only three CUI markings. In short, if an agency does not have something identified as critical and justified to the CUI EA then the three markings are all that will be permissible. Dr. Weerasinghe presented the governance structure and explained the role and responsibilities of the CUI EA, CUI Council, and participating Federal departments and agencies. The CUI council has been created as a subcommittee of the Information Sharing Council (ISC) and, as such, is Federal Advisory Committee Act exempt. Dr. Weerasinghe stated that certain important infrastructure protection agreements between the Federal Government and the private sector are not fully accommodated under and afforded exceptions in the CUI Framework (Protected Critical Infrastructure Information, Sensitive Security Information, Chemical Vulnerability Information, and Safeguards Information).

The Chair noted that during implementation of the CUI Framework, comments will be sought from federal, state, local and private sector entities.

2. In response to a question raised by Sean Carney (Department of Navy) regarding the release of safeguarding requirements of CUI, Dr. Weerasinghe stated that the Memorandum is structured similar to Executive Order 12958, as amended, as an overarching policy; implementing regulations will be forthcoming. However, safeguarding requirements for CUI should not be implemented until adequate guidance is made available. Given that there is a prohibition in the Memorandum against marking information as CUI that is required to be released to the public, Mr. Schroeder asked whether there is an implication in the Presidential Memorandum that an agency must conduct a Freedom of Information Act (FOIA) review to see whether particular paragraphs are subject to mandatory release under FOIA before applying CUI markings. Dr. Weerasinghe stated that this issue is not addressed by the Memorandum and will need to be addressed by the CUI EA.
3. Dr. Weerasinghe stated that agencies will eventually provide guidance to contractors on the requirements for handling CUI received from the Government. In response to a question from Kimberly Baugher (Department of State), Dr. Weerasinghe stated that it was the President's intent for the CUI framework to be utilized broadly within the Executive branch and applied by the head of any agency to SBU, but that CUI is mandatory for terrorism-related information within the ISE.

E. ODAA Working Group Report – A report on the working group's progress was provided by Steven Abounader (Industry) and David Cole (DSS).

1. Mr. Abounader stated since the last NISPPAC meeting, the ODAA working group continues to resolve issues and to develop process improvements. The working group has served as a conduit of communication for Industry and DSS. Concerning ongoing action items, Industry is planning to review the recently released ODAA Process Guide, Plan and Profile Templates, ODAA Automated Tools, and Standard Configurations. In working group meetings, Industry identified two areas for improvement: inconsistent guidance and timeliness of the DSS ODAA Certification and Accreditation (C&A) process. Mr. Abounader stated that DSS has met the concerns of Industry by providing an avenue to address inconsistent guidance and modifying its C&A processes. Industry requested that DSS brief and meet more with contractors concerning DSS process changes. DSS has met and briefed industry contractors, but this effort needs to be continued.
2. Mr. Cole outlined accreditation metrics. The average 2007 accreditation timelines reflected a 90-120 day review for the granting of an initial IATO. DSS established some metric gathering procedures to identify "bottlenecks" and areas for improvement. Mr. Cole stated that the current timeline reflects a 30 day average for plans received in March and April 2008, with metrics being recorded since August 2007. DSS has not experienced significant issues with granting a full ATO within the required 180 day timeframe. DSS processes approximately 4,000 accreditations annually. As of April 2008, there were 209 plans that took

longer than 90 days to be granted an IATO, thus creating a security plan backlog. Of that backlog, 164 plans are being reviewed and 45 plans are awaiting contractor responses. As a result of gathering metrics, process adjustments have been made. Consequently, DSS headquarters now has central oversight over all the plans and is positioned to quickly respond to areas requiring attention. Mr. Cole reported that Industry has improved in meeting compliance reviews when the ODAA conducts onsite verifications. He reported that in November 2007, 55% of onsite verifications required some level of modification, whereas the current rate is 38%. This improvement was brought about by changes implemented by the ODAA and communication with Industry. DSS hopes to reduce the level of modifications after onsite verifications to only 5%.

3. DSS publishes an ODAA News Bulletin to inform industry of current issues and correct misunderstandings such as those concerning the SIPRNET account process as well as C&A.
4. ODAA has also reworked Information Systems training for the Industrial Security Representatives. The long-term goal is to offer a one-week end-to-end course on the C&A process for the contractor community.
5. Mr. Cole identified five ODAA initiatives in process: (1) standardizing system security plans using templates, (2) standardizing configurations for operating systems to protect classified information, (3) creating tools to assist contractors in complying with configuration standards, (4) updating the ODAA process guide, and (5) establishing the ODAA Online System which would allow DSS to coordinate, monitor, and measure the C&A process. The ODAA Online System will be available for Industry's use. The purpose of these initiatives is to reduce security plan errors and accreditation denials which will in turn improve the timeliness and consistency of the ODAA process.
6. In response to concerns over Information Systems Security Manager (ISSM) qualifications, DSS will be drafting initial outlines to be considered by the working group in order that a solution might be reached that encompasses a balance of different skill sets, with the recognition that facility and company size may impact skill and competency requirements. Concerning the status of the multi-site corporate ISSM program for Industry, Mr. Cole stated that DSS is currently assessing the issue and weighing the concern that personnel will be readily available to respond to problems. Multi-site corporate ISSMs are permitted under certain constraints, the primary one being time/mileage to cover multiple facilities. Mr. Cole stated that a response on this issue will be given to Industry within 30 days and agreed to notify the Chair when this occurs.
7. Ray Musser (Industry) asked what number of the 4,000 accreditations are Secret systems as opposed to Top Secret. Mr. Cole stated that he could not provide this information and that DSS is refining its metrics gathering methods, but was able to confirm that the thirty day average for granting IATO (for plans received in March and April 2008) was across all levels.

ACTION: The ODAA will respond to Industry regarding the status of multi-site corporate ISSMs within the next thirty days and inform the Chair when this occurs. The ODAA Working Group will continue to resolve issues, develop

process improvements, and promote communication between Industry and the DSS on the certification and accreditation process for information systems. At the next meeting of the NISPPAC, the group will again present a report on specific measurements and improvement of the overall timeliness of the certification and accreditation process, revisions of the ODAA process guides, training efforts, the reduction of deficient SSPs, and the reduction of denials for IATO/ATO.

F. New Business

1. **CUI: Update and Status** – (see above)

2. **Security and Suitability Process Reform Team** – Mr. Fitzpatrick presented on this topic.
   a. Mr. Fitzpatrick stated that the reform team is a joint effort between the DNI, DOD, Executive Office of the President, and OPM; and includes the participation of Linda Springer (OPM), Clay Johnson (OMB), James Clapper (DOD), and Michael McConnell (ODNI). The working level leadership includes: Mr. Czajkowski, Mr. Fitzpatrick, Elizabeth McGrath (DOD) and Ana Mazzi (OMB).
   b. Mr. Fitzpatrick provided a brief overview of the past actions, and stated that in the Fall of 2007 the prior suitability reform initiative between OPM and the National Security Council (Hadley-Springer initiative) and the "Tiger Team" (Defense Intelligence led and security clearance focused) were brought together into one joint security and suitability reform effort. The President signed a memorandum on February 5, 2008, which recognized the need and goals for the reform and required a response from the team no later than April 30, 2008. Mr. Fitzpatrick then highlighted the main points of the response to the President, which puts forward that the work done to date argues for the adoption and implementation of a new process design and a vision of the "future state." The proposal includes a new governance structure, near-term actions that leverage ongoing work or are the next best steps to take, and other work ongoing to identify reform options and validate innovations or suppositions made in the process design. The chart, "Transformed Clearance Process Vision," provides an overview of the new process design (see attached presentation).
   c. Mr. Fitzpatrick then discussed the governance structure and highlighted the duties and responsibilities of the Performance Accountability Council, which will be overseeing the security clearance process. Mr. Fitzpatrick stated that the reform team is working to coordinate revisions that outline the responsibilities of the Council and the appropriate reforms. The security and suitability processes will remain distinct, and will not be homogenized. The areas that they utilize in common will be identified and brought into alignment for efficiency, timeliness, and effectiveness. This is the reason for a focus on the application process and the recommendation to generate a next generation application. The suitability and security processes are heavily manual today

as performed by agencies and major service providers. There is a need for developing modern business tools and having a strategy under which an information technology infrastructure supports the processes end-to-end. The Council will be the place where requirements for end-to-end enterprise technology are established, and then through some offices the development of that architecture will be managed over time. There are new opportunities, e.g., the DOD's strategic positioning of investment modernization in JPAS and other aspects in the Defense Information System for Security initiative and posturing of the latter to support capabilities in this new end-to-end architecture. The team is looking at other modernization programs that are part of the "as is" to see how they can be positioned. There is a significant opportunity in the alignment of investigative requirements. In monitoring performance to goals, the Council will be the place for building security alignment and continuing reform to meet the IRTPA goals.

3. **Foreign Ownership, Control, or Influence, (FOCI), Policy Issues** - Mr. Lewis presented on this topic.
   a. Mr. Lewis provided the following issues regarding FOCI that are under review within the DOD: 1) The definition of "material change" (1-302g[5], NISPOM; 2) Clarification of 2-300c, NISPOM, regarding invalidation of existing cleared companies which come under foreign ownership; 3) Inconsistencies resulting from corporate family FOCI reporting (2-302, NISPOM); and 4) Whether the questions contained on the "Certificate Pertaining to Foreign Interests" (SF-328) are serving the purposes of the Department of Defense.

4. **Combined Industry Presentation** – Mr. McQuiggan presented on this topic. The following is a summary of his presentation:
   a. Review of the NISPPAC industry members and their term expiration dates: Kent Hamilton (2008), Daniel Schlehr (2008), Timothy McGuiggan (2009), Douglas Hudson (2009), Richard "Lee" Engel (2010), Vincent Jarvie (2010), Sheri Escobar (2011), and Christopher Beals (2011).
   b. Industry places an importance upon the work accomplished by the ad hoc working groups. The working groups have provided valuable visibility and transparency into the areas of clearance processing and C&A. It is important for the continued benefit of the NISP that the working groups are continued.
   c. Sharing threat information appropriately with Industry continues to pose a challenge. The SPIRNET may be a possible solution for sharing this information, but there are a number of challenges in this regard. Industry is eager to work toward a solution. Industry anticipates discussions in the near future with DSS regarding such a solution.
   d. Industry will need to participate in the framing of CUI requirements and training policies.
   e. Industry recognizes the various challenges associated with FOCI and recommends the creation of an ad hoc working group to address issues with DSS. The Chair accepted this recommendation, requested that the NISP

signatories and Industry participate, and asked whether there exist any concerns regarding the group on the part of DOD. No concerns were expressed.

f. Industry is extremely interested in the Security and Suitability Process Reform Team. Mr. McQuiggan expressed appreciation for the cycle time data that was presented by the NISPPAC PCL Working Group, which allows corporate leaders to be adequately informed.

ACTION: A FOCI Ad Hoc Working Group will be established. The NISP signatories, DSS, and Industry will be invited to participate. A report of this working group will be presented at the next meeting of the NISPPAC.

5. **Discussion** – The Chair opened the meeting for additional discussion of the presented topics. No further discussion was initiated.

6. **NISP Signatory Update** – No updates were reported.

G. General Open Forum

1. The Chair expressed his desire to meet with individual agency representatives prior to the next NISPPAC meeting to hear their concerns and ideas.

2. Mr. Czajkowski presented an update on the deployment of the next version of the SF-86. OPM is on track to meet its August deployment goal. OPM will simultaneously provide a paper form and e-QIP. The new SF-86 will include revisions to question 21 as requested by the Secretary of Defense. Mr. McQuiggan asked whether an SF-86 completed without a revised question 21 can be processed. Mr. Czajkowski stated that OPM has not made a determination on this point to date.

H. Closing Remarks and Adjournment – The Chair expressed his gratitude to the membership and adjourned the meeting at 11:50am.

I. Summary of Action Items:

1. **ACTION: DOD will provide a formal update at the next NISPPAC meeting on efforts taken to improve and enhance the automated dissemination of threat information to industry. The Chair and DOD representatives will meet before the next NISPPAC session for an update on these efforts.**

2. **ACTION: The PCL Working Group will continue to analyze key data points that measure end-to-end clearance processing for Industry and make recommendations for resolving processing issues. The group's work will be presented at the next NISPPAC meeting. DSS will provide an update on the progress of its E-fingerprint pilot program and the implementation of new**

capabilities in JPAS.

3. **ACTION: The ODAA will respond to Industry regarding the status of multi-site corporate ISSMs within the next thirty (30) days and inform the Chair when this occurs. The ODAA Working Group will continue to resolve issues, develop process improvements, and promote communication between Industry and the DSS on the certification and accreditation process for information systems. At the next meeting of the NISPPAC, the group will again present a report on specific measurements and improvement of the overall timeliness of the C&A process, revisions of the ODAA process guide, training efforts, the reduction of deficient SSPs, and the reduction of denials for IATO/ATO.**

4. **ACTION: A FOCI Ad Hoc Working Group will be established. The NISP signatories, DSS, and Industry will be invited to participate. A report of the working group will be presented at the next meeting of the NISPPAC.**

NISPPAC Ad Hoc Working Group

May 15, 2008 NISPPAC Meeting

- NISPPAC WG Metrics vs. IRTPA 2004 Performance
- NISPPAC WG Metrics – Timeliness Trends
- IRTPA 2004 Performance
- OPM Investigation Workloads and Inventory
- DSS Adjudication Workloads and Inventory
- DSS - Automation Update

NISPPAC Ad Hoc Working Group (WG)

Members

- **Greg Pannoni, ISOO**
- **Pat Viscuso, ISOO**
- **Scott Conway, Industry Representative**
- **Doug Wickman, Industry Facilitator**
- **Deb Smith, OPM**
- **Valerie Heil, DSS**

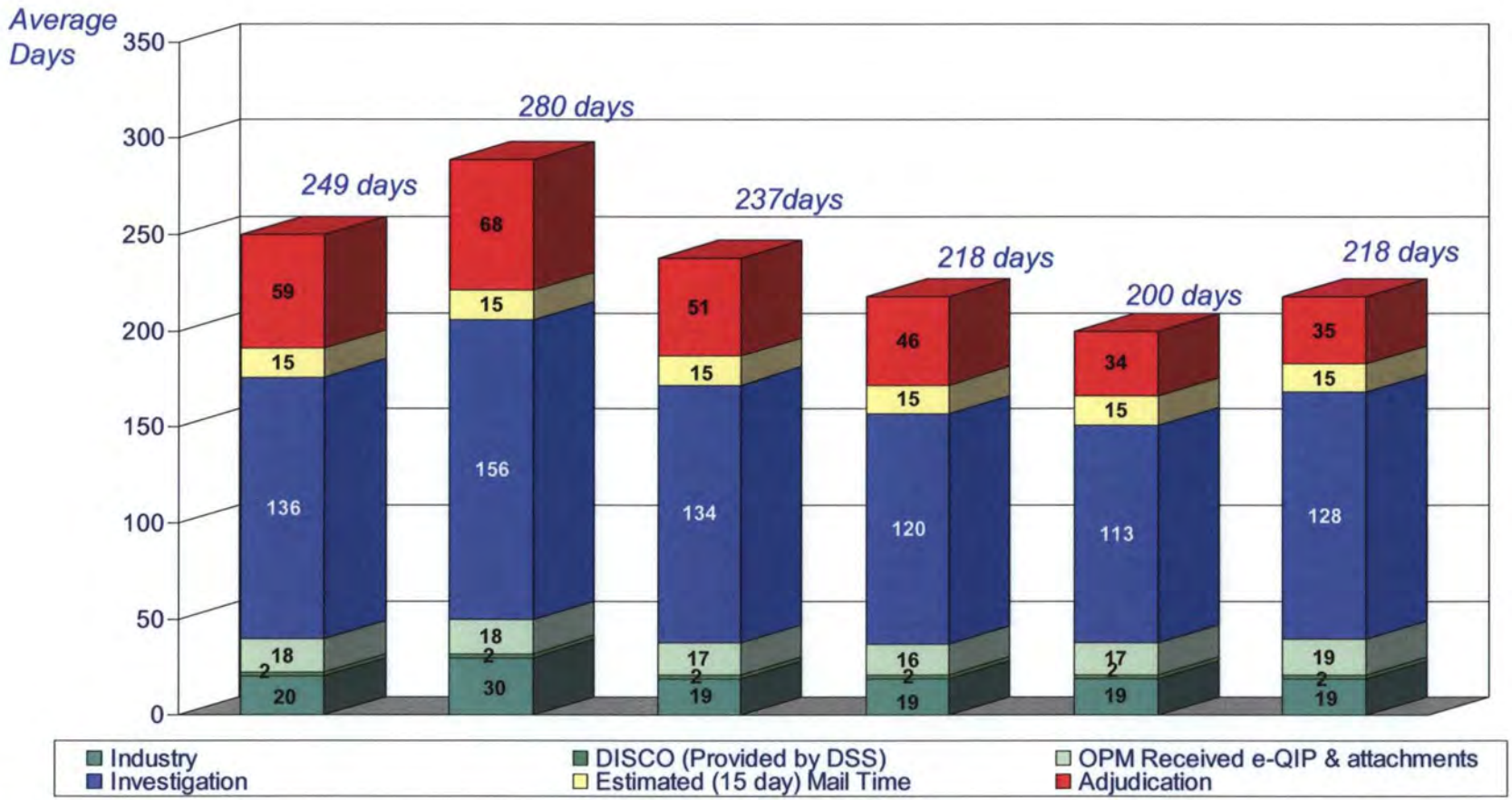
Mission

- November 2006: NISPPAC tasked a working group, comprised of Industry, OPM, DoD, and ISOO, to develop a system of metrics including key data points, to measure the timeliness of end-to-end clearance processing for Industry.
  - Expanded to include projections for clearance processing timeliness and process improvement recommendations in subsequent sessions.

NISPPAC WG's End-To-End Metrics (Industry) Versus IRTPA 2004 Performance Metrics

- NISPPAC WG End-to-End Metrics are different, but do not conflict with reported IRTPA 2004 Performance
- IRTPA metrics:
  - Apply only to *initial* investigations opened on or after *October 1, 2006*
  - End-to-end measured as the date Subject signs the e-QIP to the date of final adjudication, or, the date adjudication is placed in due process
- NISPPAC WG metrics designed to capture average processing time for each segment of the clearance process to identify areas for improvement
- NISPPAC WG metrics:
  - Include IRTPA end-to-end time *PLUS* the industry front-end time
  - Apply to *all* pending investigations, regardless of the case type or when the case was opened
- Eliminating the backlog of national security investigations and adjudications impacts overall average timelines
  - And, is a realistic measure to illustrate progress.

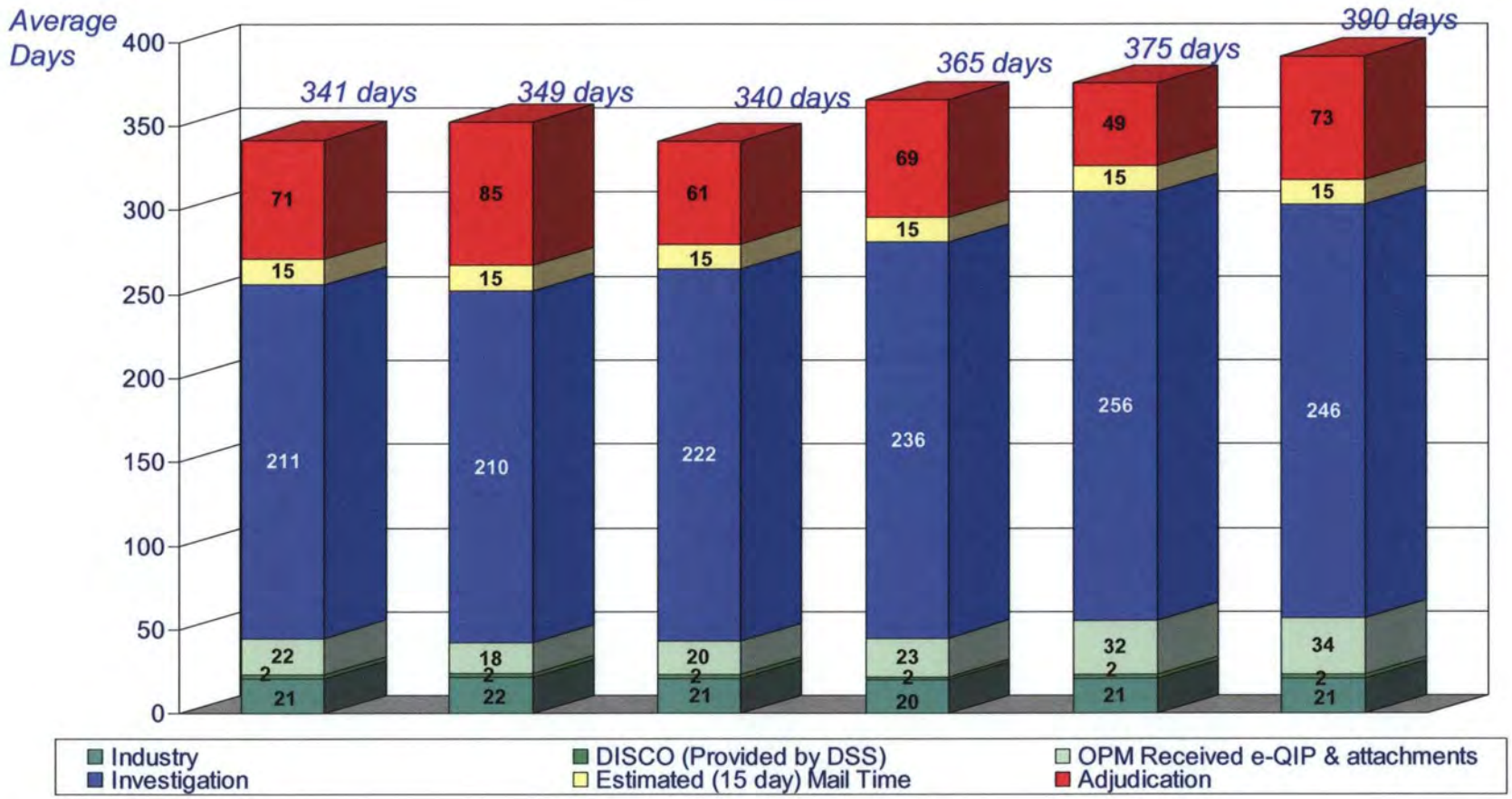
NISPPAC Working Group's End-To-End Metrics (Industry)
Initial Top Secret and All Secret/Confidential Security Clearance Decisions



Adjudications actions taken:	Oct 07	Nov 07	Dec 07	Jan 08	Feb 08	Mar 08
Sampling limited to clearances submitted using e-QIP	11,431	13,161	12,493	15,096	12,943	10,765

Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested.
The present reject rate is 13% for DISCO and 7% for OPM. The time span for the rejections is not included in the above metrics.

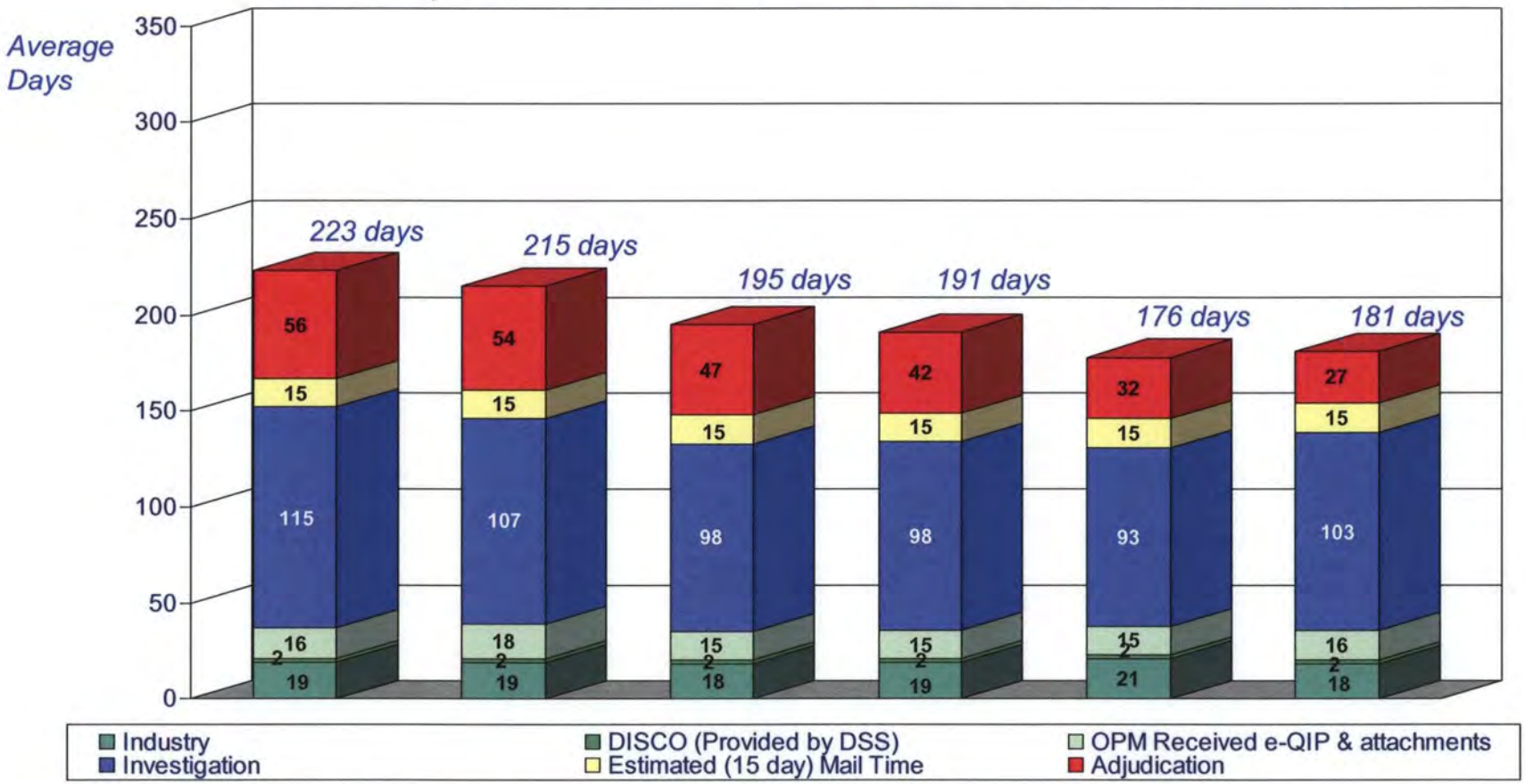
NISPPAC Working Group's End-To-End Metrics (Industry)
Initial Top Secret Security Clearance Decisions



Adjudications actions taken:	Oct 07	Nov 07	Dec 07	Jan 08	Feb 08	Mar 08
Sampling limited to clearances submitted using e-QIP	2,547	6,277	3,606	2,317	1,546	1,885

Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested. The present reject rate is 13% for DISCO and 7% for OPM. The time span for the rejections is not included in the above metrics.

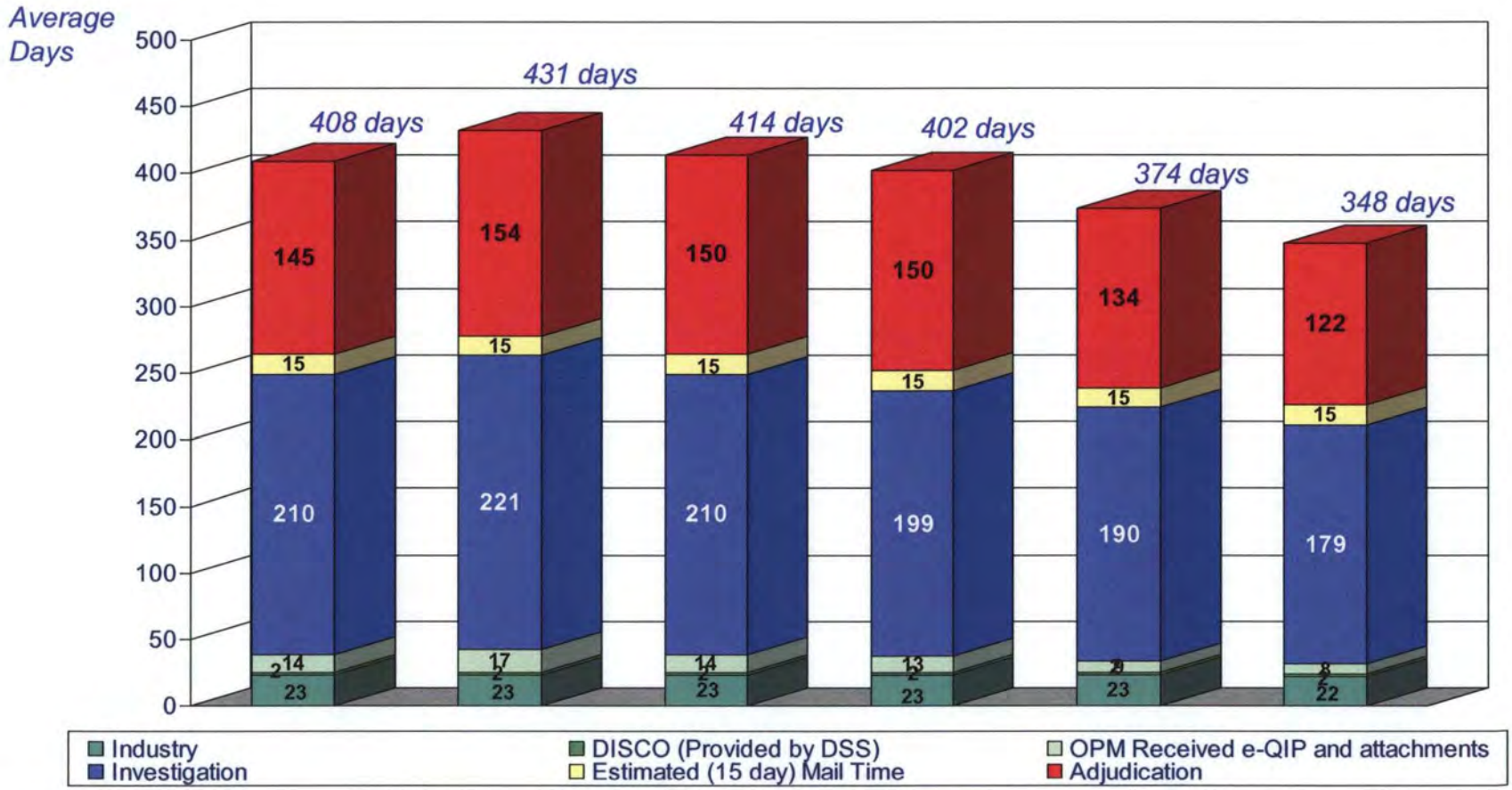
NISPPAC Working Group's End-To-End Metrics (Industry)
All Secret/Confidential Security Clearance Decisions



Adjudications actions taken:	Oct 07	Nov 07	Dec 07	Jan 08	Feb 08	Mar 08
Sampling limited to clearances submitted using e-QIP	8,884	6,884	8,887	12,779	11,397	8,880

Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested.
The present reject rate is 13% for DISCO and 7% for OPM. The time span for the rejections is not included in the above metrics.

NISPPAC Working Group's End-To-End Metrics (Industry)
Top Secret Reinvestigation Security Clearance Decisions



Adjudications actions taken:	Oct 07	Nov 07	Dec 07	Jan 08	Feb 08	Mar 08
Sampling limited to clearances submitted using e-QIP	4,100	1,952	2,093	3,797	3,947	6,093

Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested. The present reject rate is 13% for DISCO and 7% for OPM. The time span for the rejections is not included in the above metrics.

Second Quarter FY2008 IRTPA 2004 Performance Security Clearance Decisions

TOTAL Clearances –All Agencies

- Initial Top Secret and All Secret & Confidential – 147,061 Adjudication Actions Reported to OPM with the average End-to-End Age of 80% is 119 days
  - Initial Top Secret – 21,564 average End-to-End Age of 80% is 163 days
  - Secret/Confidential – 125,497 average End-to-End Age of 80% is 111 days

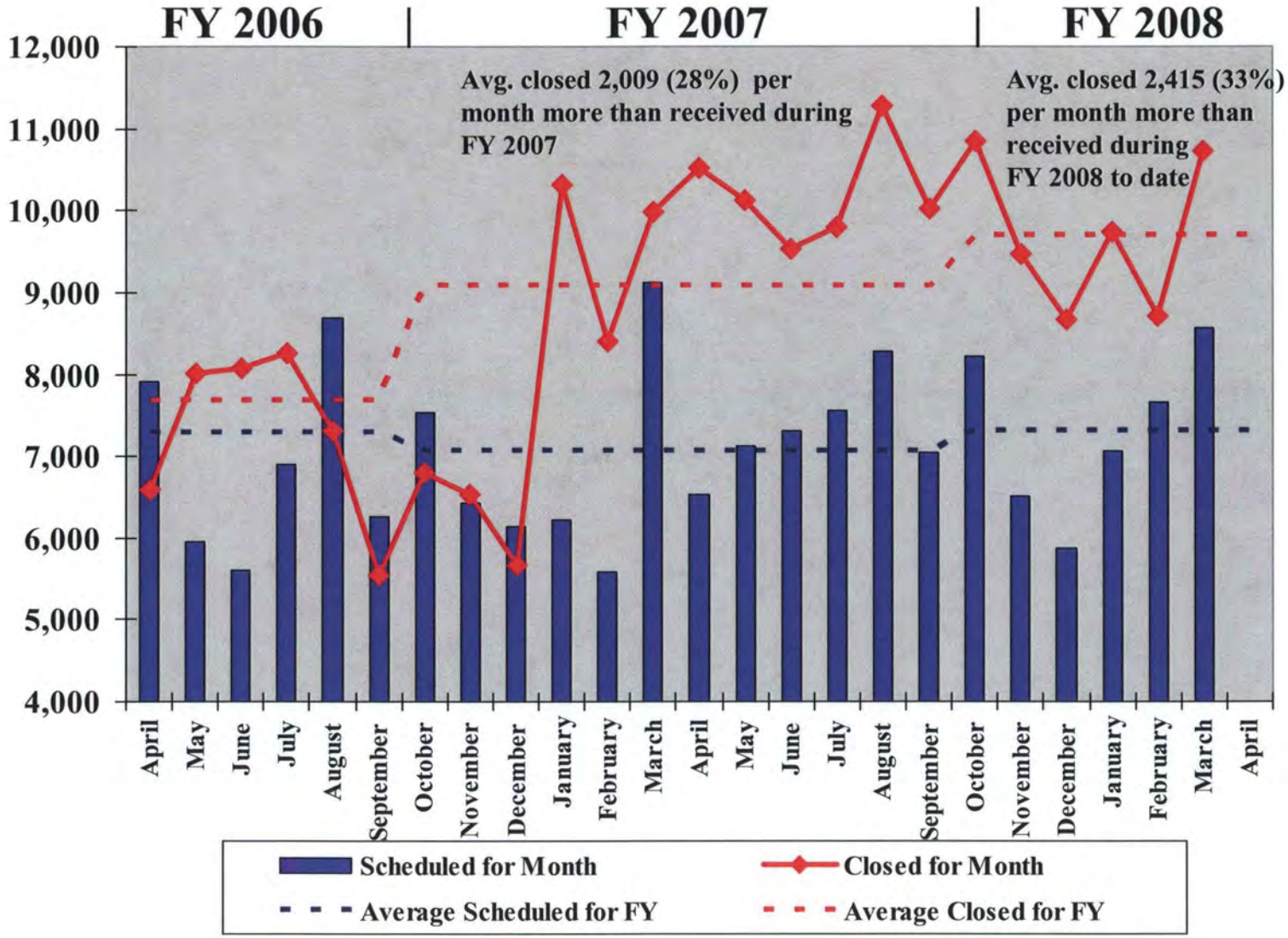
- Top Secret Reinvestigations – 25,583 Adjudication Actions Reported to OPM with the average End-to-End Age of 80% is 230 days

Industry Clearances

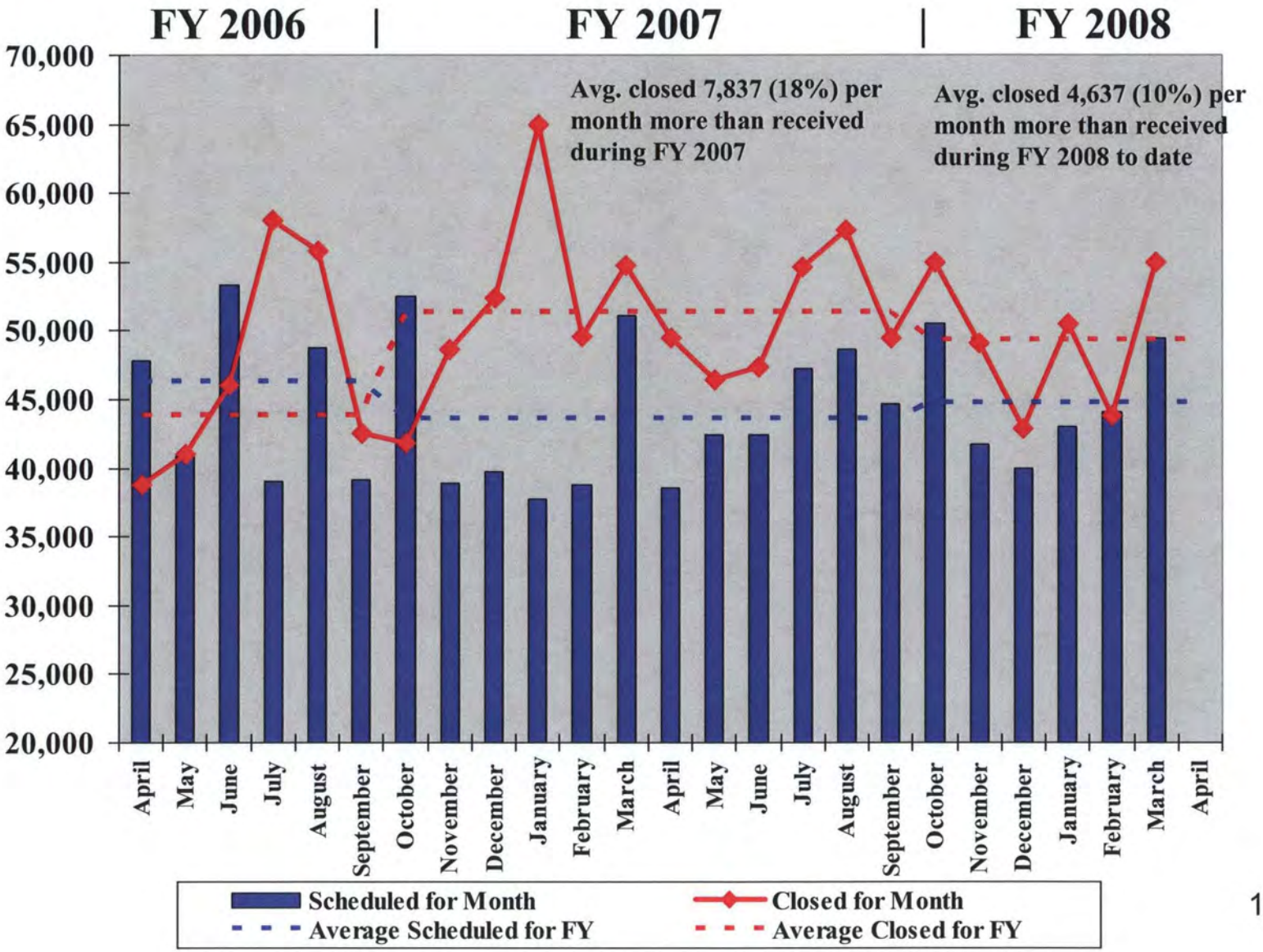
- Initial Top Secret and All Secret & Confidential – 37,253 Adjudication Actions Reported to OPM with the average End-to-End Age of 80% is 124 days
  - Initial Top Secret – 4,371 average End-to-End Age of 80% is 192 days
  - Secret/Confidential – 32,882 average End-to-End Age of 80% is 116 days

- Top Secret Reinvestigations – 12,029 Adjudication Actions Reported to OPM with the average End-to-End Age of 80% is 271 days

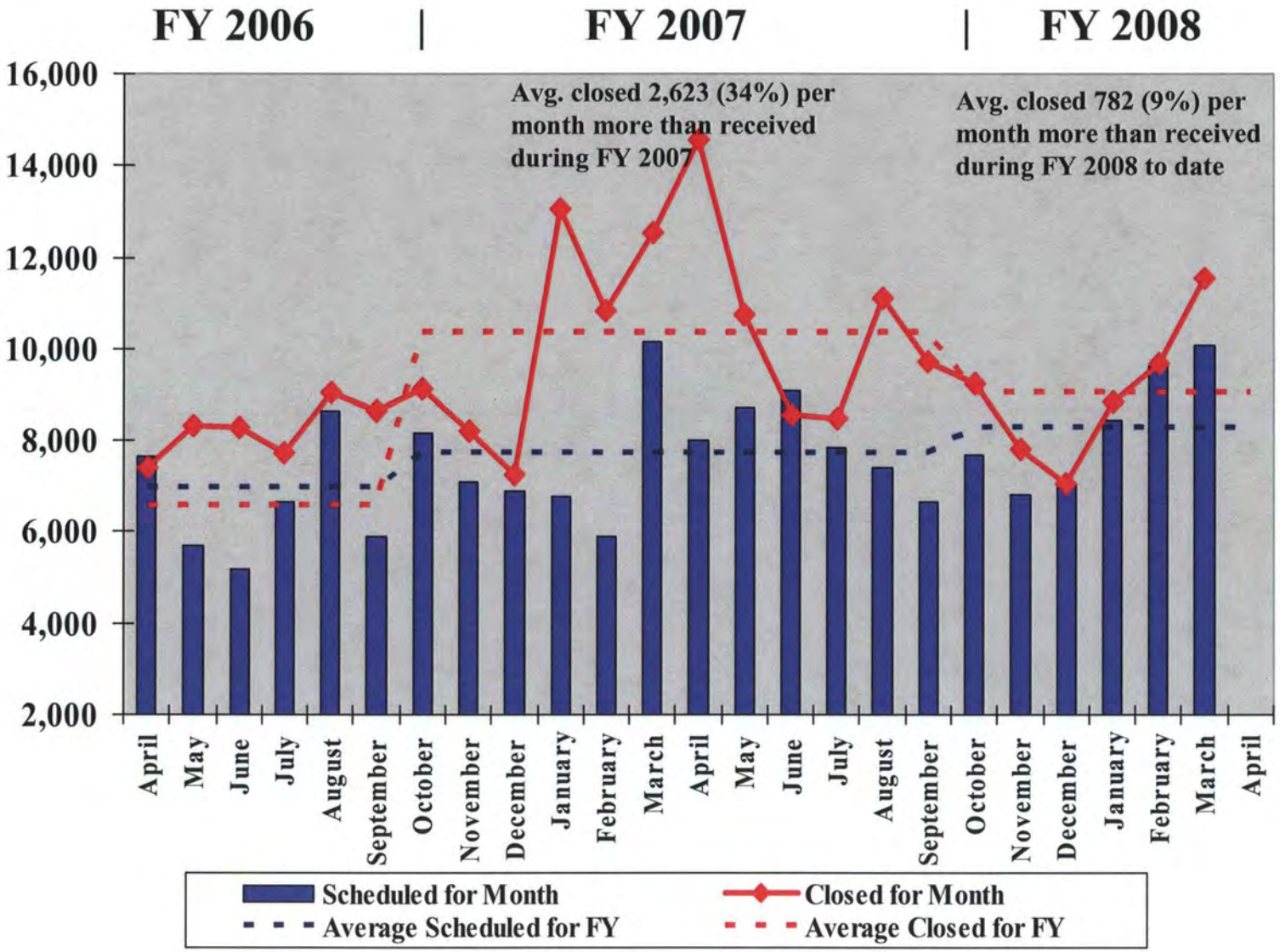
Backlog Elimination
National Security SSBI's



Backlog Elimination
NACLC's and ANACI's



Backlog Elimination
SSBI-PR's – Full Scope and Phased



OPM-FISD Pending Case Inventory
(Government and Industry Employees Combined)

Case Type	4/03/06	4/02/07	4/05/08	4/18/08
SBI	69,905	58,357	25,984	25,014
SSBI-PR/PPR	95,974	67,947	46,168	43,072
NACLC/ANACI	253,768	183,692	116,677	114,709
Other	93,194	124,263	86,401	81,916
Total	512,841	434,259	275,230	264,711

OPM-FISD's Inventory Status
(Government and Industry Employees Combined)

Case Type	Closed in FY2007	Current On Hand 4/18/08	Inventory Levels
SBI	102,621	25,014	89 days
SBIPR and PPR	119,094	43,072	132 days
NACLC/ANACI	607,809	114,709	69 days
Other	1,294,582	81,916	23 days
TOTAL	2,124,106	264,711	

DISCO

FY08 ADJUDICATION INVENTORY

CASE TYPE	Oct-07 (Start of 1Q)	Mar-08 (End of 2Q)	Delta
NACLC	11,449	488	-96%
SSBI	9,337	5,625	-40%
SBPR	4,899	3,752	-23%
PPR	8,945	4,923	-45%
Total Pending	**34,630**	**14,788**	**-57%**

- **Overall reduction of 57% for NACLC, SSBI, SBPR and Phased PR case types from 1Q FY08 to 2Q FY08.**
- **Achieved through mandatory overtime and increasing proficiency of adjudicators hired during the last 12-18 months.**

Source: DISCO Manual Counts

INDUSTRY CASES AT OPM

FY08 INVESTIGATION INVENTORY

CASE TYPE	Oct-07 (Start of 1Q)	Mar-08 (End of 2Q)	Delta
NACLC	29,575	25,085	-15%
SSBI	14,110	8,796	-38%
SBPR	11,761	9,943	-15%
PPR	7,711	7,749	0%
Total Pending	**63,157**	**51,573**	**-18%**

Overall reduction of 18% for NACLC, SSBI, SBPR and Phased PR case types from 1Q FY08 to 2Q FY08.

Source: OPM Customer Support Group

INDUSTRY

FY08 FRONT END PROCESSING TIME

FY08 REPORTING	1Q FY08			2Q FY08		
	Oct 07	Nov	Dec	Jan	Feb	Mar
Investigation Requests Approved	15,940	11,434	10,908	14,781	13,971	14,143
Average Days between DISCO Received / Approved	**1.6**	**1.8**	**1.6**	**1.5**	**1.9**	**1.7**

- **DISCO consistently averages less than two days to process investigation requests.**
- **Metrics include e-QIPs released to OPM and e-QIPs rejected to submitter.**

Source: JPAS Monthly Report

IRTPA and NISPPAC
End to End Metrics

- As presented earlier, IRTPA metrics
  - calculate the average of the fastest 80% of *initial* clearances submitted on or after 10/01/06
  - end-to-end is calculated as the time between the date of the Subject's signature on the e-QIP and the date of final determination, or the date the adjudication is referred to due process
- NISPPAC metrics
  - calculate the average for each of the case categories (not just fastest 80% of initial clearances) regardless of when opened
  - end to end processing is calculated as the time between the FSO notification to the subject to fill out the e-QIP, to the date of final eligibility or the date the adjudication is referred to due process

DSS Automation Update

- On April 17, 2008, DSS provided an automation update with highlights as noted:

- Secure Web Fingerprint Transmission (SWFT)
  - DSS CIO awarded a contract for E-Fingerprint store and forward capabilities in April 2008.
  - Workshop conducted 22-24 April with selected industry partners. DSS CIO is reviewing feedback from the workshop.
  - Pilot is scheduled to begin 30 Jun 2008 to validate initial system capabilities. Evaluation of the pilot results will drive the follow-on phases for implementation.
  - DSS anticipates that the system will process machine-scanned and card-scanned fingerprint files
  - Further details of this effort will be provided by DSS prior to full deployment of this capability.

DSS Automation Update

Joint Personnel Adjudication System (JPAS) Enhancements

- DSS is working to implement several new capabilities in JPAS including, in priority order:
  - Modifications to the Agency Use Block (required to implement E-Fingerprint)
  - Addition of the NGA CAF
  - Addition of interfaces to the Army's CATS System, Intelligence Community Scattered Castles System, and Defense Integrated Human Resources Management System and the
  - Implementation of the new SF-86 questionnaire
  - Annotation of exception, waiver and deviation clearances
  - Add/modify new person category
  - Update of adjudicative guidelines

- DSS OCIO is working now to finalize the schedule on these upgrades.

Designation and Sharing of Controlled Unclassified Information

May 15, 2008

Office Of the Program Manager, Information Sharing Environment
www.ise.gov

Presidential Memorandum | Designation of Controlled Unclassified Information

On May 09, 2008, the President released the Memorandum for the Heads of Departments and Agencies on the *Designation and Sharing of Controlled Unclassified Information*.

This Memorandum: (1) adopts, defines, and institutes "Controlled Unclassified Information" (CUI) as the single categorical designation for all information referred to as "Sensitive But Unclassified" (SBU) in the Information Sharing Environment (ISE); and (2) designates the National Archives and Records Administration (NARA) as the Executive Agent, to oversee and implement the new CUI Framework.

Definition of CUI

Controlled Unclassified Information (CUI) refers to…

CUI is defined as unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is pertinent to the national interests of the United States or to the important interests of entities outside the U.S. Federal government, and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

Designation of CUI

Information shall be designated as CUI…

- a statute so requires or authorizes; or
- the head of the originating department or agency, through regulations, directives, or other specific guidance to the agency, determines that the information is CUI. Such determination should be based on mission requirements, business prudence, legal privilege, the protection of personal or commercial rights, or safety or security. Such department or agency directives, regulations, or guidance shall be provided to the Executive Agent for his review.

Information shall not be designated CUI…

- to: (1) conceal violations of law, inefficiency, or administrative error; (2) prevent embarrassment to the U.S. Government, any U.S. official, organization, or agency; (3) improperly or unlawfully interfere with competition; or (4) prevent or delay the release of information that does not require such protection;
- if it is required by statute or Executive Order to be made available to the public; or
- if it has been released to the public under proper authority.

Marking of CUI

All CUI will carry one of three markings:

- ***Controlled with Standard Dissemination***: Information is subject to safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it is reasonably believed that it would further the execution of a lawful or official purpose.
- ***Controlled with Specified Dissemination***: Information is subject to safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Material contains additional instructions on what dissemination is permitted.
- ***Controlled Enhanced with Specified Dissemination***: Information is subject to enhanced safeguarding measures more stringent than those normally required since inadvertent or unauthorized disclosure would create a risk of substantial harm. Material contains additional instructions on what dissemination is permitted.

Marking of CUI

Controlled with Specified Dissemination

(1) Indicates the document contains Controlled Unclassified Information (CUI).

(2) Indicates that the document is subject to standard safeguards to reduce the risks of unauthorized or inadvertent disclosure.

Controlled

FEDERAL DEPARTMENT or AGENCY
WASHINGTON D.C. 20220

MEMORANDUM FOR Law Enforcement
DATE: May 15, 2007
FROM: Security
SUBJECT: CUI Markings

This memorandum reflects the proper marking of a CUI document.

Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text

Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text Text

Specified Dissemination:
Dissemination only to law enforcement personnel.

Indicates that the document will contain additional instruction on w what dissemination is permitted.

Example Only

CUI Governance Structure

CUI Executive Agent

The Presidential Memorandum designates NARA as the CUI Executive Agent. As such, NARA possesses oversight authorities and responsibilities of the CUI Framework and will develop processes and procedures to execute, monitor, and enforce them.

CUI Council

The CUI Council members shall be drawn from within the existing ISC. As appropriate, the CUI Council will consult with the ISC's State, Local, Tribal, and Private Sector Subcommittee. Representing the needs and equities of ISE participants, the CUI Council will provide advice and recommendations to the Executive Agent on ISE-wide CUI policies, procedures, guidelines, and standards

Departments and Agencies

Heads of all Federal departments and agencies will be responsible for implementing the CUI Framework standards for ISE-wide CUI policy and ensuring that their departments or agencies comply with the CUI Framework.

Exclusionary Clause

Certain important infrastructure protection agreements between the Federal government and the private sector are not fully accommodated under the current CUI Framework. As a result, the following existing Federal Regulations with their associated markings, safeguarding requirements, and dissemination limitations will be excluded from the CUI Framework

- 6 CFR Pt. 29 – PCII (**Protected Critical Infrastructure Information**)
- 49 CFR Pts. 15 (DOT) & 1520 (DHS/Transportation Security Administration) – SSI (**Sensitive Security Information**)
- 6 CFR Pt. 27 – CVI (**Chemical Vulnerability Information**)
- 10 CFR Pt. 73 – SGI (**Safeguards Information**)

Contact Information

Contact Information:
Josh K. Weerasinghe
Office of the Program Manager, Information Sharing Environment, ODNI
Joshkw@dni.gov or 202-331-0629

NISPPAC ODAA WORKING GROUP

15 May 2008

Progress since Nov 2007

- Working Group continues to resolve issues and develop process improvements
- Maintain communications conduit between Industry and DSS
- Ongoing action items:
  - Industry planning on reviewing the recently released:
    - Process Guide
    - Plan and Profile templates
    - ODAA Automated Tools
    - Standard Configurations

Working Group Discussions

- Issues raised by industry
  - Inconsistent guidance
    - ✓ ODAA has provided avenue to address inconsistent guidance
  - Timelines too long for DSS ODAA Certification and Accreditation Process (Timelines during 2007 90-120 days)
    - ✓ ODAA modified its process
- Industry Request
  - DSS brief and meet more with contractors on DSS process changes
    - ✓ ODAA and DSS have provided industry and company specific briefings

Metrics and Accreditation Improvements

- Average 2007 Timelines were 90-120 days to review and grant IATO
- Current timelines reflect a **30 day average** for plans received in March and April 2008 (metrics since Aug. 2007)
- Post Interim Approval to Operation (IATO) issuance, DSS meets 180 day timeframe to grant full Approval to Operate (ATO) --good for 3 years
- DSS processes approximately 4,000 accreditations annually
- Security plan backlog metrics
  - 209 Plans not received Interim Authority to Operate > 90 Days
    - 164 Plans Assigned and being reviewed
    - 45 Plans awaiting contractor responses
  - As a result of establishing ODAA process adjustments, HQ ODAA now has central oversight, these plans getting priority attention.

Metrics and Accreditation Improvements

- ODAA Onsite Verifications
  - Industry has improved in meeting compliance reviews
  - November 2007 55% required some level of modification currently 38%, less than 5 % is goal
- ODAA News Bulletin
  - Fiction vs. Fact
  - SIPRNET FAQ
- ODAA Training
  - ODAA has reworked the IS course for IS Reps
  - First class is being tested now
  - Goal: one week class offered to contractor community

Five ODAA Initiatives in Process

1. Standardizing System Security Plans (Templates)
2. Standard Configurations For Operating Systems
3. Tools to Assist Contractors in Complying with Configuration Standards
4. Updating ODAA Process Guide
5. Establishing an ODAA Online System
    - **Benefits**
        - Reduce security plan errors and accreditation denials = improved timeliness and consistency

NISPPAC ODAA Working Group Moving Forward

Information System Security Manager (ISSM) Qualifications

- DSS often encounters and questions contractor computer security staff (ISSM) competency to manage systems
- ISSMs require a wide range of technical skill and certification and accreditation knowledge
- DSS will draft initial outline to address issue
- Solution should encompass a balance of different skill sets
- Facility and company size may impact skill and competency

Joint Security and Suitability Reform Team

NISPPAC

15 May 2008

Presidential Memorandum

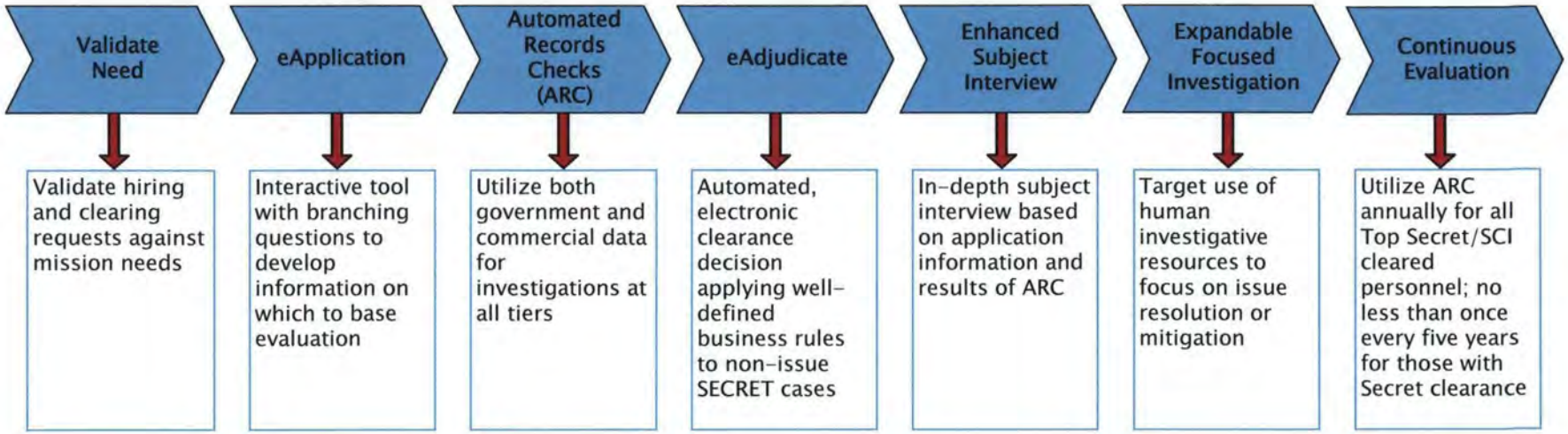
- Signed 5 February 2008
- Response due 30 April 2008
- Memo States:
  - Align security and suitability investigations and adjudications
  - Improve mobility and reciprocity
  - Enable with End-to-end Information Technology
  - Investigations that build on each other
  - Improve efficiency and effectiveness
  - Establish modernized processes and standards
- Memo Calls for:
  - "Initial reform proposal not later than April 30, 2008 that includes, as necessary, proposed executive and legislative actions to achieve the goals of reform described above"

30 April 2008 Response

- Adopt and Implement New Process Design
- Establish Governance via Executive Order
  - Performance Accountability Council
- Primary Near Term Actions
  - Develop Next-Generation Application
  - Initiate eAdjudication of Secret Cases
  - Develop Automated Record Checks
  - Develop Information Technology Strategy
- Continue to identify and validate reform initiatives

- http://www.whitehouse.gov/omb/reports/reform_plan_report_2008.pdf

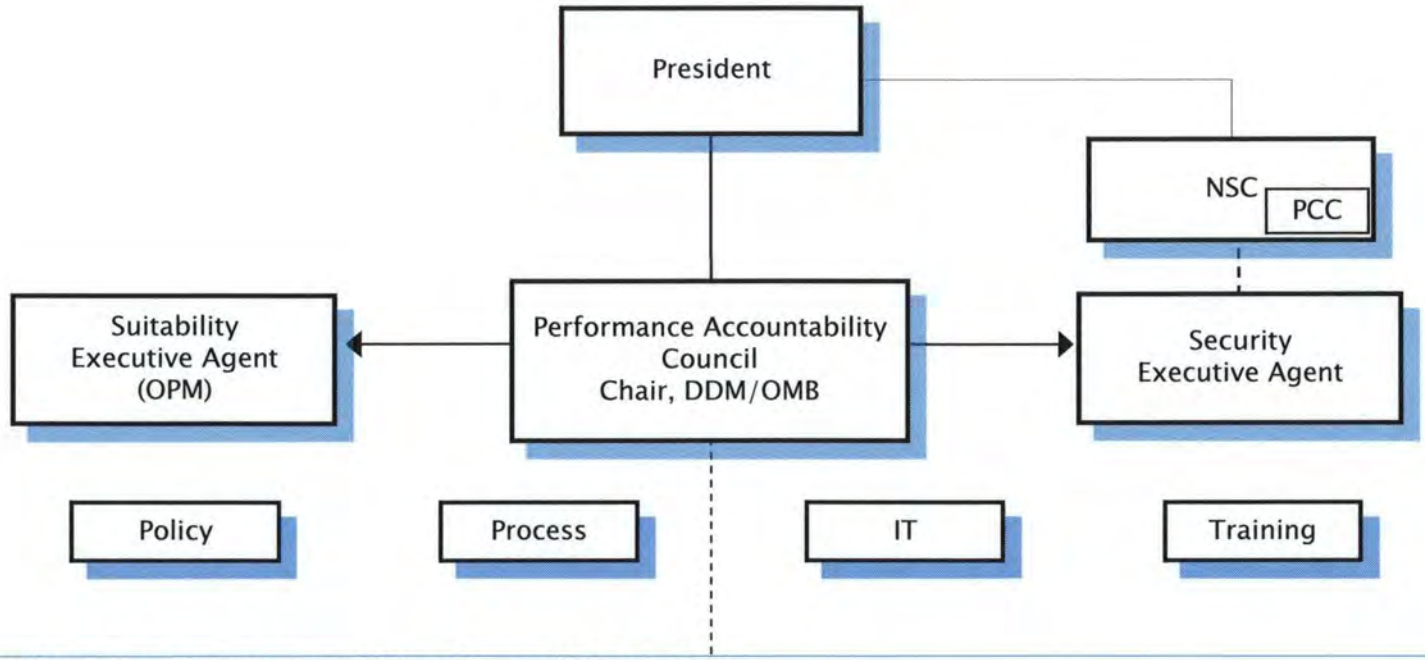
Transformed Clearance Process Vision



Key Attributes:

- End-to-end automation
- Paperless
- Digitized Finger Prints
- Electronic Signature
- e-Adjudication
- Clean Case Screening
- Continuous Evaluation
- Speed / efficiency
- Risk management instead of risk aversion
- More productive Subject Interview
- Custom process paths for Secret, TS/SCI and Suitability

Governance



Performance Accountability Council Functions

- Accountable to President for achieving goals of reform
- Ensures alignment of security and suitability investigative and adjudicative processes
- Holds agencies accountable for the implementation
- Establishes requirements for Enterprise information technology
- Monitors Performance to goals

NISPPAC
Industry Update

May 15, 2008

Industry Members/NISPPAC

Member	Company	Term Expires
Kent Hamilton	Northrop Grumman	2008
Dan Schlehr	Raytheon	2008
Tim McQuiggan	Boeing	2009
Doug Hudson	JHU/APL	2009
"Lee" Engel	BAH	2010
Vince Jarvie	L-3	2010
Sheri Escobar	Sierra Nevada	2011
Chris Beals	Fluor Corporation	2011

Industry Members/MOU

AIA	Tom Langer
ASIS	Ed Halibozek
CSSWG	Sam Kirton
ISWG	Mitch Lawrence
ITAA	Richard “Lee” Engel
NCMS	Sheri Escobar
NDIA	Dave Konicki

NISPPAC Ad Hoc Working Groups

- ODAA
- Personnel Security Clearance Processing

Information Sharing - Threat

Institutionalized Process:

- Information
- Communication methodology
- Feedback

Controlled Unclassified Information

- 9 May 2008 Memorandum
  - Designation and Sharing of Controlled Unclassified Information (CUI)
- Industry partners

Foreign Ownership Control and Influence

Collaborative effort through the NISPPAC

- Definitions
- Process
- Product

Joint Security Clearance Process Reform Team

- Projects/proof of concept
- Policy changes needed to enable transformed process
- IT Architecture