

**NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)**

SUMMARY MINUTES OF THE MEETING

The NISPPAC held its 31st meeting on Thursday, November 20, 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 minutes have been finalized and certified.

The following members/observers were present:

- William J. Bosanko (Chair)
- Kathy Watson (Defense Security Service)
- Daniel McGarvey (Department of the Air Force)
- Lisa Gearhart (Department of the Army)
- George Ladner (Central Intelligence Agency)
- David Bell (Department of Commerce)
- Stephen Lewis (Department of Defense)
- John Fitzpatrick (Office of the Director of National Intelligence)
- Richard Donovan (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)
- Kimberly Baugher (Department of State)
- Joy Fairtile (Office of Personnel Management) – Observer
- Chris Beals (Industry)
- Richard Lee Engel (Industry)
- Sheri Escobar (Industry)
- Kent Hamilton (Outgoing Industry Member)
- Douglas Hudson (Industry)
- Timothy McQuiggan (Industry)
- Daniel Shlehr (Outgoing Industry Member)
- Vincent Jarvie (Industry)
- Scott Conway (Industry)
- Marshall Sanders (Industry)
- Nuclear Regulatory Commission- Not Present
- National Aeronautics & Space Administration – Not present

I. Welcome, Introductions, and Administrative Matters

The Chair greeted the membership and attendees. After thanking those Government and Industry members who had taken the time since the last meeting to express their general concerns with respect to the National Industrial Security Program (NISP) to him, the Chair requested that those NISPPAC members who had not yet done so, share their concerns. In a similar vein, the Chair requested all NISPPAC to members

provide their top five issues or areas of concern regarding the NISP, by close of business, Monday, December 8, 2008.

The Chair acknowledged the service of Industry members, Daniel Schlehr and Kent Hamilton, whose terms have expired. Their replacements, Scott Conway (Northrop Grumman) and Marshall Sanders (SRA International), were introduced.

Following the roll call, the Chair noted that the minutes from the May 15, 2008, NISPPAC meeting were finalized by e-mail on September 30, 2008, and posted on the ISOO website. (<http://www.archives.gov/isoo/oversight-groups/nisppac/committee.html>).

ACTION: The Chair requested the NISPPAC members to provide their top five issues or areas of concern regarding the NISP, by close of business, Monday, December 8, 2008.

II. Old Business

The Chair requested that Greg Pannoni, ISOO, lead a discussion reviewing action items from the May 15, 2008, 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.

Mr. Pannoni stated that this action item would be addressed through the report on this topic from Stephen Lewis (Office of the Undersecretary of Defense for Intelligence) (OUSDI).

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.

Mr. Pannoni stated that this action item would be addressed through the report of the Personnel Security Clearance (PCL) Working Group from Deborah Smith (Office of Personnel Management) (OPM) and Valerie Heil (Defense Security Service) (DSS).

ACTION: The ODAA will respond to Industry regarding the status of multi-site corporate ISSMs within the next 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.

Mr. Pannoni stated that this action item would be addressed through the report of the Office of the Designated Approving Authority (ODAA) Working Group from David Cole, DSS. In addition, Mr. Pannoni stated that an update on the status of multi-site corporate Information System Security Managers (ISSMs) would be provided.

ACTION: A Foreign Ownership, Control, or Influence (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.

Mr. Pannoni deferred to the Chair who provided an update on the status of the FOCI Working Group. The Chair informed that due to a number of other ongoing initiatives, neither ISOO nor DSS was in a position to fully support the FOCI Working Group effort; thus, there has not been a meeting to date. It was noted, however, that Kathy Watson, DSS, and the Chair recognize the importance of the subject matter and remain committed to soliciting concerns, proposed solutions, and clarifications regarding FOCI from the NISPPAC members.

The Chair stated that a focused, extended meeting to discuss FOCI has been scheduled for Wednesday, February 4, 2009, at the National Archives Building, Washington, D.C. Within the next 30 days, a notice will be sent which will provide additional details and solicit initial input. The Chair noted that the goal of the meeting will be to identify concerns and areas for clarification, as well as to propose solutions to same. The Chair noted that the results from this meeting will help guide any future efforts regarding FOCI.

ACTION: The Chair stated that a focused, extended meeting to discuss FOCI has been scheduled for Wednesday, February 4, 2009, at the National Archives Building, Washington, D.C. Within the next 30 days, a notice will be sent that will provide additional details and solicit initial input.

III. Working Group Updates

A) PCL Working Group Report

Before commencing with the Working Group's update, the Chair expressed his appreciation to all of the members for their work since the group's creation in November 2006. A report on the Working Group's progress was provided by Ms. Smith and Ms. Heil. (Reference Appendix 1 for Working Group's PowerPoint presentation.)

Ms. Smith began her report by noting that the group is seeking to improve the PCL process for Industry. In order to do this, the Working Group has captured metrics on

each step of the process, starting with the beginning date when the subject is initiated into the Joint Personnel Adjudication System (JPAS) and ending on the date of adjudication. With these metrics, the Working Group has been able to note the average major timelines and the fastest 80%, 85%, and 90% of cases. Ms. Smith then reported on the Working Group's recorded End-to-End Performance Metrics, which included the submission, investigation, and adjudication timeframes.

Ms. Smith reported that the average cycle time of the End-to-End Industry Roll up for initial Top Secret and all Secret/Confidential clearance decisions for FY 2008 was 172 days. The average cycle time of the fourth quarter of FY 2008 was reported to be 143 days. Ms. Smith noted that the fourth quarter had a faster cycle time because the backlog of both investigations and adjudications had been addressed. In order to help reduce the overall timeliness of clearance decisions, the Working Group is focusing on reducing the amount of time, within Industry, of the initial processing stages.

In response to a question from Industry, Ms. Smith stated that the Working Group's metrics are different from the Intelligence Reform and Terrorism Prevention Act's (IRPTA) goals as the Working Group is including the front-end time when the subject is first initiated into JPAS. A discussion was then initiated on the reported metrics as they relate to IRPTA's goals. With regard to this topic, John Fitzpatrick (Office of the Director of National Intelligence) (ODNI) drew attention to a new subcommittee which was formed under the Performance Accountability Council (PAC), which has the role of broadening all performance measurement aspects of the clearance reform efforts. Mr. Fitzpatrick inquired as to whether there had been a discussion within the Working Group about aligning its goals with the goals of the Council. Ms. Smith responded that the Working Group is capturing metrics mainly to target areas of process improvement and to measure the effects of improvements. In response, Mr. Fitzpatrick suggested that the Working Group discuss the development of uniform methods of measurement, with the goal of having uniform definitions and numbers across the board. The Chair requested further information in order to discuss this suggestion in more depth.

Ms. Heil presented metrics on the FY 2008 adjudication inventory at the Defense Industrial Security Clearance Office (DISCO), noting an overall 90% decrease in total inventory. Ms. Heil noted that this decrease was achieved through mandatory overtime (which ceased in October), and an increased proficiency of adjudicators. Ms. Heil then stated that there was an overall reduction of 48% of Industry investigation cases at OPM.

Ms. Heil reviewed the top five reasons for e-QIP rejections, noting that two of the five were related to the issue of fingerprints. Ms. Heil informed the NISPPAC that the Department of Defense (DOD) is currently looking into a way for the e-QIP system to verify, before submission, that subjects have input all of the required information (e.g., selective service number). Ms. Heil briefly noted the value and importance of Industry's clearance projections through the Personnel Security Investigations (PSI) Projections Survey. Following this, Ms. Heil provided a DSS

automation update to include the Secure Web Fingerprint Transmission System. Ms. Heil noted that DSS has had a successful ongoing pilot program, with four industry partners, which has tested electronic fingerprint transmission. The NISPPAC was informed that further details will be provided prior to the full deployment and that the initial operating capability is planned for the third quarter of FY 2009.

Finally, Ms. Heil reported on the Case Management System (CMS) for DISCO, which is a system that would process electronic investigation files for adjudication. Ms. Heil reported that the Business Transformation Agency has assumed responsibility for deployment of CMS, which is expected for March 2009. It is believed that CMS will assist DISCO to help reduce overall timeliness, particularly with regard to the electronic transmission of cases from OPM to DISCO.

ACTION: The Chair requested further information about uniform definitions and methods of measurement, in order to discuss, in more detail, the suggestion of aligning the PCL Working Group with the goals of the PAC.

B) ODAA Working Group Report

A report on the Working Group's progress was provided by Mr. Cole. (Reference Appendix 2 for Working Group's PowerPoint presentation.)

Mr. Cole stated that the metrics presented represent data from the past year. In general, the metrics demonstrate an improvement in the overall timeliness of the accreditation process and Mr. Cole stated that he is confident that future improvements will continue to be made. He reported that, on average, it takes 35 days to receive an Interim Approval to Operate and the average wait time, which is the time period from when industry submits a System Security Plan (SSP) to the time when DSS begins the review process, is 20 days. Mr. Cole stated that ODAA has been able to electronically disseminate SSPs, which is expected to further improve overall timeliness.

Mr. Cole reviewed metrics pertaining to on-site verifications, informing the NISPPAC that 31% of systems required some level of modifications either due to minor or significant discrepancies. Mr. Cole stated that it is ODAA's goal to work with Industry to decrease this number. In response to Industry's inquiry, he stated that, in general, modifications are required because the systems reviewed do not always adequately represent the original SSPs. Mr. Cole added that, in line with the recommendations of the ODAA Working Group, DSS will begin to alert Industry of any significant issues and will begin to work with Industry on training opportunities.

Mr. Cole reviewed the metrics on SSP Reviews, and stated that on average, 24.5% of all plans submitted require some changes prior to the on-site verification for Approval to Operate. Mr. Cole then reviewed, and provided metrics for some of the common errors with SSPs. (See slide Nos. 6 and 7 in Appendix 2.) The Chair, in noting the increasing number of plans that had inaccurate or incomplete configuration diagram/system description, asked what the shift in numbers represented. Mr. Cole

stated that the shift correlates with the on-site verifications, wherein ODAA will find some sort of error and require a modification to the plan.

Mr. Cole informed that ODAA has developed standard SSP templates, which address the many common errors, and he expressed confidence that these templates will help bring about a decrease in the amount of errors. In response to a question from Industry, Mr. Cole stated that ODAA will start to bring corporate visibility to the common errors within specific companies, and if solicited, will conduct workshops and other training. He also stated that ODAA is building an on-line system which will allow for corporate-wide cage code visibility in order for companies to look at trends within facilities, ISSMs, common errors, etc. In response to additional questions, Mr. Cole stated that currently, ODAA is not capturing metrics based on company size; thus, ODAA's metrics are not broken down into subsets of larger companies versus smaller companies. In clarifying, Mr. Cole stated that ODAA is not currently tracking accreditation information through the standard Industrial Security Facilities Database. However, once the online system is deployed, ODAA will be able to associate cage codes with industry ranking categories and thus, be able to capture metrics in much more specificity.

Mr. Cole finished his presentation with a discussion on the standards, guidance, and policies that ODAA is currently working. He stated that the standardized SSP templates should cover roughly 90% of the SSPs that are reviewed. Mr. Cole reported that ODAA is also working on establishing technical standards that will be in conformance with DOD and other government initiatives (e.g., ODNI initiatives). Further, ODAA is working with OUSDI to draft an Industrial Security Letter (ISL), which will provide additional guidance for the DSS Accreditation Process and Technical Standards. Mr. Cole also reported that ODAA completed the corporate/traveling ISSM pilot project and is planning on drafting an ISL to provide further guidance on the concept. ODAA is also working on ISSM training and certification guidance, Radio Frequency Identification Directive, and National Industrial Security Program Operating Manual (NISPOM) Chapter 8 updates. In response to a question, Mr. Cole stated that the technical standards initiatives and the Chapter 8 updates are being worked simultaneously. Mr. Cole also stated that when establishing standards, whether technical or process, ODAA reviews all the appropriate standards (e.g., Defense Information Systems Agency, NISP, National Security Agency, etc.) in order to identify which standards are the best to utilize. In response to a request from the Chair, Mr. Cole stated that ODAA will clarify what standards are being referenced at the next meeting. In concluding the presentation, Mr. Cole briefly reviewed some of the topics discussed during ODAA workshops, for example, security templates, guidance on downgrading a classified system, etc.

At the conclusion, the Chair requested that DSS continue to provide metrics updates at the NISPPAC meetings. Following this, the Chair announced that the ODAA Working Group will be suspended, in order to start up the FOCI Working Group. With regard to the FOCI Working Group, it is hoped that an understanding of the

issues will be gained so that they can be addressed. Once this occurs, resources can be used to address ODAA Working Group concerns.

ACTION: Per the request of the Chair, ODAA will clarify what standards are being reviewed and used for reference and guidance when ODAA is establishing its own technical and/or process standards.

The Chair announced that the ODAA Working Group will be suspended, in order to start up the FOCI Working Group. Despite this suspension, the Chair requested that DSS continue to provide metrics updates at the NISPPAC meetings.

IV. New Business

A) Controlled Unclassified Information

Patrick Viscuso, Controlled Unclassified Information Office (CUIO), National Archives and Records Administration (NARA), and Frederick V. Riccardi, Member, CUI Council (Private Sector), presented on this topic. (Reference Appendix 3 for associated PowerPoint presentation.)

Dr. Viscuso briefly reviewed the history of CUI, starting with the May 9, 2008, Presidential Memorandum, "Designation and Sharing of Controlled Unclassified Information," and reinforced the point that a Presidential Memorandum will not lose its legal effectiveness upon a change in administration. He noted that the CUIO has been established within NARA and that the Program Manager, Information Sharing Environment has activated the CUI Council, which is a subcommittee of the Information Sharing Council and the CUI Council had its first meeting on August 21, 2008. The CUI Council serves as the primary advisor to the Executive Agent on issues pertaining to the CUI framework. Dr. Viscuso then reviewed the CUI Governance Structure, stressing the vital role of departments and agencies.

Dr. Viscuso briefed on the milestones and actions that have already been achieved by the CUIO and those that are forthcoming. With regard to the setup and handling of CUI guidance, he informed that the CUIO is attempting to handle those parts of the CUI guidance and framework that will have the greatest budgetary impact for both Industry and Government. Dr. Viscuso also stated that the CUIO is mindful that the CUI framework presents an opportunity to end confusion, improve information sharing, and bring about standardization across the information sharing community. He noted that the CUI framework must be implemented by May 9, 2013.

Mr. Riccardi then expressed his thoughts regarding CUI and Industry. Mr. Riccardi noted that during the setup of CUI, Industry can use its lessons learned and "best practices" in handling proprietary information, in order to fulfill many of the CUI objectives.

Following the presentation, the Chair acknowledged the dedicated service of Mr. Riccardi. The Chair also stressed to both Government and Industry that CUI markings will not begin until 2011 and asked they be mindful of this, and further stressed that pending further CUI policy development, requirements should not be levied on Industry.

B) Joint Security and Suitability Process Reform Team Update

Mr. Fitzpatrick presented on this topic. (Reference Appendix 4 for associated PowerPoint presentation.)

Mr. Fitzpatrick began by discussing the governance structure which was enacted through the passage of Executive Order (E.O.) 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," on June 30, 2008. Mr. Fitzpatrick noted that the policy, process, information technology, and training functions that are part of the reform effort are now structured under the PAC and its two subcommittees, the Performance Measurement and Management Subcommittee (PMMS) and the Training Subcommittee. The PMMS seeks to expand beyond the IRTPA requirements for performance measurements and seeks to use performance measurements as a tool to improve the security clearance and suitability end-to-end processes. Mr. Fitzpatrick suggested that the definitions, tools, measures and reporting structures of both Industry and Government be aligned for better clarity and understanding.

Mr. Fitzpatrick advised that E.O. 13467 mandates the alignment of suitability and security clearance processes and designates the Director, OPM, as the Suitability Executive Agent and ODNI as the Security Executive Agent. The E.O. also clarifies Continuous Evaluation policy.

Mr. Fitzpatrick also discussed the contents of the upcoming report to the President on the status and on-going plans of the reform effort. Besides serving as an informative piece to the outgoing administration, Mr. Fitzpatrick noted that the report will serve as a plan of action during the transition period and thereafter.

At the conclusion of the presentation, Industry inquired as to when the security and suitability processes would be reduced, and also, what part of the suitability process would be abbreviated. Mr. Fitzpatrick stated that the investigative standards incorporated a concept of aligning investigative requirements of suitability cases with those of clearance cases in a tiered model. Doing such would reduce the variations in investigation types and the composition between the two processes so that the same information resulting from a security clearance investigation of an individual could be used for making a suitability determination for that person. Mr. Fitzpatrick stated that the investigative standards state that one is to build upon the lower tiers in order to reduce and eliminate duplicative action. Mr. Fitzpatrick stated that it has yet to be determined when this translates into performance because one of the challenges facing the PMMS is to develop performance measures for suitability.

C) Automated Dissemination of Threat Data to Industry

Mr. Lewis presented on this topic.

He informed that his presentation would be related specifically to the Defense Industrial Base Cyber-Security Information Assurance Program. This program is a voluntary, collaborative operational information sharing environment that involves the Federal government and Defense Industrial Base (DIB) partners. This sharing environment involves the sharing of threat information data by DOD with its DIB partners, with the understanding that though threats cannot be completely eliminated, the risks posed by same can be more effectively mitigated and managed through a voluntary partnership between DOD and DIB.

Mr. Lewis reported that because of the vast community, collaboration with every member of the DIB is not practical. Therefore, DOD has developed a phased-approach, which will gradually increase the number of participants as the program's policies, procedures, and processes become more refined.

D) FOCI Policy Issues

Mr. Lewis presented on this topic.

He stated that there will be changes made to the NISPOM with regard to FOCI policy issues. As discussed during the last NISPPAC meeting, the changes include the defining of "material change" and "significant change," the present ambiguity in the NISPOM with respect to what happens after a cleared company has been acquired by a foreign interest when there is no mitigation in place, and issues regarding corporate family certificates pertaining to foreign interests.

Mr. Lewis reported that, upon review of the relevant issues, it became apparent that changes were needed for the NISPOM, in general. At this time, dialogue has been initiated with ODNI, Department of Energy (DOE), DSS, and ISOO; the Nuclear Regulatory Commission will be involved in future discussions. Finalizing the update, Mr. Lewis stated that the Government plans to develop basic positions on the relevant issues, and will then invite Industry input through the NISPPAC framework.

In responding to a question from Industry regarding the possible cancellation of the NISPOM supplement, Mr. Lewis informed that there have been discussions to make modifications in Chapter 9 (such as placing references within Chapter 9 to other publications that provide guidance on Special Access Programs). In response to a question regarding changes to the Industrial Security Regulation (ISR), he stated that the ISR has been rewritten and DOD is preparing for internal, pre-coordination of the document.

E) National Defense Appropriation Act (NDAA) Reporting Requirements Update (Impact & Implementation)

Mr. Lewis presented on this topic.

He provided a brief update on the responsibilities of DOD under the Act. Mr. Lewis noted the dedication of sufficient resources for oversight of contractors and the prescribing and revising of regulation and policy guidance as two examples. Following this, Mr. Lewis listed those reports which DOD will have to provide to Congress in order to detail the status of industrial security within DOD.

F) DSS Update

Ms. Watson presented on this topic.

She reported that DSS has made significant changes within the past year and will continue its process of transformation. Reference was made to the DSS study, which was requested by the Deputy Secretary of Defense. Ms. Watson stated that the key recommendation of the study was that DSS needed to focus on enhancing the NISP through reinvigorating the security education, training, and awareness program. She also reported that DSS is appropriately funded so that it is not only able to process PCLs for Industry, but is also able to implement agency-wide programs. Ms. Watson noted that DSS's industrial security mission is growing and that DSS is hiring accordingly.

In order to meet the aforementioned study's recommendations and manage the entire program, DSS has reorganized itself such that there is an increased emphasis on field and counter-intelligence activities. Ms. Watson noted that DSS now has three Directors for Industrial Security: Director for Industrial Security Policy and Programs (responsible for industrial security policy, FOCI, and International); Director for Industrial Security Field Operations (responsible for ODAA, facility clearance branch, DISCO, and any direct support to field); and Director of Counter-Intelligence.

Ms. Watson stated that DSS is focusing on integrating counter-intelligence efforts much more intricately into the industrial security program. The goal is to forge an enhanced relationship with Industry to better protect information and maintain Industry's competitive edge. Ms. Watson reported that the counter-intelligence office is trying to become more proactive. She also informed that the unclassified version of "A Trend Analysis of Reporting from Defense Industry" is undergoing final approval and has an estimated second quarter 2009 release. This report will contain data from FY 04-05 and FY 06-07 and classified hard copies will be available in December 2008. Dissemination to cleared defense industry will be coordinated with the industrial security field operations.

Ms. Watson provided a report on the PCL Office. She informed that DSS has staffed the Clearance Liaison Office, which works with OPM and department components on the quality of oversight to improve the PSI process. Ms. Watson stated that DSS is in the process of implementing recommendations from the aforementioned study in this area. Ms. Watson also reported that DSS has established a Clearance Oversight Office, which is responsible for developing and implementing DOD PSI workload

projections, monitoring PSI funding, resolving billing issues, and working with OPM on metrics. She noted that a portion of the office will remain in DSS and will focus on Industry, whereas other parts will be transitioning sometime in the next calendar year.

Ms. Watson expressed thanks to those who participated in DSS's online PSI Projections survey. Remarking on the success of the survey, she noted that 92% of the cleared contractor population participated and stated that the results will help DSS understand Industry's requirements. Ms. Watson informed that the PSI survey will be conducted annually in the spring to coincide with DSS's budget cycle.

Ms. Watson also provided an update on DSS's training academy, noting that a new web-based course, "Facility Security Officer's Role in the NISP," and an electronic newsletter have been introduced. She reported that the Academy released a new resource tool for security professionals this past August.

On the issue of e-FOCI, Ms. Watson stated that DSS is still assessing the e-FOCI tool and intends to make a decision regarding the tool within the next few months. She also stated that a training component would be included with the tool's roll-out. In response to a question from Industry regarding the roll-out, Ms. Watson stated that the roll-out would occur as material changes occur. She reaffirmed that there will be no need for duplicate e-FOCI submissions, as the idea is to streamline the process between DOD and DOE. Mr. Lewis also remarked that there is reciprocity between DOE and DSS regarding FOCI determinations.

Industry then inquired about the DISCO transfer. Ms. Watson stated that DISCO will stay within DSS in order to properly integrate the counter-intelligence office.

G) Combined Industry Presentation

Vincent Jarvie, NISPPAC Industry Spokesperson, presented on this topic. (Reference Appendix 5 for associated PowerPoint presentation.)

Mr. Jarvie expressed his appreciation to Mr. Hamilton and Mr. Schlehr for their service on the NISPPAC and welcomed new members, Mr. Conway and Mr. Sanders.

Mr. Jarvie stated that one of the key issues to be addressed is a more focused approach between the NISPPAC and Memorandum of Understanding (MOU) groups, as there are higher-level, transcending issues that need to be addressed. He reported that there have already been meetings to discuss these transcending issues and that these high-level issues will be tracked by Industry at the NISPPAC and larger MOU group levels.

With regard to Industry's key issues, Mr. Jarvie identified the importance of the ODAA Working Group and the PCL Working Group. He noted that these two Working Groups have helped bring transparency to government rules and regulations.

As such, Mr. Jarvie noted the efforts and progress of the ODAA Working Group and expressed Industry's interest in continued collaboration with Government. He stressed the importance of the continued effort to refine the submission processes. With regard to the PCL Working Group, Mr. Jarvie noted the importance of the PCL process and program and stressed the importance of having a predictable and consistent clearance processing program.

He then presented the four main concerns of Industry, which were identified as: sharing of threat information, CUI, FOCI, and PCL processing.

Mr. Jarvie thanked Mr. Lewis for the update on the NDAA, and he asked Mr. Lewis to let Industry know if any resources are needed in order to meet the requirements of the NDAA.

Mr. Jarvie then addressed the issue of sharing of threat information. He noted that Industry is experiencing threats from three areas: cyber, the insider, and front companies. Threats are experienced on both the front and back end, and Industry is looking for as much assistance as possible on the front end. Mr. Jarvie stressed the seriousness of this issue for Industry, noting that national security is now linked to economic well-being. In conclusion, he remarked that the answer to this national security threat is that, collectively, both Government and Industry, require indication and warning, thus necessitating the sharing of threat information. Mr. Jarvie stated that the role of Industry is to not only be the receiver of threat information but to also help validate such information.

He then addressed CUI. After thanking the CUI presenters for their presentation, Mr. Jarvie expressed his appreciation to Mr. Riccardi for representing Industry. Concluding, Mr. Jarvie noted that CUI policy development has been a transparent effort.

Mr. Jarvie then expressed thanks for the presentation on FOCI and articulated his interest in the upcoming February 4, 2009, meeting. He stated that he looked forward to addressing the many aspects of FOCI. Mr. Jarvie stressed the need for an electronic reporting process and emphasized the importance of feedback to ensure that all needs are being met.

Mr. Jarvie then briefly commented on the Joint Security and Suitability Process Reform Team update. He stated that Industry wants to be prepared to leverage the efficiencies of the initiative as soon as available.

G) Discussion

As there was significant discussion during the individual presentations, the Chair determined that no further discussion time was needed.

H) NISP Signatories Update

No updates were reported.

I) Proposed Amendments to the Bylaws

The Chair noted that due to current standard operating procedures, and requirements established by the Federal Advisory Committee Act, amendments to the NISPPAC Bylaws are required. As such, the Chair requested that the NISPPAC membership review the current Bylaws prior to the next NISPPAC meeting. (Reference Appendix 6.) Proposed revisions to the Bylaws will be sent to the membership for review prior to the next meeting, and these revisions will be on the next meeting's agenda.

ACTION: Per the request of the Chair, the NISPPAC membership should review the current NISPPAC Bylaws prior to the next NISPPAC meeting. The Chair will distribute to the NISPPAC membership, for review, the proposed revisions to the Bylaws prior to the next NISPPAC meeting. A vote on the proposed revisions will be on the next meeting's agenda.

V. GENERAL OPEN FORUM

No comments were made.

VI. Closing Remarks and Adjournment

Before adjourning the meeting, the Chair reminded the members to provide their top five NISP-related concerns by Monday, December 8, 2008. The Chair also reminded the members of the upcoming FOCI meeting scheduled for Wednesday, February 4, 2009. Finally, the Chair informed the members that the next NISPPAC meeting had been scheduled for Thursday, April 2, 2009.

The meeting adjourned at 12:06 pm.

Summary of Action Items

- A)** The Chair requested the NISPPAC members provide their top five issues or areas of concern regarding the NISP, by close of business, Monday, December 8, 2008.
- B)** The Chair stated that a focused, extended meeting to discuss FOCI has been scheduled for Wednesday, February 4, 2009, at the National Archives Building, Washington, D.C. Within the next 30 days, a notice will be sent that will provide additional details and solicit initial input.
- C)** The Chair requested further information about uniform definitions and methods of measurement, in order to discuss, in more detail, the suggestion of aligning the PCL Working Group with the goals of PAC.
- D)** Per the request of the Chair, ODAA will clarify what standards are being reviewed and used for reference and guidance when ODAA is establishing its own technical and/or process standards.

- E) The Chair announced that the ODAA Working Group will be suspended, in order to start up the FOICI Working Group. Despite this suspension, the Chair requested that DSS continue to provide metrics updates at the NISPPAC meetings.

- F) Per the request of the Chair, the NISPPAC membership should review the current NISPPAC Bylaws prior to the next NISPPAC meeting. The Chair will distribute to the NISPPAC membership, for review, the proposed revisions to the Bylaws prior to the next NISPPAC meeting. A vote on the proposed revisions will be on the next meeting's agenda.

Appendix 1- Personnel Security Clearance Working Group Presentation

Appendix 2- Office of the Designated Approving Authority Working Group Presentation

Appendix 3- Controlled Unclassified Information Presentation

Appendix 4- Joint Security and Suitability Process Reform Team Presentation

Appendix 5- Combined Industry Presentation

Appendix 6- NISPPAC Bylaws

Appendix 1
Personnel Security Clearance Working Group Presentation

NISPPAC WG's End-To-End Performance Metrics

Includes Submission, Investigation, & Adjudication Time

FY 2008 End to End Industry Roll up for Initial Top Secret and Secret/Confidential Clearance Decisions

- **All 139,309 Industry cases: 172 day average cycle time**
- **Fastest 90% of cases: 144 day average**
- **Fastest 85% of cases: 135 day average**
- **Fastest 80% cases: 127 day average**

FY 2008 End to End Break Down for Industry

- **TS Initial – All 30,048 cases: 223 day average cycle time**
- **TS Initial – Fastest 80% cases: 177 days average**
- **Secret – All 109,261 cases (Initial & PR): 158 day average**
- **Secret – Fastest 80% cases: 115 days**
- **TS PR – All 48,133 cases: 278 day average**
- **TS PR – Fastest 80% cases: 225 days**

NISPPAC WG's End-To-End Performance Metrics Includes Submission, Investigation, & Adjudication Time

FY 2008 4th Quarter End to End Industry Roll up for Initial Top Secret and Secret/Confidential Clearance Decisions

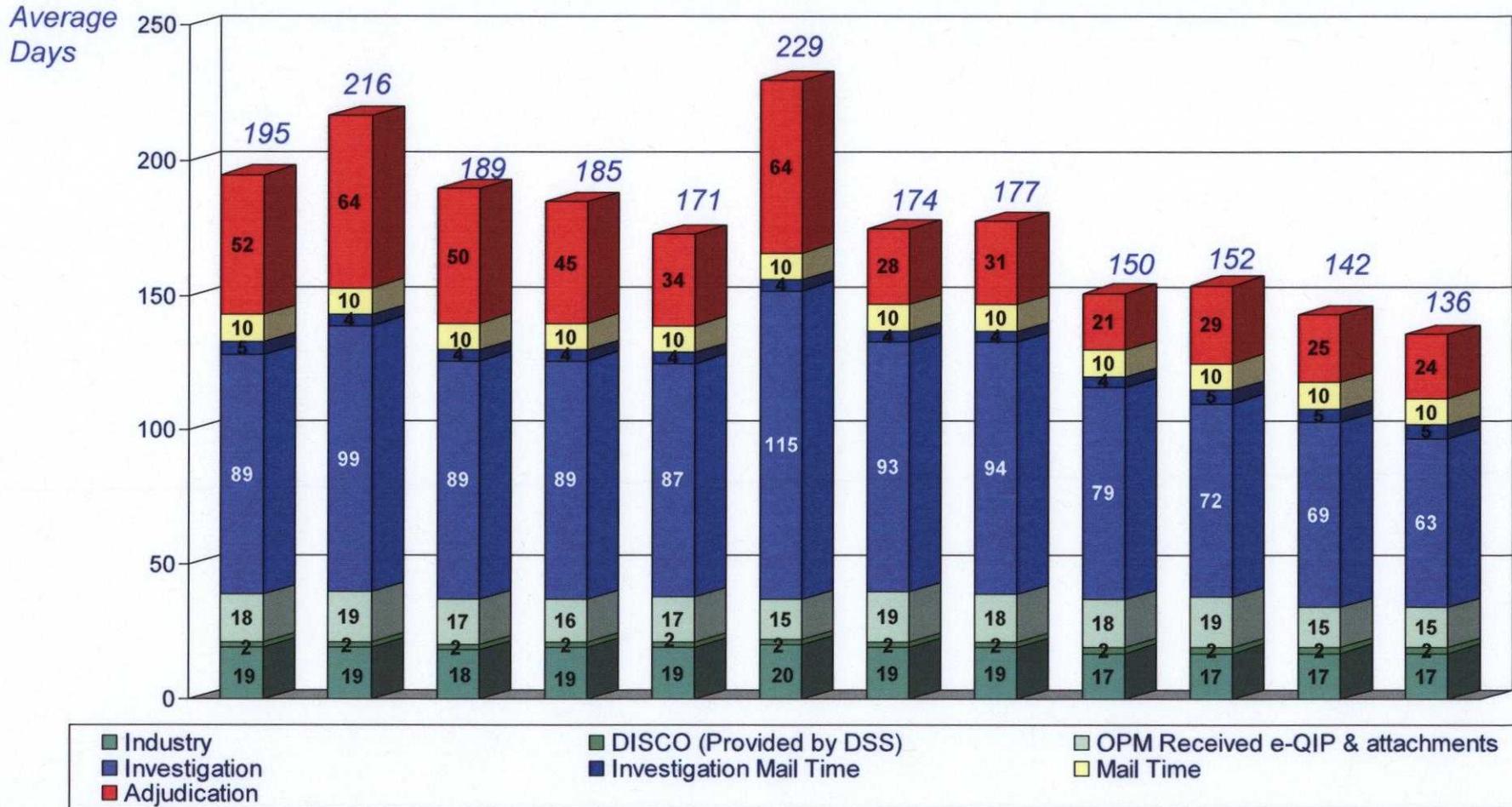
- **All 32,548 Industry cases: 143 day average cycle time**
- **Fastest 90% of cases: 113 day average**
- **Fastest 85% of cases: 107 day average**
- **Fastest 80% cases: 102 day average**

FY 2008 4th Quarter End to End Break Down for Industry

- **TS Initial – All 6,472 cases: 178 day average cycle time**
- **TS Initial – Fastest 80% cases: 130 days average**
- **Secret – All 26,076 cases (Initial & PR): 135 day average**
- **Secret – Fastest 80% cases: 95 days**
- **TS PR – All 19,127 cases: 243 day average**
- **TS PR – Fastest 80% cases: 177 days**

NISPPAC Working Group's End-To-End Metrics (Industry)

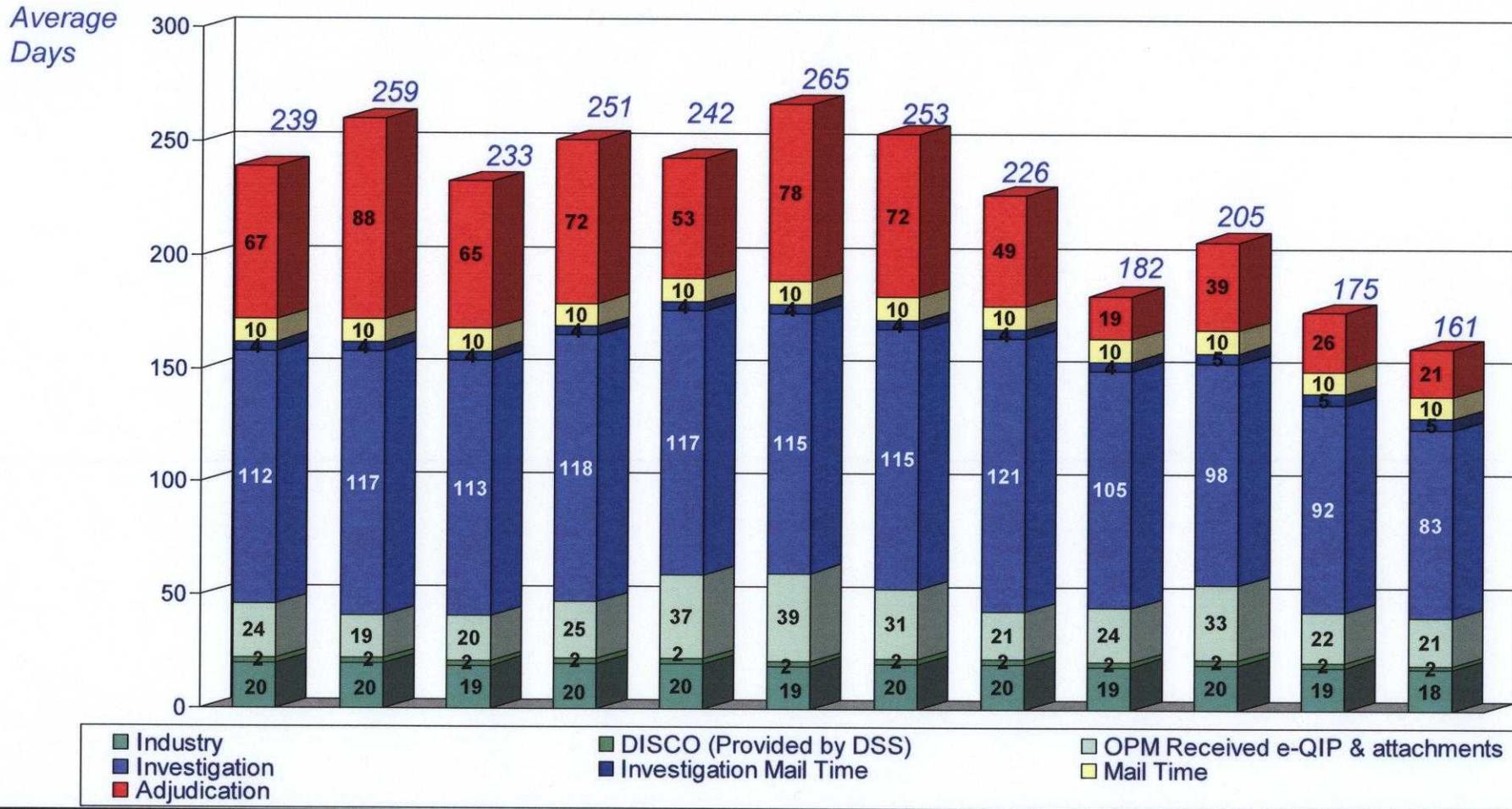
Initial Top Secret and All Secret/Confidential Security Clearance Decisions



Adjudications actions taken:	Oct 07	Nov 07	Dec 07	Jan 08	Feb 08	Mar 08	Apr 08	May 08	June 08	July 08	Aug 08	Sept 08
Sampling limited to clearances submitted using e-QIP	9,698	10,991	11,187	14,134	12,333	15,698	10,973	14,262	13,061	9,203	10,696	11,719

Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested. 3
 The present reject rate is 10.6% for DISCO and 4.7% 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

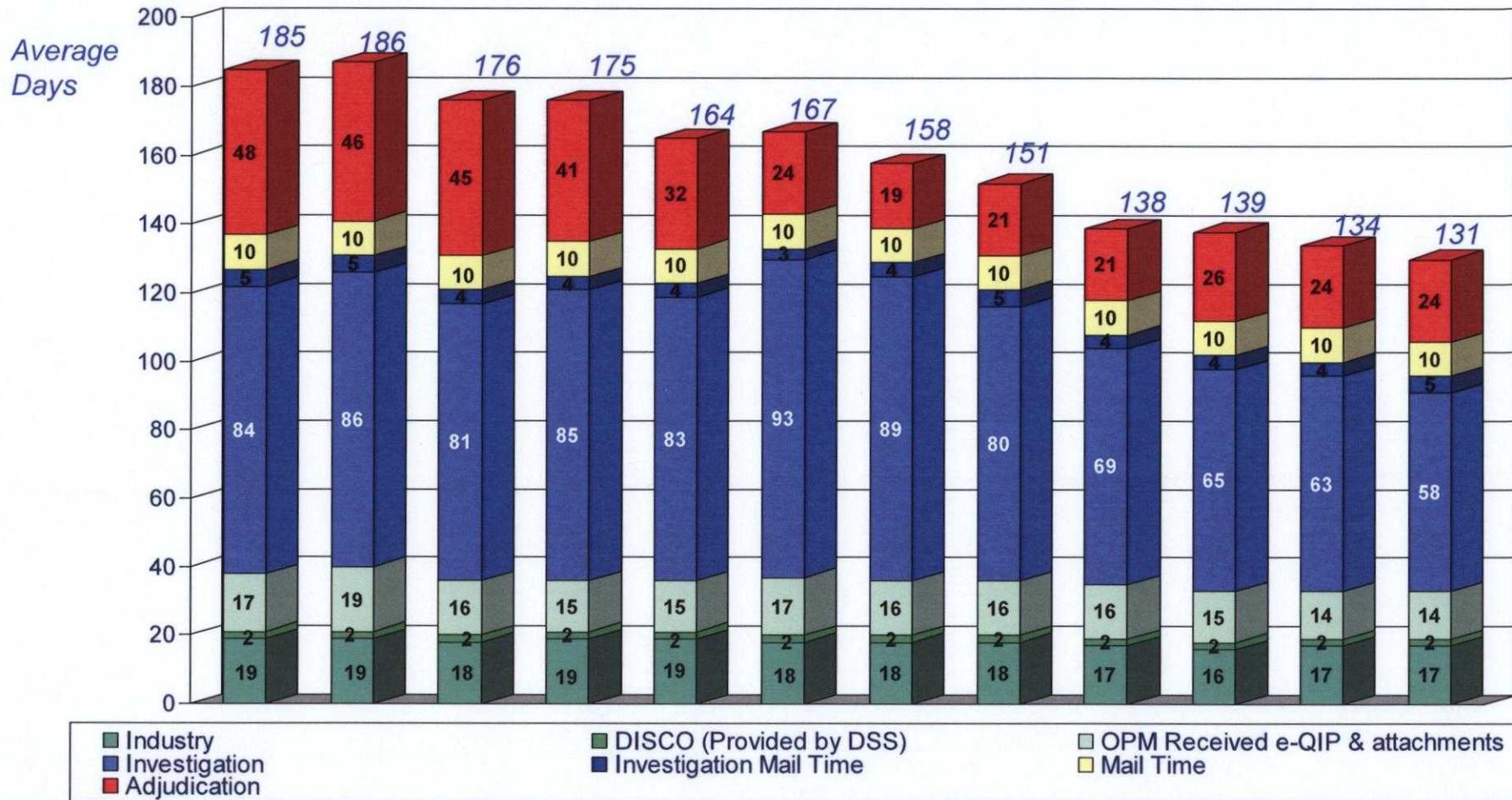


Adjudications actions taken:	Oct 07	Nov 07	Dec 07	Jan 08	Feb 08	Mar 08	Apr 08	May 08	June 08	July 08	Aug 08	Sept 08
Sampling limited to clearances submitted using e-QIP	1,756	4,582	2,682	1,733	1,120	1,416	1,798	4,984	3,504	1,854	2,220	2,213

Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested.

The present reject rate is 10.6% for DISCO and 4.7% for OPM. The time span for the rejections is not included in the above metrics.

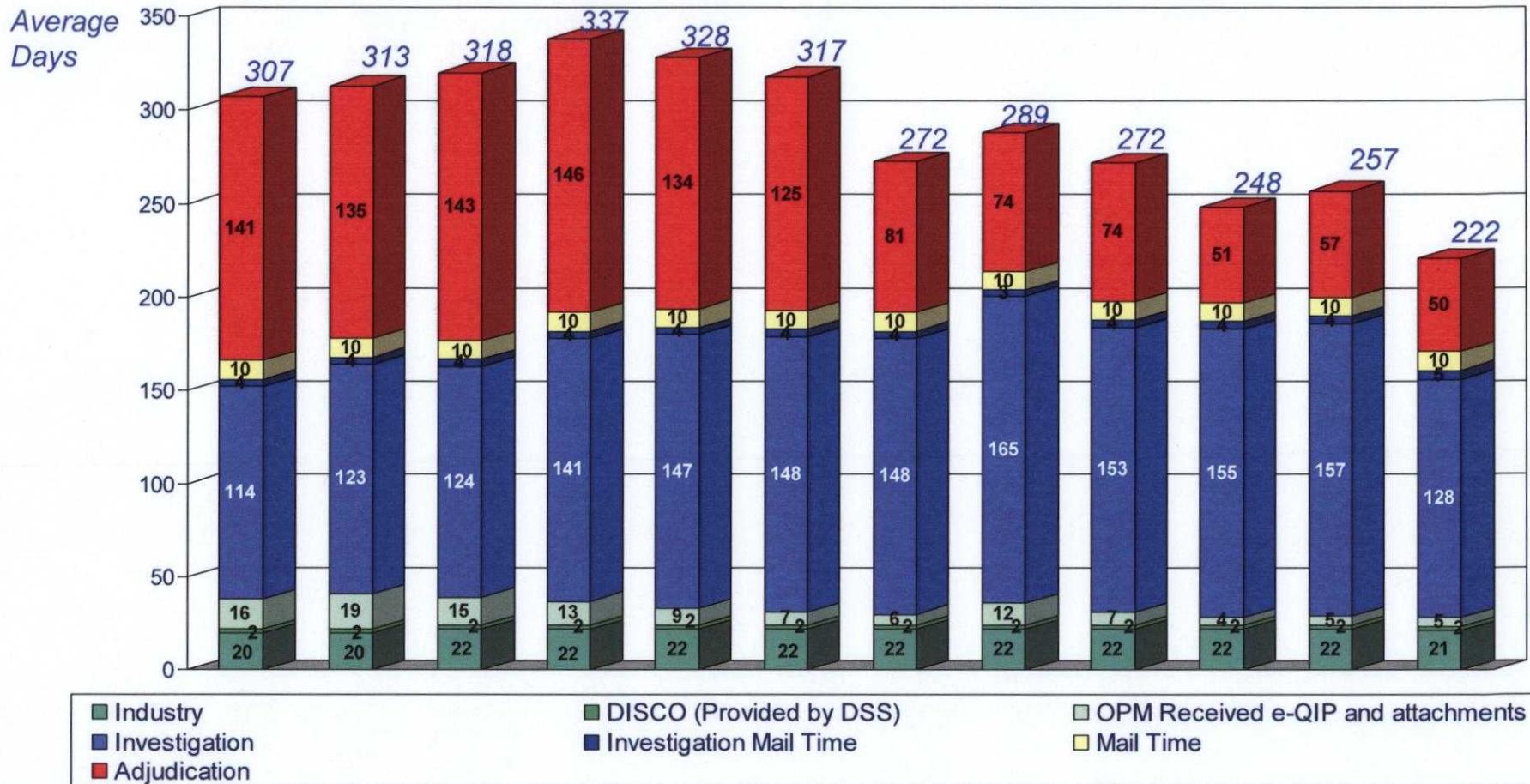
NISPPAC Working Group's End-To-End Metrics (Industry) All Secret/Confidential Security Clearance Decisions



Adjudications actions taken:	Oct 07	Nov 07	Dec 07	Jan 08	Feb 08	Mar 08	Apr 08	May 08	June 08	July 08	Aug 08	Sept 08
Sampling limited to clearances submitted using e-QIP	7,942	6,409	8,505	12,401	11,213	8,706	9,175	9,278	9,557	7,349	8,476	9,506

Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested. The present reject rate is 10.6% for DISCO and 4.7% for OPM. The time span for the rejections is not included in the above metrics. 5

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	Apr 08	May 08	June 08	July 08	Aug 08	Sept 08
Sampling limited to clearances submitted using e-QIP	2,389	1,116	1,347	2,938	3,387	5,576	5,452	2,096	4,705	7,491	6,459	4,858

Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested. 6
The present reject rate is 10.6% for DISCO and 4.7% for OPM. The time span for the rejections is not included in the above metrics.

DISCO

FY08 ADJUDICATION INVENTORY

CASE TYPE	Q1 FY 08	Q2 FY 08	Q3 FY 08	Q4 FY 08	Delta (Q1 vs Q4)
NACLC	11,449	488	240	1953	-83%
SSBI	9,337	5,625	30	354	-96%
SBPR	4,899	3,752	5,973	757	-85%
PPR	8,945	4,923	4,210	330	-96%
TOTAL PENDING	34,630	14,788	10,453	3,394	-90%

Overall reduction of 90% for NACLC, SSBI, SBPR and Phased PR case types from 1Q to 4Q of FY08.

Achieved through mandatory overtime and increasing proficiency of adjudicators hired during the last 12-18 months.

INDUSTRY CASES AT OPM

FY08 INVESTIGATION INVENTORY

CASE TYPE	Q1 FY 08	Q2 FY 08	Q3 FY 08	Q4 FY 08	Delta (Q1 vs Q4)
NACLC	29,575	25,085	22,077	15,561	-47%
SSBI	14,110	8,796	7,404	6,720	-52%
SSBI-PR	11,761	9,943	5,639	4,167	-65%
Phased PR	7,711	7,749	6,734	6,408	-17%
TOTAL PENDING	63,157	51,573	41,854	32,856	-48%

Overall reduction of 48% for NACLC, SSBI, SBPR and Phased PR case types from 1Q to 4Q of FY08.

Rejections & Tips for Successful eQIP Submissions

• FY08 REASONS FOR REJECTION

(Source: Query of the 25 Facilities with the most rejects in FY 08)

- Missing/Insufficient In-Laws Information 1
- Missing Selective Service Number 2
- Non-receipt of fingerprint cards within 30 days of submission 3
- Not listing proper Current Employer 4
- Rejected fingerprint cards: illegible / unclassifiable 5

• Guidance/Tips on DSS Website: www.dss.mil

• Personnel Security Clearance:

- <https://www.dss.mil/GW/ShowBinary/DSS/psco/psco.html>

• JPAS:

- http://dssa.dss.mil/seta/documents/appli_tips_for_success_e-qip_submission.pdf

• SETA

- <http://dssa.dss.mil/seta/downloads.html>

INDUSTRY CLEARANCE SUBMISSIONS VS PROJECTIONS

- OMB performance goal is +/- 5%
 - 4Q Status: At the close of FY08, Industry clearance submissions were .9% above overall Industry/DSS projections.
 - Demonstrates the value of projections provided by Industry through the annual PSI Projections Survey.

FY08 Projection	Weekly Projected	Year to Date	% of Projection
179,070	3,444	3,474	100.9%

DSS Automation Update

On October 30, 2008, DSS provided an automation update with highlights as noted:

- **Secure Web Fingerprint Transmission System (SWFT)**
 - Cleared Contractor Submission of Electronic Fingerprint Files
 - Modeled on Army's "store and forward" system at 85 installations
 - Contractor firms and associations will control the front-end scanners
 - DSS will operate and maintain server infrastructure
 - Pilot with 4 industry partners from 30 Jun 08 - 30 Nov 08
 - Further details of this effort will be provided prior to full deployment
 - Initial Operating Capability planned 3Q FY09
- **Case Management System (CMS) for DISCO**
 - Processes electronic investigation files for adjudication
 - BTA has assumed responsibility for this deployment, expected Mar 09
 - DSS also working now to create interfaces to JPAS, DCII, and ISFD

Appendix 2
Office of the Designated Approving Authority
Working Group Presentation

NISPPAC ODAA WORKING GROUP

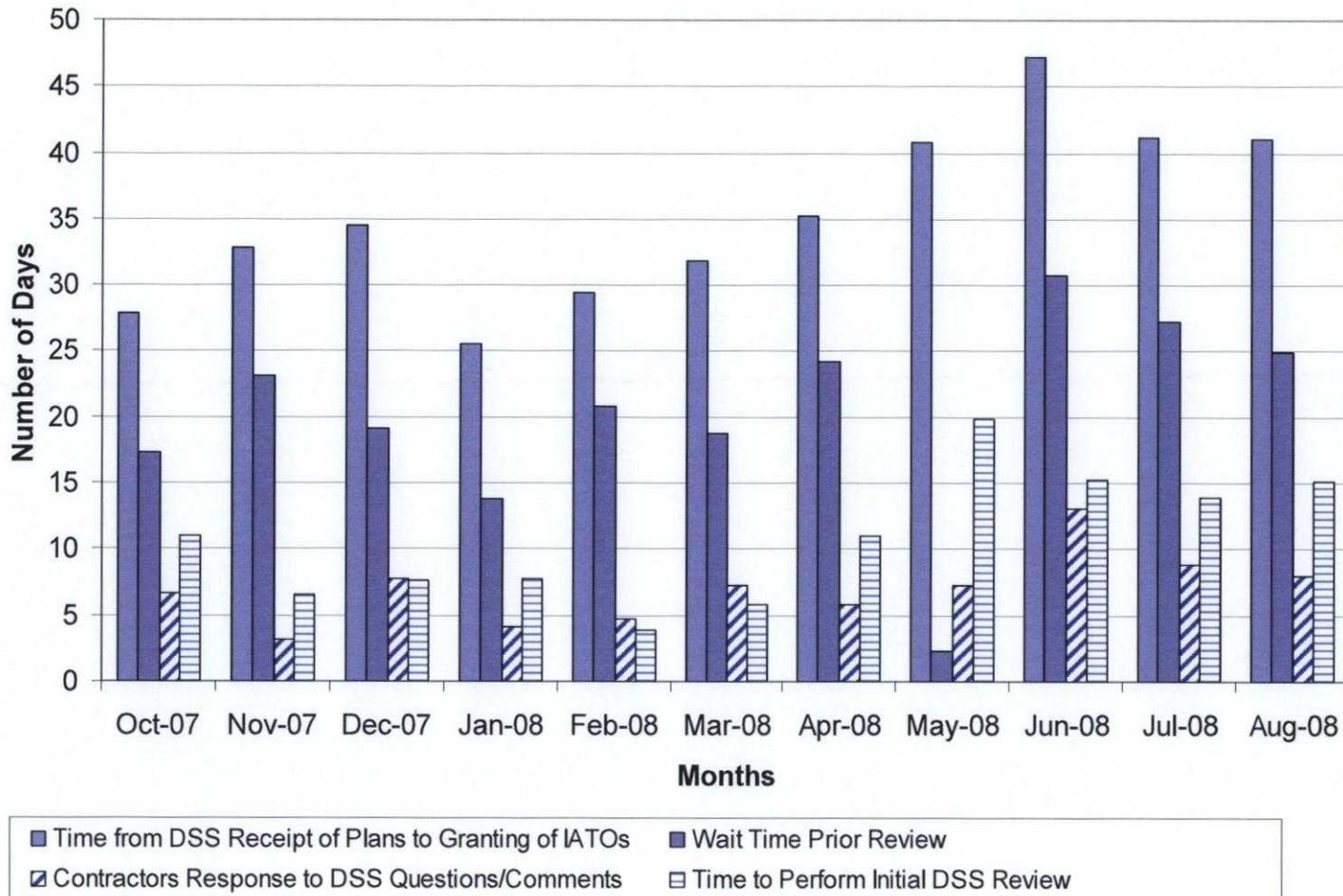
20 NOV 2008

Background of the NISPPAC ODAA Working Group

- Impetus: Director, DSS and Director, ISOO agreed to establish a working group to develop metrics to measure the end-to-end Certification and Accreditation (C&A) process for information systems
- Established: August 2007
- Composition: ISOO, Industry, DSS

DSS, ODAA Improving Accreditation Timeliness and Consistency

ODAA Metrics for # Days to Process Plan Submissions



During the Past Year Oct 2007 – August 2008

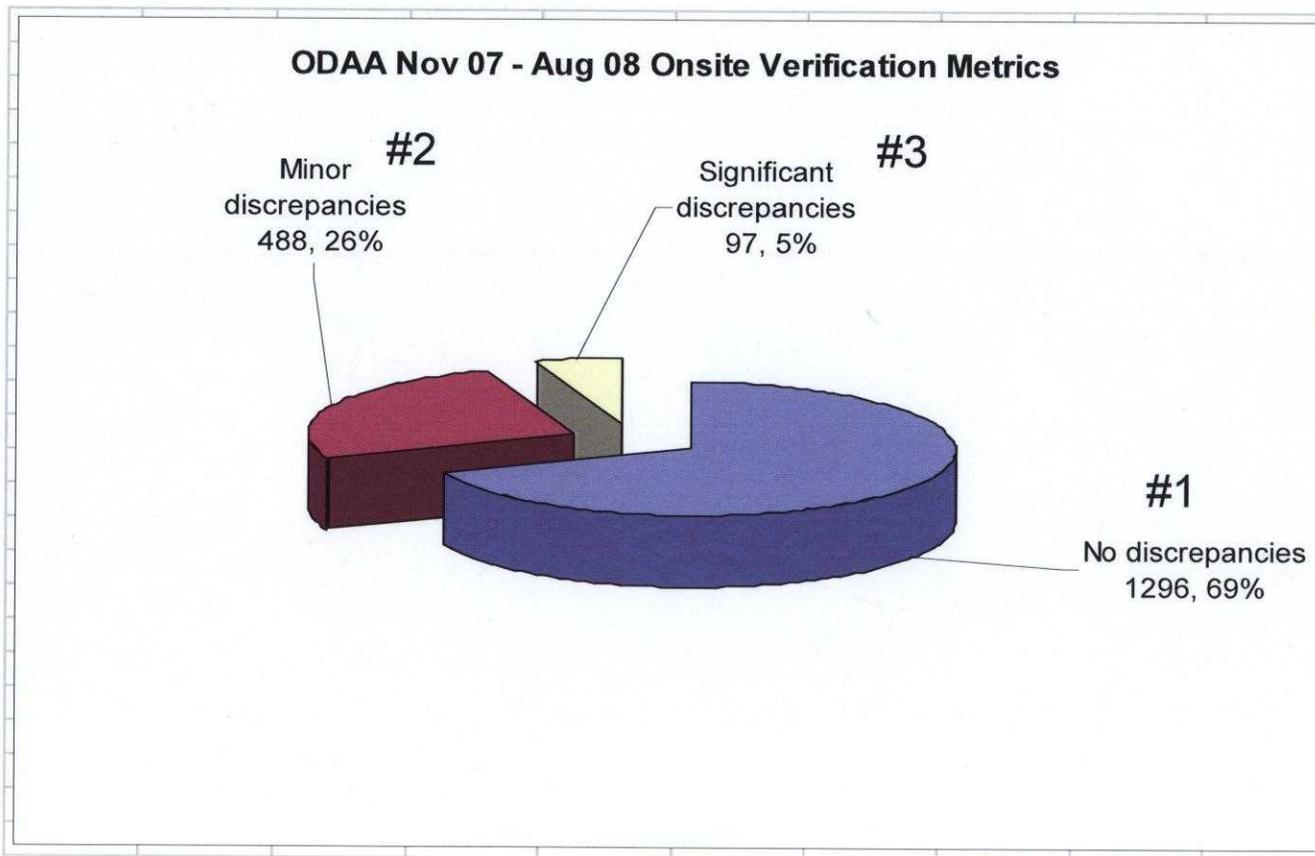
- Average number of Days to Receive an IATO after receipt of a Submission is 35 Day
- Average Waiting Time before a review process is initiated is 20 Days
- Average number of Days for the Review time to be completed is 11 Days

Currently – August 2008

- Average number of Days to Receive an IATO after receipt of a Submission is 43 Day
- Average Waiting Time before a review process is initiated is 25 Days
- Average number of Days for the Review time to be completed is 18 Days

DSS, ODAA Metrics and Organization

On-site Verification Stats (31% Required Some Level Modifications)



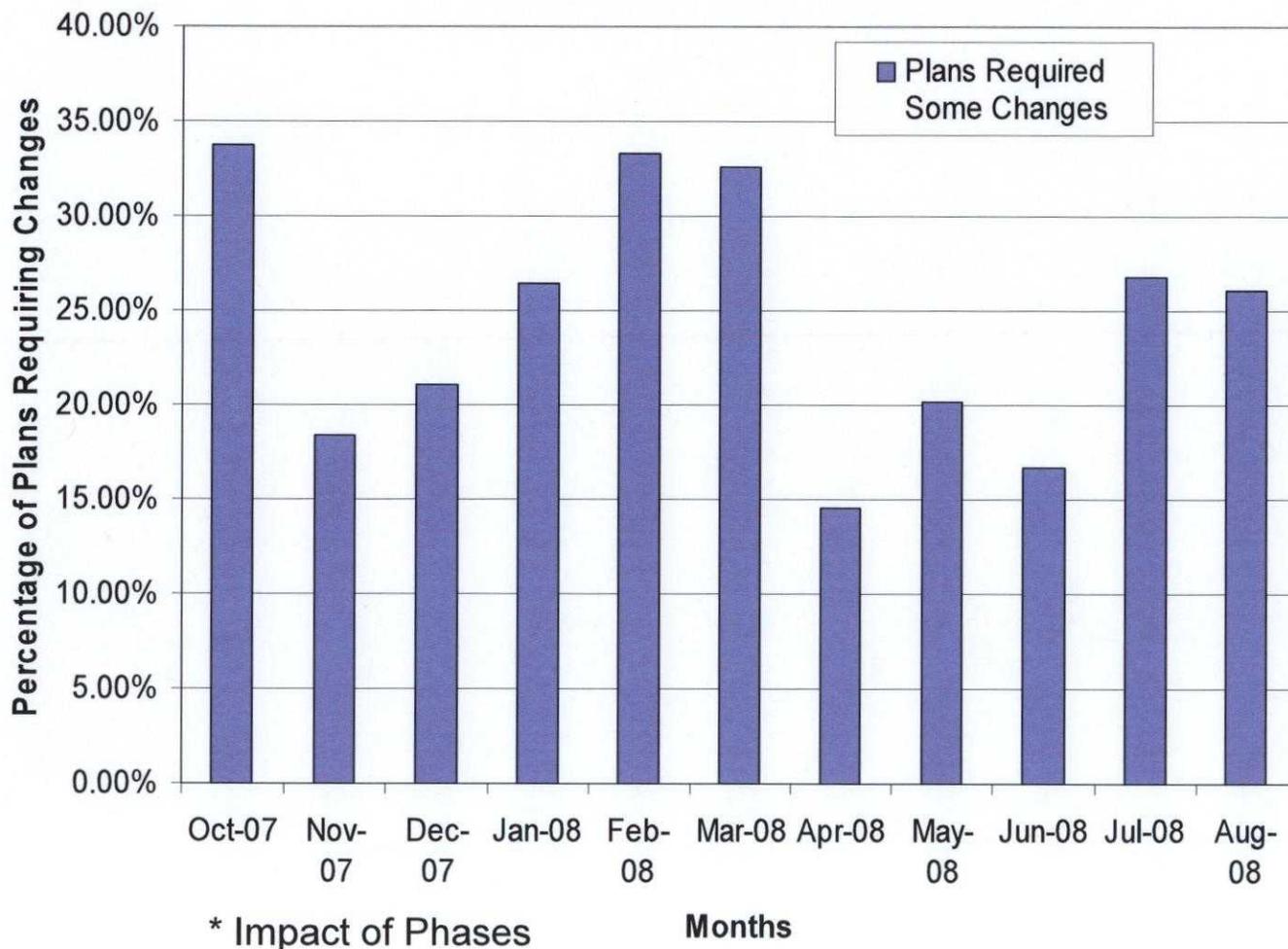
- #1. No discrepancies discovered during on-site validation.
- #2. Minor discrepancies noted and corrected during on-site validation.
- #3. Significant discrepancies noted which could not be resolved during on-site validation.

DSS, ODAA Metrics

Security Plan Reviews

Security Plan Review Questions and/or Comments, Errors and Corrections Noted

Plans Required Some Changes



Of the 1241 plans received from Oct 2007 – August 08

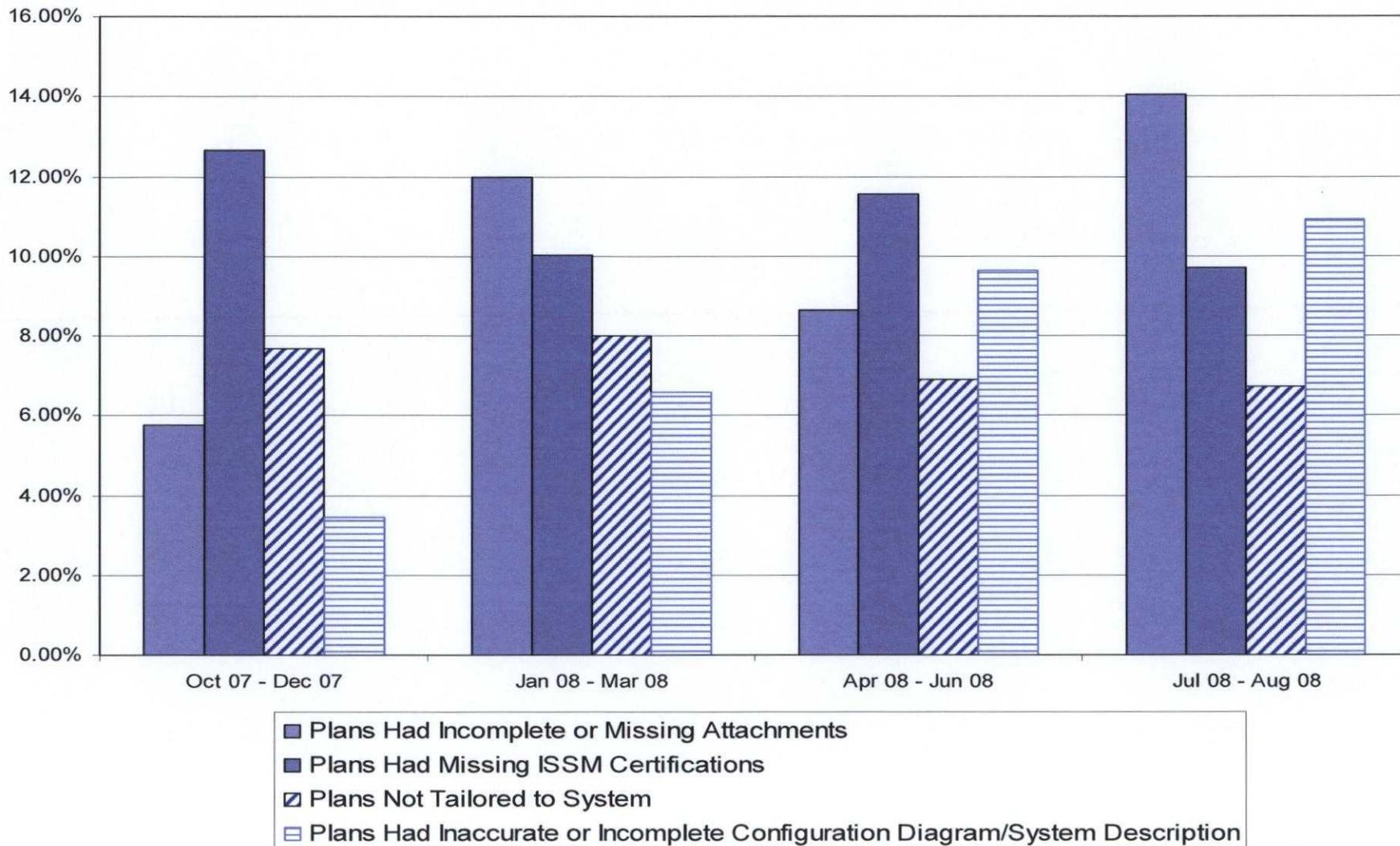
- On Average 24.5 % of all plans submitted required changes prior to the On-site Verification for ATO

For the August 08 26% of all plan (144 Plans) submitted required corrections from Industry

DSS < ODAA Metrics

Security Plan Reviews Common Errors

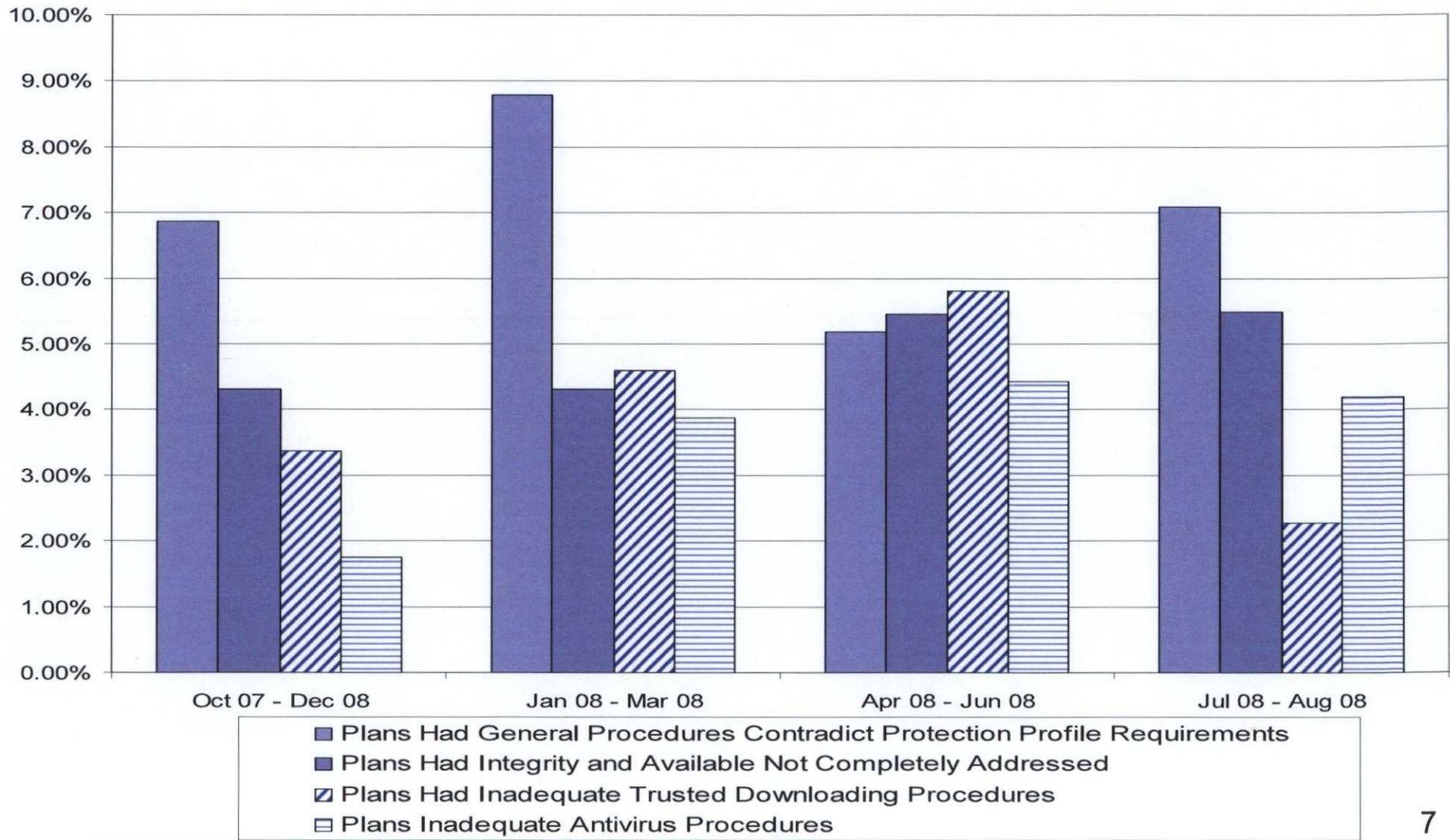
Part One



DSS, ODAA Metrics

Security Plan Reviews Common Errors

Part Two



Standards, Guidance, and Policy

Standardizing System Security Plans (Templates) Standards

Establishing Technical Standards in Conformance with DoD and other Federal Initiatives

Working with DOUSD(I) Policy on Industrial Security Letter (ISL) that will provide additional guidance for the DSS Accreditation Process and Technical Standards

Corporate/Traveling ISSM Pilot Project Completed (Future ISL to be Drafted)

Future Guidance and Policy

- Information System Security Manager Training and Certification Guidance**
- Radio Frequency Identification (RFID)**
- NISPOM Chapter 8 Information Assurance**

Industry Work Shops on Accreditation

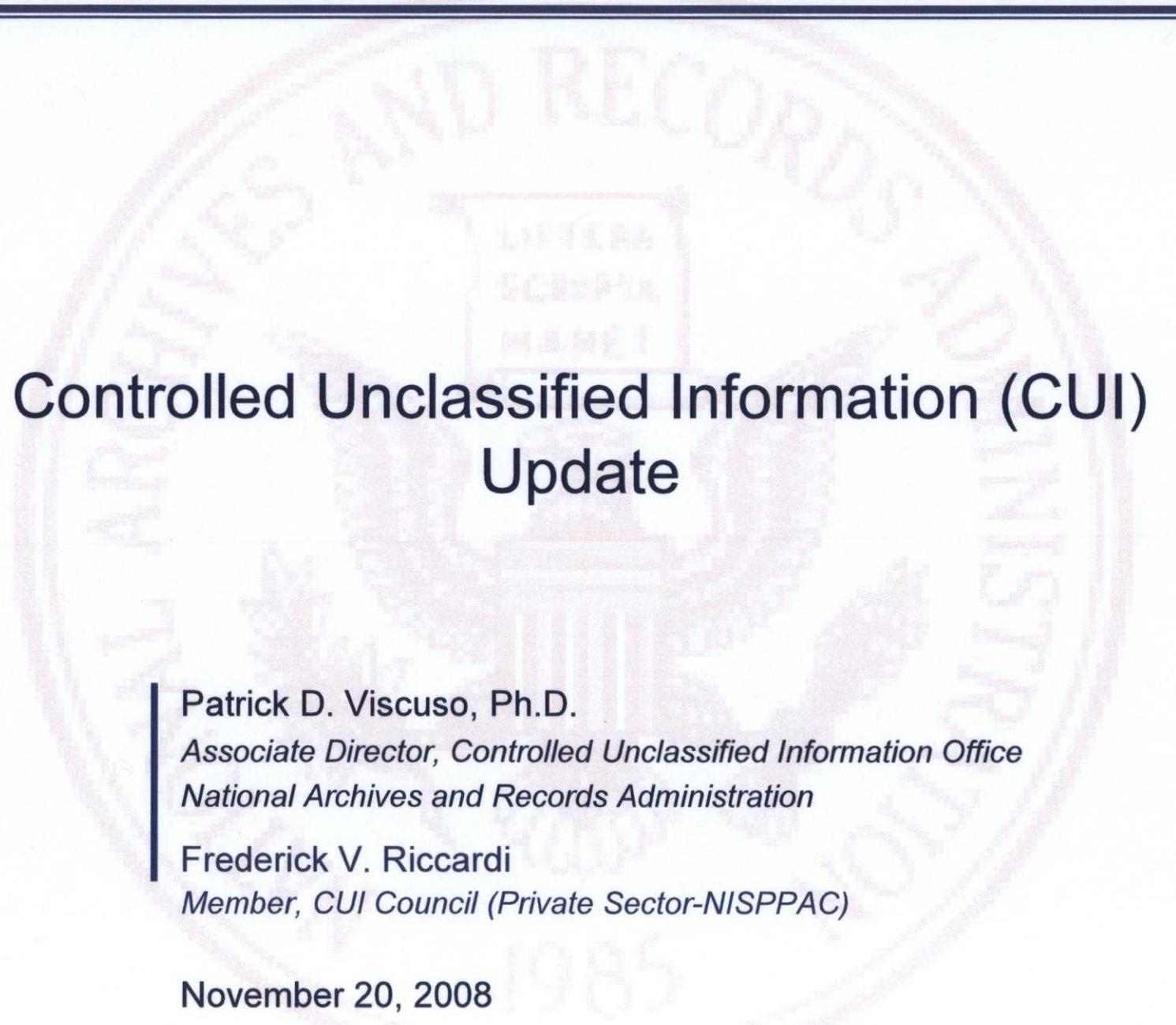
ODAA is working with industry through Work Shops that go over

- **ODAA Accreditation Process Guide**
- **System Security Templates**
- **DSS Technical Configuration Templates**
- **Operating Systems Implementation Guides**
- **Guidance on**
 - **Downgrading a Classified System**
 - **Preparing and submitting a SSP for submission to ODAA**
 - **Use of ODAA Tools**

Most Recent: Aerospace Industries Association (AIA) San Diego, CA. November 5, 2008

- **40+ Industry Information System Professionals Attended**
- **Positive Comments Received from Work Shop Survey**

Appendix 3
Controlled Unclassified Information Presentation



Controlled Unclassified Information (CUI) Update

Patrick D. Viscuso, Ph.D.

*Associate Director, Controlled Unclassified Information Office
National Archives and Records Administration*

Frederick V. Riccardi

Member, CUI Council (Private Sector-NISPPAC)

November 20, 2008



May 9th Presidential Memorandum

On May 9, 2008, the President released the Memorandum for the Heads of Executive Departments and Agencies on the *Designation and Sharing of Controlled Unclassified Information*.

The Memorandum:

- 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
- Establishes a corresponding new **CUI Framework** for designating, marking, safeguarding, and disseminating information designated as CUI; and
- Designates the **National Archives and Records Administration (NARA)** as the Executive Agent, to oversee and implement the new CUI Framework.

The purpose of the Framework is to standardize practices and thereby improve the sharing of information.



Actions since May 9, 2008

- On **May 21, 2008**, the Archivist of the United States established the CUI Office within NARA to oversee and manage the implementation of the new CUI Framework.
- The CUI Office and PM-ISE have partnered to brief Federal partners, Congress, and Open Government groups on the CUI Framework.
- On **June 30, 2008**, the Director of the CUI Office sent a letter out to Departments and Agencies that introduced the Executive Agent and tentative plans for implementation of the CUI Framework.
- On **July 9, 2008**, the PM-ISE activated the CUI Council, as a subcommittee of the Information Sharing Council (ISC) and requested department and agency designees.
- On **August 21, 2008**, the organizational meeting for the CUI Council was held at the National Archives Building in Washington, D.C. Currently, the CUI Council is scheduled to meet monthly.
- In **August 2008**, the CUI Office launched its website at www.archives.gov/CUI. The website will provide current information on the CUI Framework.



CUI Governance Structure

CUI Executive Agent

The Presidential Memorandum designates NARA as the CUI Executive Agent. On May 21, 2008, the Archivist of the United States established the CUI Office within NARA to oversee and manage the implementation of the new CUI Framework.

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. The PM-ISE issued guidance establishing the CUI Council on July 9, 2008. The first CUI Council meeting was held on Aug. 21, 2008.

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. On June 30, 2008, the Director of the CUI Office sent a letter to Departments and Agencies with initial implementing guidance for CUI.



The CUI Council

The CUI Council will carry out the following functions as directed by the President:

- Serve as the primary advisor to the Executive Agent on issues pertaining to the CUI Framework
- Advise the Executive Agent in developing procedures, guidelines, and standards necessary to establish, implement, and maintain the CUI Framework;
- Ensure coordination among the depts. and agencies participating in the CUI Framework; and
- Resolve complaints and disputes among departments and agencies about proper designation or marking of CUI.

- Department of Commerce
- Department of Defense
- Director of National Intelligence (IC)
- Department of Energy
- Federal Bureau of Investigation
- Department of Health and Human Services
- Joint Staff
- Department of Homeland Security
- Department of Interior
- Department of Justice

- Office of Management and Budget
- Program Manager for the Information Sharing Environment
- Department of State
- Department of Transportation
- Department of Treasury
- Environmental Protection Agency
- Nuclear Regulatory Commission
- Two SLT members and two private sector members on the CUI Council.



Two Private Sector Representatives

Frederick V. Riccardi

- Senior Executive Director
Security and Mission Assurance
ManTech International Corporation
- National Defense Industrial Association – Chairman Industrial Security Committee
2008-2009
- Nominated by the NISPPAC membership for representation on CUI Council

Turner D. Madden, Esquire

- Madden & Patton, LLC
- Vice Chairman of the Partnership for Critical Infrastructure and the Co-Chairman of the Commercial Sector Coordinating Council for the U.S. Department of Homeland Security
 - Elected by the private sector 16 sub-sector chairs of the Commercial Sector
- Nominated by the industry members of the Critical Infrastructure Partnership Advisory Council (CIPAC) for representation on CUI Council

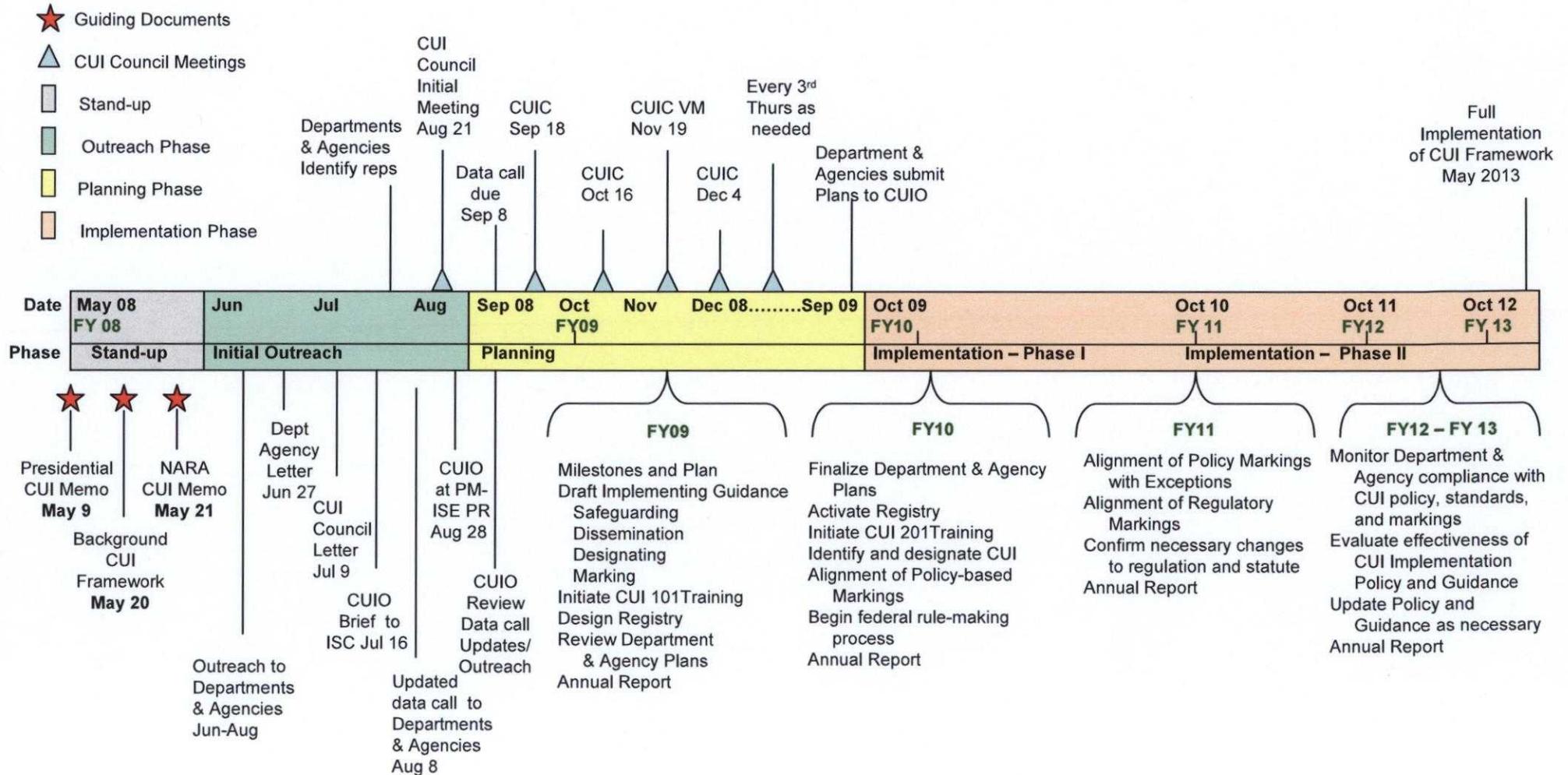


Tentative FY09 Actions

- **Development of Centralized Implementation Plan**
 - Set priorities for implementation
 - Establish milestones for alignment to CUI Framework
 - Establish training schedule
- **Development of Implementation Policies**
 - Define Safeguarding Standards
 - Define Department and Agency CUI Dissemination Policies
 - Develop detailed guidance on CUI life cycle, portion marking, and application of CUI Framework to archived information
 - Establish Centralized CUI Training (“CUI 101”)
- **Begin the development of Department- and Agency-specific Implementation Plans**
 - Establish Department- and Agency-specific CUI Training (“CUI 201”)

Our intent is to provide departments and agencies the information that they need to plan for implementation and align this implementation with their normal budget cycles.

CUI Framework Implementation Timeline Overview





Guiding Principles

Sharing	CUI will be shared as broadly as possible.
Protection	CUI will be appropriately protected.
Rationalization	CUI policy will be developed with deliberate consideration to managing risk and information sharing.
Flexibility	CUI policy development will respond to changes through centralized management and distributed execution.
Inclusiveness	CUI policy will address the needs of all ISE partners, both users and producers of information, taking into account all media types.
Standardization	CUI policy will be standardized so all participants are governed by uniform definitions and practices.
Transparency	CUI policy will be developed with input by State, local, tribal, and private sector entities and comment by the public.



Contact Information

Controlled Unclassified Information Office
National Archives and Records Administration
700 Pennsylvania Avenue, N.W., Room 100
Washington, DC 20408-0001

(202) 357-5250 (voice)

(202) 357-5907 (fax)

cui@nara.gov (email)

www.archives.gov/CUI (website)

Appendix 4
Joint Security and Suitability Process Reform Team Presentation

The logo for the Joint Reform Team, featuring a stylized American flag design with stars and stripes in shades of blue and white. The text "Joint Reform Team" is overlaid in white.

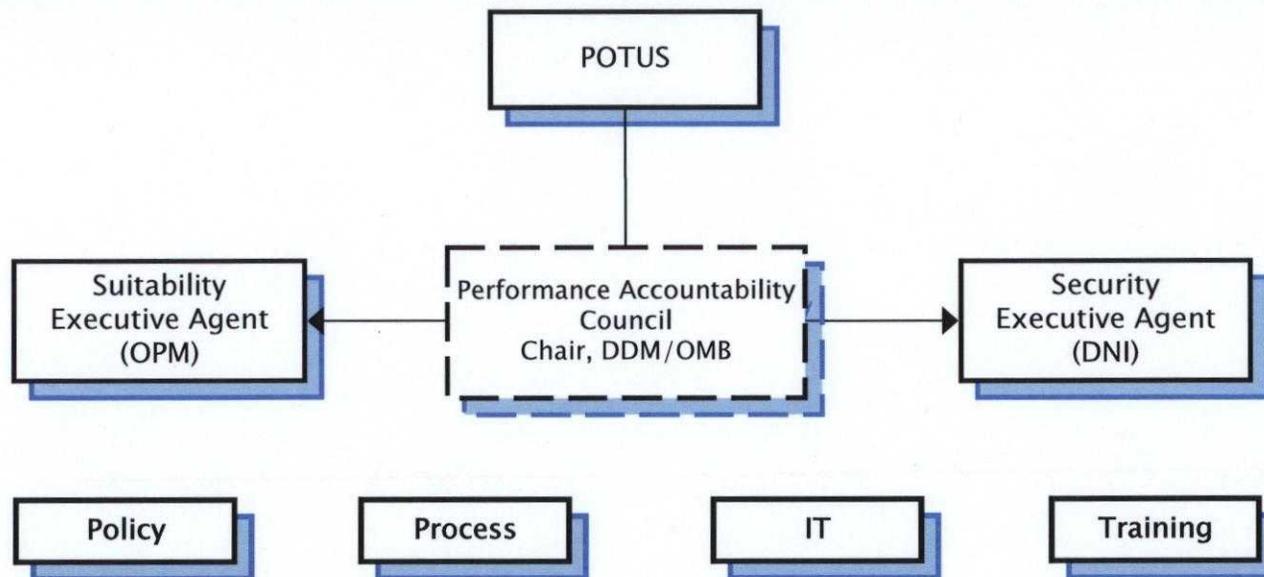
Joint
Reform
Team

Joint Suitability and Security Clearance Reform Team

NISPPAC

November 20, 2008

GOVERNANCE



Performance Accountability Council

- **Accountable to President for achieving goals of reform**
- **Ensures alignment of security and suitability investigative and adjudicative processes**
- **Holds agencies accountable for implementation**
- **Establishes requirements for Enterprise Information Technology**
- **Monitors performance to goals**

EXECUTIVE ORDER 13467

- **Mandates Alignment of Suitability and Security Clearance Processes**
 - Aligns processes related to federal employment, contractor fitness, and eligibility for access to classified national security
- **Establishes Performance Accountability Council**
 - Senior inter-agency forum with authority to ensure alignment and drive implementation of the reform effort
- **Designates D/OPM Suitability Executive Agent**
 - OPM will continue in its statutory and regulatory role as the Federal government's authority over suitability matters
- **Designates DNI Security Executive Agent**
 - DNI's role consolidates security clearance responsibilities previously dispersed across the security community
 - Assigns IRTPA Responsibilities to Security Executive Agent
- **Clarifies Continuous Evaluation policy**

Appendix 5
Combined Industry Presentation

A faded, semi-transparent image of the United States flag is positioned in the background, centered behind the text. The flag's stars and stripes are visible but light in color, serving as a decorative backdrop.

NISPPAC Industry Update

November 20, 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
Scott Conway	Northrop Grumman	2012
Marshall Sanders	SRA	2012

* Term expires

Industry Members/MOU



AIA

Scott Conway

ASIS

Ed Halibozek

CSSWG

Sam Kirton

ISWG

Mitch Lawrence

ITAA

Richard "Lee" Engel

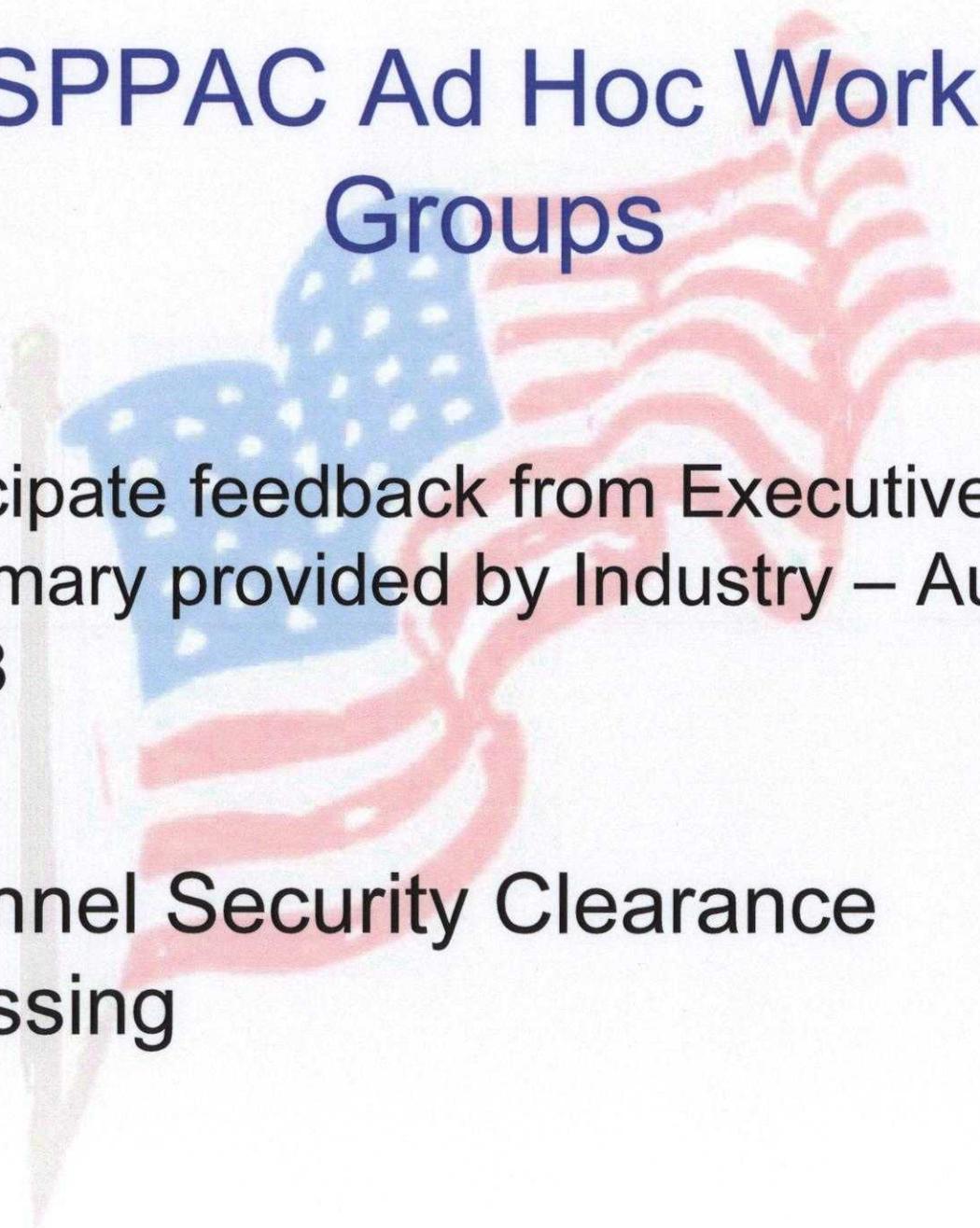
NCMS

Paulette Hamblin

NDIA

Fred Riccardi

NISPPAC Ad Hoc Working Groups

A large, semi-transparent watermark of the United States flag is positioned in the background of the slide, centered behind the main text.

- ODAA
 - Anticipate feedback from Executive summary provided by Industry – August 2008
- Personnel Security Clearance Processing

NISPPAC Reports

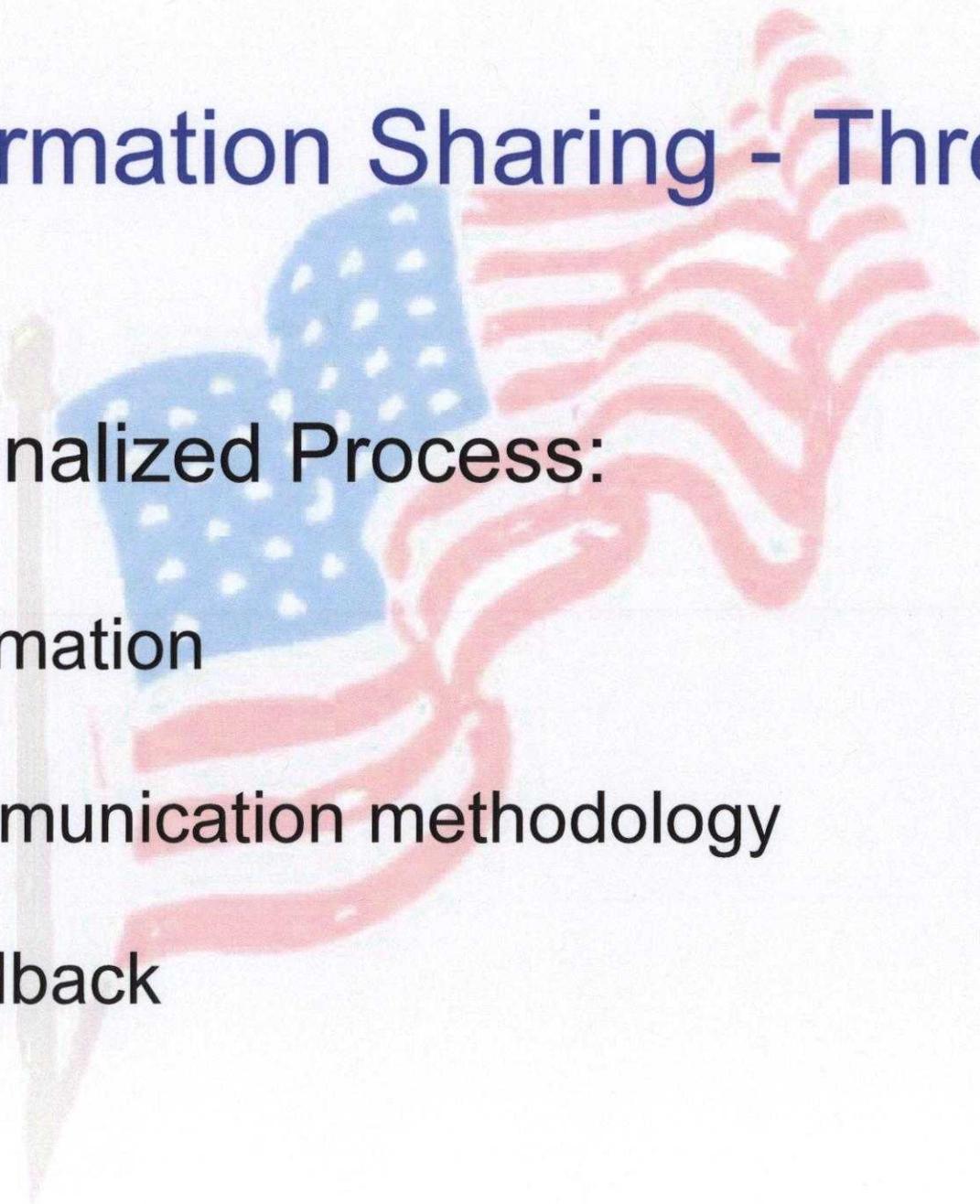
(Industry concerns presented 15 May 2008)

- Information Sharing - Threat
- Controlled Unclassified Information
- Foreign Ownership Control & Influence (FOCI)
- Personnel Security Clearance Processing

NISPPAC Reports

- Impact and implementation process for requirements delineated within National Defense Authorization Act:
 - **SEC. 845. DEFENSE INDUSTRIAL SECURITY.**
 - (a) *Defense Industrial Security-*
 - (1) *IN GENERAL- Subchapter I of chapter 21 of title 10, United States Code, is amended by adding at the end the following new section:*
 - **Sec. 438. Defense industrial security**

Information Sharing - Threat

A faded, semi-transparent image of the United States flag is positioned in the background, centered behind the main text. The flag's stars and stripes are clearly visible but have a low opacity, serving as a decorative backdrop.

Institutionalized Process:

- Information
- Communication methodology
- Feedback

Controlled Unclassified Information

A large, faded graphic of the United States flag is positioned in the background, behind the title and list. The flag is tilted and appears to be waving, with the stars and stripes clearly visible but semi-transparent.

- 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

A faded, semi-transparent image of the United States flag is positioned in the background, centered behind the title and list. The flag's stars and stripes are clearly visible but have a low opacity, serving as a decorative backdrop.

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

Appendix 6
NISPPAC Bylaws

THE U.S. NATIONAL ARCHIVES & RECORDS ADMINISTRATION

National Industrial Program Policy Advisory
Committee (NISPPAC)

Bylaws (As amended in May 2007)

Article 1. Purpose

Article 2. Authority

Article 3. Membership

- A. Primary Membership
- B. Nominations
- C. Appointment
- D. Term of Membership
- E. Clearance
- F. Compensation
- G. Observers

Article 4. Meetings

- A. General
- B. Quorum
- C. Open Meetings
- D. Closed Meetings
- E. Agenda
- F. Conduct of Meetings
- G. Minutes
- H. Public Comment

Article 5. Voting

- A. Voting Eligibility
- B. Voting Procedures
- C. Reporting of Votes

Article 6. Committee Officers and Responsibilities

- A. Chairman
- B. Designated Federal Officer
- C. Executive Secretary

D. Committee Staff
Article 7. Documents

Article 8. Committee Expenses and Cost Accounting

Article 9. Amendment of Charter and Bylaws

Article 1. Purpose.

The purposes of the NISPPAC are to advise the Chairman on all matters concerning the policies of the National Industrial Security Program (NISP), including recommended changes to those policies; and to serve as a forum to discuss policy issues in dispute.

Article 2. Authority.

Executive Order 12829, "National Industrial Security Program," as amended, establishes the NISPPAC as an advisory committee acting through the Director, Information Security Oversight Office, who serves as the Chairman of the Committee, and who is responsible for implementing and monitoring the NISP, developing directives implementing E.O. 12829, as amended, reviewing agency implementing regulations, and overseeing agency and industry compliance. The framework for the Committee's membership, operations, and administration is set for in the Order. The NISPPAC is subject to the Federal Advisory Committee Act (FACA), the Freedom of Information Act (FOIA), and the Government in the Sunshine Act (GISA).

Article 3. Membership

A. Primary Membership.

Executive Order 12829, as amended, conveys to the Chairman of the NISPPAC the authority to appoint all members. The Committee's total membership of 24 voting members shall be comprised of 16 representatives from executive branch agencies (including the Chairman) and eight representatives from industry. The Chairman shall also appoint the Staff Director of the Security Policy Board as a member of the NISPPAC, but that representative shall have non-voting status, and such membership shall not affect other numerical requirements in these bylaws including quorums and votes. At least one industry member shall be representative of small business concerns, and at least one shall be representative of Department of Energy/Nuclear Regulatory Commission contractors or licensees. An industry member serves as a representative of industry, not as a representative of his or her employing company or

corporation. For purposes of federal ethics law, the non-federal members of the NISPPAC have been determined to be "representatives" rather than "special government employees."

- B. **Nominations.** The Chairman will solicit and accept nominations for Committee membership: (1) for representatives of the respective agencies, from the agency head; and (2) for representatives of industry, from the governing boards of professional, trade and other organizations whose membership is substantially comprised of employees of business concerns involved with classified contracts, licenses, or grants. Although an industry representative does not represent his or her employing company, the Chairman will solicit the approval of the Chief Executive Officer of that company to allow the nominated individual to serve on the NISPPAC.
- C. **Appointment.** The Chairman shall appoint all Committee members. Membership includes the responsibility of the member to attend NISPPAC meetings personally as often as possible. However, a member may select one or more alternates who may, with the advance written approval of the Chairman, serve for the member at meetings of the Committee when the member is unable to attend. An alternate so selected shall have all rights and authorities of the appointed member. When a member selects a previously approved alternate to attend any Committee meeting, the Chairman will be notified as soon as possible in advance of that meetings.
- D. **Term of Membership.** The term of membership for Government representatives shall be three years, with the terms of initial members ending on September 30, 1996. When renominated by the head of his or her agency, a representative of a Government agency may be selected to serve successive three-year terms. Commencing in fiscal year 1998, the term of membership for industry representatives shall be four years. The terms of industry representatives shall be staggered so that the terms of two industry representatives are completed at the end of each fiscal year. The terms of the industry representatives serving in fiscal year 1998 shall be adjusted so that they permit the establishment of staggered four-year terms. Industry representatives may not serve successive terms. When a Government or industry member is unable to serve his or her full term, or when, in view of the Chairman, a member has failed to meet his or her commitment to the NISPPAC, a replacement shall be selected in the same manner to complete the unexpired portion of that member's term. Each representative's term of membership shall be conveyed by letter from the Chairman.

- E. **Clearance.** Members and alternates must possess a current security clearance at the Secret level or above, and clearance certification shall be provided to the Chairman by the employing agency or company.
- F. **Compensation.** Federal Government employees serving on the Committee are not eligible for any form of compensation. The Government will pay travel and per diem for industry members at a rate equivalent to that allowable to Federal Government employees. Industry members will submit travel vouchers to the Executive Secretary within 15 days after each meeting.
- G. **Observers.** Any NISP participating organization (industry or Government) may send observers to attend meetings of the Committee. Such observers will have no voting authority and will be subject to the same restrictions on oral presentation, as would any member of the public. As determined by the Chairman, observers may be permitted to attend closed meetings. Industry observers will not receive travel or per diem compensation.

Article 4. Meetings

- A. **General.** The NISPPAC will meet at least twice each calendar year as called by the Chairman. As the situation permits, the Executive Secretary will canvass the membership in advance of the scheduling of meetings in order to facilitate attendance by the largest number of members. The Chairman will also call a meeting when so requested by a majority of the 16 Government members, and a majority of the eight industry members. The Chairman will set the time and place for meetings and will publish notice in the Federal Register at least five calendar days prior to each meeting.
- B. **Quorum.** NISPPAC meetings will be held only when a quorum is present. For this purpose, a quorum is defined as a simple majority of the 16 Government members or alternates and a simple majority of the eight industry members or alternates.
- C. **Open Meetings.** Unless otherwise determined in advance, all meetings of the NISPPAC will be open to the public. Once an open meeting has begun, it shall not be closed for any reason. All matters brought before or presented to the Committee during the conduct of an open meeting, including the minutes of the proceedings of an open meeting, shall be available to the public for review or copying.
- D. **Closed Meetings.** Meetings of the NISPPAC will be closed only in limited circumstances and in accordance with applicable law. When the Chairman has determined in advance that discussions during a Committee meeting will involve matters about which public disclosure would be harmful to the interests of the

Government, industry, or others, an advance notice of a closed meeting, citing the applicable exemptions of the GISA, will be published in the Federal Register. The notice may announce the closing of all or just part of a meeting. If, during the course of an open meeting, matters inappropriate for public disclosure arise during discussions, the Chairman will order such discussion to cease, and shall schedule it for closed session. Notices of closed meetings will be published in the Federal Register at least 15 calendar days in advance.

- E. **Agenda.** The Chairman shall approve the agenda for all meetings. The Chairman will distribute the agenda to the members prior to each meeting and will publish an outline of the agenda with the notice of the meeting in the Federal Register. Items for the agenda may be submitted to the Chairman by any regular member or alternate member of the Committee. Items may also be suggested by non-members, including members of the public. To the extent possible, all written recommendations for NISP or NISPOM policy changes, whether or not they are placed on the agenda, will be provided to the Committee membership prior to the start of any scheduled meeting. The Chairman will advise the party making the recommendation what action was taken or is pending as a result of the recommendation.
- F. **Conduct of Meetings.** Meetings will be called to order by the Chairman, following which the Chairman or Executive Secretary will call the roll or otherwise take attendance and read or reference the minutes of the previous meeting. At that time the minutes will be corrected, as necessary, and approved by the membership and certified by the Chairman. The Chairman will then make announcements, ask for reports from subgroups or individual members (as previously arranged), open discussion of unfinished business, introduce new business, and invite membership comment on that business. Public oral comment may be invited at any time during the meeting, but most likely at the meeting's end, unless the meeting notice advised that written comment was to be accepted in lieu of oral comment. Upon completion of the Committee's business, as agreed upon by the members present, the meeting will be adjourned by the Chairman.
- G. **Minutes.** The Committee's Executive Secretary shall prepare minutes of each meeting and will distribute copies to each Committee member. Minutes of open meetings will be available to the public upon request. The minutes will include a record of the persons present (including the names of committee members, names of staff, and the names of members of the public from whom written or oral presentations were made) and a

complete and accurate description of the matters discussed and conclusions reached, and copies of all reports received, issued or approved by the Committee.

- H. **Public Comment.** Members of the public may attend any meeting or portion of a meetings that is not closed to the public, and may at the determination of the Chairman, offer public comment during a meeting. The meeting announcement published in the Federal Register will note that oral comment from the public is excluded and will invite written comment as an alternative. Members of the public may submit written statements to the Committee at any time.

Article 5. Voting.

When a decision or recommendation of the NISPPAC is required, the Chairman shall request a motion for a vote. Any member or approved alternate of the NISPPAC, including the Chairman, may make a motion for a vote. No second after a proper motion shall be required to bring any issue to a vote.

- A. **Voting Eligibility.** Only the Chairman and the appointed members, or their designated alternates may vote on an issue before the Committee.
- B. **Voting Procedures.** Votes shall ordinarily be taken and tabulated by a show of hands. Upon a motion approved by two-thirds of the members present, a vote by secret ballot may be taken. However, each ballot must indicate whether the vote is from and industry or Government representative.
- C. **Reporting of Votes.** The Chairman will report to the President, Executive Agent of the NISP, or other Government officials the results of Committee voting that pertain to the responsibilities of that official. In reporting or using the results of NISPPAC voting, the following terms shall apply: (1) Unanimous Decision. Results when every voting member, except abstentions, is in favor of or opposed to a particular motion; (2) Government and Industry Consensus. Results when two-thirds of those voting, including two-thirds of all Government members and two-thirds of all industry members, are in favor of or are opposed to a particular motion; (3) General Consensus. Results when two-thirds of the total vote casted are in favor of or are opposed to a particular motion; (4) Government and Industry Majority. Results when the majority of the votes casted, including a majority of all Government members and a majority of all industry members, are in favor of or are opposed to a particular motion; (5) General Majority. Results when a majority of the total votes cast are in favor of or are opposed to a particular motion.

Article 6. Committee Officers and Responsibilities

- A. **Chairman.** As established by Executive Order 12829, as amended, the Committee Chairman is the Director of the Information Security Oversight Office. The Chairman will: (1) call meetings of the full Committee; (2) set meeting agenda; (3) determine quorum; (4) open, preside over and adjourn meetings; and (5) certify meeting minutes. The Chairman also serves as the Committee's Designated Federal Officer, a position required by the FACA.
- B. **Designated Federal Officer.** The FACA requires each advisory committee to have a Designated Federal Officer (DFO) and alternate, one of whom must be present for all meetings. The Director and Associate Director, Information Security Oversight Office, are, respectively, the Designated Federal Officer and alternate for the NISPPAC. Any meeting held without the DFO or alternate present will be considered as a subgroup or working group meeting.
- C. **Executive Secretary.** The Executive Secretary shall be a member of the staff of the Information Security Oversight Office and shall be responsible for: (1) notifying members of the time and place for each meeting; (2) recording the proceedings of all meetings, including subgroups or working group activities that are presented to the full Committee; (3) maintaining the roll; (4) preparing the minutes of all meetings of the full Committee, including subgroups and working group activities that are presented to the full Committee; including subgroup and working group activities that are presented to the full Committee; (5) attending to official correspondence; (6) maintaining official Committee records and filing all papers and submissions to the Committee, including those items generated by subgroups and working groups; (7) acting as Committee Treasurer to collect, validate and pay all vouchers for preapproved expenditures presented to the Committee; (8) preparing a yearly financial report; and (9) preparing and filing the annual Committee report as required by the FACA.
- D. **Committee Staff.** The staff of the Information Security Oversight Office shall serve as the NISPPAC staff on an as needed basis, and shall provide all services normally performed by such staff, including assistance in the fulfilling of the functions of the Executive Secretary.

Article 7. Documents.

Documents presented to the Committee by any method at any time, including those distributed during the course of a meeting, are part of the official Committee files, and become agency records within the meaning of the FOIA, and are subject to the provisions of that Act. Documents originating with agencies of the Federal Government shall remain under the primary control of such agencies and will be on loan to the Committee. Any FOIA request for access to documents originating with any agency shall be referred to that agency. Documents originating with industry that have been submitted to the NISPPAC during the course of its official business shall also be subject to request for access under the FOIA. Proprietary information that may be contained within such documents should be clearly identified at the time of submission.

Article 8. Committee Expenses and Cost Accounting.

Committee expenses including travel and per diem of non-Government members will be borne by the Information Security Oversight Office to the extent of appropriated funds available for these expenditures. Cost accounting will be performed by the Committee's Executive Secretary. Expenditures by the Committee or any subgroup or working group must be approved in advance by the Chairman or the Executive Secretary.

Article 9. Amendment of Charter and Bylaws.

Amendments to the Charter and Bylaws of the Committee must conform to the requirements of the FACA and Executive Order 12829, as amended, and be agreed by two-thirds of the 16 Government members or alternates and two-thirds of the eight industry members or alternates. Confirmed receipt of notification to all Committee members must be completed before any vote is taken to amend either the Charter or bylaws.

Page URL: <http://www.archives.gov/isoo/oversight-groups/nisppac/bylaws.html>

The U.S. National Archives and Records Administration

8601 Adelphi Road, College Park, MD 20740-6001 • Telephone: 1-86-NARA-NARA or 1-866-272-6272