NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

SUMMARY MINUTES OF THE MEETING

The NISPPAC held its 32nd meeting on Tuesday, April 7, 2009, at 1:00 p.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 were finalized and certified on July 16, 2009.

The following members/observers were present:

- William J. Bosanko (Chair)
- Daniel McGarvey (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)
- Gina Otto (Office of the Director of National Intelligence)
- Richard Donovan (Department of Energy)
- John Young (Department of Homeland Security)
- Anna Harrison (Department of Justice)
- Dennis Hanratty (National Security Agency)
- Sean Carney (Department of the Navy)
- Michael Hawk (Department of State)
- Richard Lee Engel (Industry)
- Sheri Escobar (Industry)
- Douglas Hudson (Industry)
- Timothy McQuiggan (Industry)
- Vincent Jarvie (Industry)
- Scott Conway (Industry)
- Marshall Sanders (Industry)
- Darlene Fenton (Nuclear Regulatory Commission)
- Drew Winneberger (Defense Security Service)
- Steven Peyton (National Aeronautics & Space Administration)
- Merton Miller (Office of Personnel Management) – Observer

I. Welcome, Introductions, and Administrative Matters

William J. Bosanko, Director, ISOO and NISPPAC Chair, greeted the membership and attendees and introduced two new Government members to the NISPPAC: Drew Winneberger, Acting Director, Industrial Security Policy and Programs, Defense Security Service (DSS), and, Darlene Fenton, Senior Facility Security Specialist, Division of Facilities and Security, Nuclear Regulatory Commission (NRC).

The Chair informed the NISPPAC that the minutes from the November 20, 2008, meeting had been finalized and certified by e-mail on March 20, 2009, and are posted at http://www.archives.gov/isoo/oversight-groups/nisppac/committee.html on the ISOO website.

The Chair then spoke to the future of the NISPPAC. Specifically, the Chair informed the NISPPAC membership that there would now be three meetings per year, as opposed to two,

and noted that upcoming NISPPAC meetings are tentatively scheduled for the months of July and October 2009. The Chair mentioned the Obama Administration's focus on increased openness within the Government and noted possible changes with regard to the Federal Advisory Committee Act (FACA), for example, the introduction of meeting transcripts. The Chair further stated that he would like to see more discussion within the NISPPAC membership. Accordingly, the Chair recalled that the NISPPAC was created for the specific purpose of discussing changes to policy (specifically, Executive Order 12829, as amended, "National Industrial Security Program," (NISP) (the Order) and issuances (to include the "National Industrial Security Program Operating Manual" (NISPOM)) that fall beneath it. Additionally, so as to have more fulsome Executive Branch representation and discussion at the NISPPAC meetings, the Chair stated that he expected more active participation from the NISPOM Signatories, to include meetings between regular NISPPAC meetings.

II. Old Business

After leading the discussion on the first action item from the November 20, 2008, NISPPAC meeting, the Chair requested that Greg Pannoni, Associate Director, Operations and Industrial Security, ISOO, lead the discussion reviewing the remainder of the action items.

ACTION: 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.

The Chair expressed his appreciation for the input that was received and noted that responses addressed a wide-spectrum of issues. The Chair noted that the top concerns were related to personnel security clearances (PCLs), foreign ownership, control, or influence (FOCI), information technology security and threats, and controlled unclassified information (CUI). After noting that issues surrounding PCLs and FOCI will continue to be addressed in future NISPPAC meetings and meetings of its working groups, the Chair noted that the other concerns will be elevated in order to work on them.

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.

Mr. Pannoni stated that the FOCI working group met and that he would be addressing this action item through the report on this topic.

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 PAC.

Mr. Pannoni stated that this action item would be addressed through the report of the PCL Working Group from Deborah Smith, Office of Personnel Management (OPM) and Vera Denison (DSS).

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.

Mr. Pannoni stated that this action item would be addressed through the metrics update report from the Office of the Designated Approving Authority (ODAA) by David Cole (DSS).

ACTION: 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.

Mr. Pannoni stated that this action item would be addressed through the metrics update report by Mr. Cole.

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.

Mr. Pannoni stated that this action item would be addressed under "New Business." Mr. Pannoni informed that the changes to the NISPPAC Bylaws were primarily generated due to FACA requirements.

III. Working Group Updates

Before commencing with the working group updates, the Chair expressed his appreciation for the contributions of all the working group members.

A) PCL Working Group Report

A report on the working group's progress was provided by Ms. Smith, Ms. Denison, and Mr. Mansfield.[1]

Ms. Smith reported on end-to-end performance metrics, which include the initiation, investigation, and adjudication timeframes. Ms. Smith stated that the metrics presented were captured by the Personnel Investigation Processing System and include clearance decisions made during the first quarter of fiscal year (FY) 2009.

Ms. Smith noted the timeliness for all initial investigations for Top Secret, Secret, and Confidential clearances and periodic reinvestigations. Her report captured metrics on the average cycle time, in calendar days, which include the initiation, investigation, and adjudication timeframes, and average timeliness trends for the fastest 90 percent of clearances granted. Ms. Smith noted that the reported timeframe starts when the subject certifies the SF-86, "Questionnaire for National Security Positions," to the date that an adjudication decision is made. With regard to Industry's average end-to-end timeliness for

[1] Reference Appendix 1 for Ms. Smith's presentation. Reference Appendix 2 for Ms. Denison's presentation. Reference Appendix 3 for Mr. Mansfield's presentation.

the first 90 percent of initial clearances, Ms. Smith noted that the reported range for the first quarter of FY 2009 was 92–97 days and thus, represented a significant improvement.

Ms. Smith explained that OPM now captures metrics from the date that a case is received to the date the case is mailed "out the door."[2] Ms. Smith noted that when investigations are transmitted electronically, the date that is used to stop the investigation time is the date the customer agency receives the case file. Following the review of the captured metrics, Ms. Smith reported that the initiation time has improved and stated that it will continue to improve with the introduction of electronic fingerprints. In short, Ms. Smith noted that the automation initiatives that are underway will improve overall timeliness.

Ms. Smith reported that the prior investigative case backlog has been eliminated. Further, Ms. Smith stated that the investigations program has been working very closely with the customer agencies to implement those automation initiatives that will accelerate the overall process. Ms. Smith then yielded to Ms. Denison.

Ms. Denison reported that on January 17, 2009, the Department of Defense (DOD) implemented required agency use block fields to enable submission of the July 2008, version of the SF-86 for Industry users. She also reported that on January 16, 2009, DSS posted guidance with changes in completing Requests for Investigations on the Joint Personnel Adjudication System website. At this point, Ms. Smith noted that these two factors were "good news" for overall timeliness.

Ms. Denison presented metrics on the FY 2009 adjudication inventory at the Defense Industrial Security Clearance Office (DISCO), noting an overall reduction of nine percent from the beginning of the first quarter of FY 2009 to February 2009, and that the more significant decrease in FY08 was accomplished by mandatory overtime. DISCO terminated mandatory overtime in November 2008. She then noted an overall three percent reduction of Industry cases at OPM for the same timeframe. With regard to the first quarter of FY 2009 case rejection rates, Ms. Denison noted that DISCO's rejection rate was 8.1 percent and OPM's was five percent. Ms. Denison stated that OPM's rejections were typically due to fingerprint cards not being received within the required 30-day time period or faulty prints. She reviewed some of DISCO's top reasons for case rejection and noted that with the advent of the new SF-86, the percentage of errors should decrease. Finishing her report, Ms. Denison reminded the NISPPAC that the Intelligence Reform and Terrorism Prevention Act's goal is for requests for clearances to be within five percent of projections and noted that, currently, Industry's clearance submissions were 6.5 percent below overall Industry/DSS projections. She noted, however, that submissions typically trend downward during winter months and then peak during the spring and summer months. Ms. Denison then yielded to Mr. Mansfield.

Mr. Mansfield presented on the Secure Web Fingerprint Transmission System (SWFT). Mr. Mansfield noted the four major SWFT business functions: capture, upload, store, and release. While discussing these four functions, Mr. Mansfield noted the differences between the current pilot system and the new system.[3]

---

[2] Reference blue sections of bar graphs on slides 2–5 in Appendix 1.
[3] Reference the red bullet points on slide 2 in Appendix 3.

Mr. Mansfield then reviewed some of the new features, such as a secure web service, which would allow for system-to-system level transmission of data and the ability of account management. With regard to the configuration of the system, Mr. Mansfield reported that the primary system will be located at DSS headquarters, with a backup site in Monterey, California. He noted that there will be automated replication of data between the two sites so as to allow for minimal data loss should one of the systems fail. Finally, Mr. Mansfield discussed the transition of the Pilot system to the new system, noting that Phase 2 of SWFT will be activated in June and will be available in July.

At the conclusion of Mr. Mansfield's comments, Mr. Pannoni noted that due to the equipment needed for this technology, it may be difficult for smaller companies to find the technology "investment worthy." Following Mr. Pannoni's comment, Kathy Watson, Director, DSS, stated that it was her impression and DSS's position, that the larger Industry entities had indicated they would help smaller colleagues with the equipment. A discussion ensued, especially with regard to how smaller companies would leverage larger companies' equipment. After some discussion, it was determined that small companies would need DISCO's Security Office Identifier (SOI) and Submitting Office Number (SON). In response to a question from the audience, Ms. Watson stated that DSS would be happy to explore those areas where DSS's help is needed; however, she reaffirmed DSS's understanding that Industry would assume the role of assisting their smaller colleagues.

At the conclusion of the discussion, the Chair requested that the working group address, at the next working group meeting, Industry's current capabilities, as well as, any other options available, that would help address the issue of supporting small industrial facilities with the introduction of the new SWFT technology. Following this, the Chair noted that, at present, although the resources and capabilities to deploy the new technology did not exist everywhere, there is a need to find ways to make the tools work favorably for both Government and Industry.

ACTION: The Chair requested that the PCL Working Group address, at the next working group meeting, Industry's current capabilities, as well as, any other options available, that would help address the issue of supporting small industrial facilities with the introduction of the new SWFT technology.

B) Foreign Ownership, Control, or Influence (FOCI) Working Group Report
A report on the Working Group's progress was provided by Mr. Pannoni.[4]

Before proceeding with the working group update, the Chair recalled that the FOCI working group had been formed at the November 20, 2008, meeting of the NISPPAC. Prior to the working group's first meeting, potential items to be addressed and discussed were solicited from the NISPPAC membership. The Chair noted that the FOCI Working Group met on February 4, and March 4, 2009. The Chair then stated that though there may be a need for one more meeting of the working group, it has largely accomplished what it was initially formed to do. Last, the Chair expressed his appreciation for the efforts of all those involved and then yielded to Mr. Pannoni.

[4] Reference Appendix 4 for Mr. Pannoni's presentation.

Mr. Pannoni reported that FOCI has been, and will continue to be, a growth area in the industrial security field. He then stated that the purpose and focus of the FOCI working group was to evaluate the NISP FOCI process and develop recommendations for improvement.

Paraphrasing the NISPOM, Mr. Pannoni addressed the question as to when a contractor is considered under FOCI: 1) when a foreign interest has the power that may result in unauthorized access to classified information, and 2) when a foreign interest has the power that may adversely affect the performance of classified contracts.

With regard to the focus of the working group, Mr. Pannoni stated the group sought to provide recommendations to the unique reporting requirements pertaining to FOCI, especially when an update is required due to a material or significant change. Mr. Pannoni first discussed the development of a Material Change Matrix, which, he informed had already been in the development phase within DOD. Mr. Pannoni noted that the Matrix was developed to assist in determining what constitutes a material change. He then reported that the Matrix is under review by DSS and that any changes would come before the NISPPAC for further review.

Mr. Pannoni noted that since the NISPOM provides minimal guidance on the issue of National Interest Determinations (NIDs), the working group drafted a change to the implementing directive for E.O. 12829, as amended, 32 C.F.R. Part 2004, in order to provide greater clarity in terms of required actions. As the working group members had already provided input on the proposed draft, Mr. Pannoni requested that the NISPPAC provide formal responses to the draft within 30 days. The Chair concurred and then informed the group that the proposed change to the Directive would subsequently proceed through the Federal rule-making process.

The third recommendation that Mr. Pannoni reported was that the working group decided that there needed to be a revision in the language of the NISPOM pertinent to NIDs and the definitive language—"shall not harm the national security…" The working group determined that such a proposition is often difficult to prove and believed that the language involving NIDs should be more along the lines of "…is consistent with the national security interests…" Mr. Pannoni stated that this was included in the draft Directive language and thus, likely needs to be reflected in an update to the NISPOM.

Mr. Pannoni stated that the working group also recommended the creation of a NID point of contact database, wherein agencies could refer to see where information should be forwarded. Mr. Pannoni informed the group that DSS had agreed to create and maintain the database.

With regard to e-FOCI, Mr. Pannoni reported that the Department of Energy (DOE) e-FOCI system that was demonstrated to the working group provided an efficient means for meeting the FOCI reporting requirements. He further stated that it was understood that DOD would be implementing e-FOCI on a "phased approach" and is planning to have all DSS field activities operational by September 30, 2009. Ms. Watson clarified that DSS is also planning to use the system to process all new facility security clearance requests and that on-line

training for the system is available. Ms. Watson further clarified that, temporarily, the Industrial Security Facilities Database will continue to exist in a separate venue.

Mr. Pannoni then raised the working group's concern regarding the use of the SF-328, "Certificate Pertaining to Foreign Interests." He advised that the concern is that data from the form is being used by Government agencies for purposes other than NISP FOCI determinations, particularly in connection with acquisition initiatives/efforts. Thus, such use is outside the purpose and authority of the form.

Closing the report, Mr. Pannoni recommended that the working group reconvene at least one more time.

Following Mr. Pannoni's remarks, Industry raised a point of clarification regarding the use of a corporate-wide SF-328 method for reporting FOCI information. Stephen Lewis, OUSD(I), advised that the working group had discussed this issue because of the concern that a corporate-wide submission of the SF-328 could lead to a situation where the Government was not receiving all of the information needed at the subsidiary level; thus, preventing the Government from acquiring the information it needs in order to determine how to mitigate for FOCI at all levels in the corporate structure. At present, a NISPOM change is being considered, though Mr. Lewis acknowledged that the solution might be a matter of providing better instructions to be used when preparing corporate-wide SF-328s. In response to Mr. Lewis' comments, Industry stated that the working group needs to address this due to the upcoming reporting changes. A discussion followed and Industry commented that there was an agreement that corporate roll-ups will still be allowed, although it is now understood that if a corporate roll-up includes a foreign-owned subsidiary, specific changes for the latter shall be reported. Industry further noted that a legal entity that is under the corporate Multiple Facility Organization would still be included in a corporate roll-up as the attachments are all the same. At the end of the discussion, Mr. Pannoni noted that Industry has agreed to provide a draft definition of "organization."

Following the discussion, the Chair noted that there will be at least one more working group meeting and that the need for subsequent meetings could be evaluated later, depending on progress in resolving the issues raised to date, etc.

ACTION: Members of the NISPPAC are to provide formal responses with regard to the proposed changes to the Directive within 30 days.

Industry will provide a draft definition of "organization" within 30 days.

Per the Chair, following the next meeting of the FOCI Working Group, the issues involving FOCI will be reevaluated at a later date.

IV. New Business

A) Amendments to Bylaws

The Chair asked that the NISPPAC members review the current bylaws in light of standard operating procedures, FACA requirements, as well as to address grammatical errors. The

Chair advised that the proposed amendments[5] to the bylaws have been sent to all NISPPAC members for their review and asked that they provide formal comments within 30 days. Finally, the Chair informed that a report on the subject will be provided at the next NISPPAC meeting and at that time, following Article 9 of the bylaws, a vote will be taken to amend the bylaws.

ACTION: The NISPPAC members are to review the proposed amendments to the bylaws and provide formal comments within 30 days. Following Article 9 of the bylaws, a vote to approve the proposed bylaws will occur at the next meeting of the NISPPAC.

B) Industrial Security Regulation (ISR) Replacement, Directive Type Memorandum (DTM), and NISPOM Revision Update
Mr. Lewis, Director, Industrial Security Policy, OUSD(I) Security Directorate, presented on this topic.

Mr. Lewis informed that there are currently three major policy issues being worked within OUSD(I). Mr. Lewis first addressed the issue that more guidance is needed for DOD activities and those non-DOD agencies that use the industrial security services of DOD. He noted that a FOCI directive-type memorandum has been drafted, which informs Government activities of their responsibilities with respect to FOCI. Mr. Lewis advised that issuance is expected very soon and that the directive-type memorandum will serve as the FOCI chapter of the ISR replacement.

Mr. Lewis mentioned that the ISR, which dates back to 1985, has been rewritten to reflect the NISP and all the changes that have occurred. Mr. Lewis noted that an extensive coordination process was achieved within the activities that fall under OUSD(I) and that the draft ISR will be sent to the military services and other DOD components for their comment. Mr. Lewis stated that due to the age of the ISR, many comments are expected, which will result in a comprehensive document.

Mr. Lewis stated that OUSD(I) is working on various NISPOM interpretations in collaboration with DSS. With regard to the topic of what constitutes a "material change" in FOCI, the FOCI working group matrix document had the key elements. Thus, Mr. Lewis reported that once the material change document is updated it will be issued as an Industrial Security Letter (ISL). Given that this ISL will be based on the output of the FOCI working group, Mr. Lewis stated the document would be shared with the NISPPAC FOCI Working Group before being finalized. Mr. Lewis reported that the document maintains the essence and spirit of the matrix and that the quantitative thresholds for "material change" have been retained.

With regard to the NISPOM rewrite, Mr. Lewis advised that the deadline for the initial draft is the beginning of May. Mr. Lewis stated that after the rewrite was revised internally, the final rewrite would be accomplished in consultation with the NISPPAC and ISOO. Mr. Lewis reported that there was a general agreement with the other NISPOM Signatories as to what areas required change.

[5] Reference Appendix 5 for the proposed changes to the bylaws.

The Chair followed Mr. Lewis' remarks stressing the need for not only policy updates at NISPPAC meetings, but actual discussion regarding policy.

C) ODAA Metrics Update; Information Systems Security Accreditation Guidance; March 2009 ISL; Standards for Reference and Guidance Used by ODAA to Establish Technical and/or Process Standards.

Mr. Cole, Deputy Director, Industrial Security Field Operations, DSS, presented on this topic.[6]

The Chair reported that at the prior meeting of the NISPPAC, the ODAA Working Group had been temporarily suspended in order to concentrate on the efforts of the FOCI Working Group. Further, this action was due to the upcoming issuance of an ISL from DSS, which was to address the issues that the working group had been working. Though the working group would not meet, the Chair noted that the ODAA would continue to provide a metrics update.

Mr. Cole noted that DSS now has a formal metrics gathering process and thus has sufficient data in order to identify trends and areas for improvement within the Certification and Accreditation process. Mr. Cole presented ODAA's metrics on the number of days it takes to process system security plan (SSP) submissions.[7]

Mr. Cole reported that the average number of days it takes to receive an Interim Authority to Operate after the receipt of a submission is 39 days, which is significantly below what it was a year ago. Mr. Cole advised that this was due to internal improvements and the standardization of many of the required processes. At this point, Industry inquired as to why, despite this long-term trend, the reported data seems to have inclined over the past six months (September 2008 – February 2009). Mr. Cole responded that the spikes in the data were a result of the convergence of the prior multi-phased accrediting approach to the single-phased approach, which includes plans being centrally received and then sent to regional offices. Mr. Cole also noted that the increase is due to the reaccredidation of the numerous master SSPs that were submitted. Mr. Cole stated that the plans are being worked and that he expects the numbers to level off as Industry begins to use the SSP templates designed by DSS. After some brief discussion on SSP submissions, Mr. Cole mentioned that within the next year, DSS will have a more comprehensive dataset from which to better analyze trends.

Mr. Cole then reported on the metrics for on-site verification, which is the on-site inspection in order to grant an Authority to Operate (ATO). Mr. Cole reported that the data regarding this aspect has remained relatively consistent for the past 12 months in that for 25 percent of the time, some level of modification was required before an ATO was granted. Of the 25 percent, only four percent of the cases had such significant discrepancies that they could not be resolved during the on-site verification. In response to this, Industry inquired as to whether there was a way to identify the most common issues in the four percent so that the problems could be addressed. Mr. Cole responded that there has not been much data mining in order to get this information and that future data mining would need to be done. In addition, Mr. Cole stated that the use of the SSP templates would address many of the

[6] Reference Appendix 6 for Mr. Cole's presentation.
[7] Reference slide 2 in Mr. Cole's presentation.

inconsistencies. In response to Industry's desire to investigate this four percent further, Mr. Cole noted that DSS is hoping to design an information system that would help manage the accreditation process by gathering metrics down to not only individual Commercial and Government Entity codes, but Information Security Systems Managers (ISSMs) as well.

Mr. Cole then reported on metrics relating to errors found during SSP reviews. Mr. Cole stated that the common errors had been accounted for in preparing the SSP templates, which he hopes will resolve the continuation of these errors. Mr. Cole reported that of the 1,700 SSPs received from February 2008 – February 2009, on average, 25 percent of all plans submitted required changes prior to the on-site verification for ATO. Mr. Cole noted that the 25 percent represents those times that DSS needs to have Industry provide clarification regarding the system. Following the review of the metrics, Mr. Cole then reported on the details of the common errors found during SSP reviews.[8]

During the review of the metrics, the Chair noted that the errors have been consistent and, in fact, the frequency of the errors seems to be on the increase; thus, the Chair urged the ODAA and Industry to continue to work on how to address and resolve the common errors. Following these remarks, Industry inquired as to what the errors are attributed to, for example, ISSM lack of knowledge or size of facility. Mr. Cole responded that there are many reasons for the errors; however, the ODAA is not currently capturing the reasons for the errors in its metrics. In response, Industry noted that knowing the finer details of the errors is vital in order to address the problems. A discussion ensued regarding how best to capture these types of metrics. Ms. Watson noted that capturing these metrics is a responsibility shared between DSS and Industry, and that Industry needs to let DSS know what is most needed so that DSS can respond accordingly. She noted that Industry is receiving some of the vital data through the out-processing reports, which detail the rating DSS assigned and the reason why the rating was given; however, Industry responded noting that the finer details that are reported are not being communicated to senior management. Ms. Watson then noted that DSS is dedicated to meeting the needs of Industry and thus, expressed her desire for Industry to communicate those needs to DSS.

Ms. Watson also mentioned that there are many reasons for why a system is not given a satisfactory rating (thus, resulting in classified information not being properly protected) and noted the problem of Industry processing classified information on unaccredited systems. In response to this, the Chair requested that when found, these instances need to be brought to the attention of ISOO and noted the importance of understanding the reasons why systems are not being accredited.

Mr. Cole discussed the recently released ISL (ISL 2009-01, March 5, 2009) which implemented the ODAA "Manual for the Certification and Accreditation of Classified Systems Under the NISPOM" and the "Standardization of Baseline Technical Security Configurations." Mr. Cole noted that the ISL changed the names of what were formerly known as the "ODAA Process Guide" and the "Windows Technical Configuration Baseline." Mr. Cole noted that there was no other significant change achieved in the issuance of the ISL. Industry inquired as to whether the ISL superseded Chapter 8 of the NISPOM. In response, Mr. Lewis noted that the ISL is meant to be an interpretation of Chapter 8. In response to

[8] Reference slides 5–6 of Mr. Cole's presentation.

Industry's comment that the ISL included additional requirements, Mr. Lewis noted that the ISL is an interpretation of what it takes to permit operation of an information system in a specified environment at an acceptable level of risk. Mr. Cole further noted that the ISL was meant to bring greater clarity to the issues at hand.

Ms. Watson noted that DSS is trying to get to a point where there is a baseline understanding of what is required of Industry so that improvements can be made on matters of policy consistency and guidance, timeliness, and also so that information systems are properly protected. Following Ms. Watson's remarks, Industry noted that a current problem with the ISL is that there are technical requirements that can cause problems for some systems. In response, Ms. Watson stated that the ISL's guidelines only need to be followed during the setup of new systems, or during the reaccreditation of older systems. Ms. Watson stated that DSS is willing to work with Industry in special situations. She also stressed that the purpose of the ISL guidelines is to establish baseline standards.

Following Ms. Watson's remarks, the Chair applauded the efforts of DSS and DOD in filling the gap due to the outdated nature of Chapter 8 of the NISPOM. The Chair noted that from his perspective, the guidance was more policy in nature. The Chair stated that in the future, before such guidance/policy is released it should be brought before the NISPPAC and the NISPOM Signatories. As the recently released guidance/policy did not get this level of attention, the Chair stated that he would like to reintroduce the ODAA Working Group (under the title of the "Certification and Accreditation Working Group") in order to determine how to take the released policy/guidance and work it in a way that meets the needs of protecting the information and supporting Industry's ability to perform on Government contracts. The Chair further explained that the group is to identify those examples that DSS needs in order to better understand where the ISL is posing a challenge. The Chair also addressed the issue as to whether some of the ISL requirements exceed the requirements of Government. The Chair informed the NISPPAC that ISOO, DOD, and DSS are working through this issue but also noted that in some areas, the ISL requirements may exceed the requirements for Government only because there is a void in guidance in those areas for Government.

Mr. Cole added that DSS, with OUSD(I), coordinated with DOD Networks and Information Integration (NII), in order to compare the proposed technical standards with NII's technical standards and, ultimately, did not find problems with any material issues. DSS also compared the technical settings with the Common Desktop Configuration, which is being promoted within the Government, and which is going to be a common baseline of standards. Mr. Cole noted that in those areas where there were inconsistencies, DSS worked with NII to clarify why DSS supported the settings, and ultimately, obtained resolution from NII, which represents DOD's information assurance community. In response to a question from Industry, Mr. Cole stated that the technical settings are going to be first applied to unclassified systems. Further, Mr. Cole noted that DSS did not make any settings arbitrarily that were inconsistent with standards that were already being used. During the brief discussion that followed, Ms. Watson stressed the need to have examples of those policies that Industry is unable to implement. Industry responded by suggesting that a "wave-on" rollout process would be a good approach to implementing the guidance. Mr. Cole responded that this would not be necessary since the changes only need to be made with new

systems or during the reaccreditation of systems. Due to time constraints, the discussion was abated.

Finishing his report, Mr. Cole reported that ODAA is working with OUSD(I) with the revision of Chapter 8 of the NISPOM. Mr. Cole also reported that training initiatives are currently being worked.

Following Mr. Cole's remarks, the Chair expressed his appreciation for the update and asked for a similar update at the next NISPPAC meeting.

ACTION: The Chair reintroduced the ODAA Working Group, under the name, "Certification and Accreditation Working Group" in order to work the policy/guidance addressed in the ISL in a manner that meets the needs of protecting information, while supporting Industry's ability to perform on Government contracts. In addition, the group is to identify those examples that DSS needs in order to better understand where the ISL is posing a challenge.

The ODAA will provide a metrics update at the next meeting of the NISPPAC.

D) Combined Industry Presentation
Vince Jarvie, NISPPAC Industry Spokesperson, presented on this topic.[9]

Mr. Jarvie began his update noting that the NISPPAC membership terms would be expiring this year for Timothy McQuiggan and Douglas Hudson. Thus, new members will be sought to fill these spaces. Mr. Jarvie also noted that Randy Foster, Raytheon Corporation, is the new representative for the Contractor SAP Security Working Group, which is now meeting on a regular basis.

Mr. Jarvie discussed the FOCI Working Group and noted its success in bringing many different people to the table in order to discuss the relevant issues. Mr. Jarvie specifically expressed his appreciation to Mr. Lewis for his participation and hard work with regard to the Material Change Matrix, corporate submissions, and the NID process. Mr. Jarvie also discussed the PCL Working Group and noted the hard work of the group and the progress that has been made. Mr. Jarvie noted that Industry is committed to the promulgation of meaningful and implementable policy.

Mr. Jarvie emphasized Industry's concern regarding controlled unclassified information (CUI), specifically with respect to the point that CUI does not turn into a fourth classification category. Mr. Jarvie stressed that CUI has to be congruent with the way Industry protects its proprietary information. To that end, Mr. Jarvie noted that Industry often protects its information at levels higher than are used in the Government.

Mr. Jarvie addressed the topic of the sharing of threat information data. Mr. Jarvie noted that Industry continues to have issues with cyber-attacks, insider-threats, and front-companies. Mr. Jarvie noted that Industry is still looking for a centralized location from which to receive threat data; however, he noted that there are Government agencies that are now sharing data

[9] Reference Appendix 7 for Mr. Jarvie's presentation.

with Industry, specifically the Federal Bureau of Investigation (FBI) and the Defense Industrial Base (DIB) Information Assurance Group. With respect to communication methodology, Mr. Jarvie noted the formation of the DIB-net, which is now providing information to Industry on a real-time basis, in addition to the promotion of the FBI-net.

E) Defense Security Service Update
Kathy Watson, Director, DSS, presented on this topic.

Ms. Watson reported that DSS has reorganized its information security programs into three elements: Field Operations, Policy and Programs, and Counter-Intelligence (CI). With regard to Field Operations, Ms. Watson reported that DSS has developed a "Facility of Interest" list, which implements a risk-based approach to facility inspections. Ms. Watson noted that DSS has identified what it believes to be high-risk factors and companies that have those factors are on the list. Ms. Watson then emphasized that DSS has reduced the ODAA accreditation-cycle timeliness from 120 days to 30-45 days. She stressed that she expects continued improvements in this area with the use of the standard templates.

Ms. Watson addressed CI and noted that DSS has recently published an unclassified and a classified version of "U.S. Technologies: A Threat Analysis of Reporting from Defense Industry." The next edition will be published this summer, and DSS is hoping to move to a quarterly reporting mechanism. Ms. Watson noted that this report is made possible only though Industry's reporting. However, she stated that currently, only about 10 percent of cleared Industry actually report on suspicious foreign contacts. She noted that this needs to be addressed. Ms. Watson then stated that DSS is planning to triple the number of CI analysts on staff. Ms. Watson noted that once DSS has this additional capability, it will be better able to receive and provide information. Ms. Watson also reported that DSS has developed a methodology which helps prioritize suspicious contact reports and which ensures that the most sensitive instances are being addressed.

With regard to Policy and Programs, Ms. Watson noted that the office is more operationally agile in working FOCI cases. Currently, DSS is working with a consultant to look at their processes.

Ms. Watson then addressed the forecasting of Industrial PCLs, and reported that the requirements continue to be 96 percent accurate. Ms. Watson expressed her appreciation for Industry's help with this and stressed the importance of participating in the forecasting.

Ms. Watson then stated her top four priorities for the year, which are CI, FOCI, training, and human resources. With regard to CI, Ms. Watson noted that cyber-threats continue to be a main focus. Accordingly, DSS is participating in the DIB Cyber-security Taskforce and is also starting a cyber-cell within its counter-intelligence unit. With respect to FOCI, Ms. Watson noted that DSS has realigned its FOCI workload to provide field-level adjudication. Ms. Watson stressed that the focus is to understand cases on the strategic level. Ms. Watson then addressed training, noting that DSS is continuing to make improvements in this area and is moving to a more web-based approach. She indicated that DSS just formed the Defense Security Training Council, which will be leveraged in order to help with curriculum development. Finally, Ms. Watson addressed her priorities with respect to human resources.

She noted that DSS is appropriately funded to implement all programs and is moving to make massive hires.

Following Ms. Watson's remarks, the Chair expressed his appreciation to DSS for the hard work and progress made.

F) NISPOM Signatories Update
No updates were reported.

G) Discussion
As there was significant discussion throughout the meeting, the Chair determined that no further discussion time was needed.

V. General Open Forum
No comments were made.

VI. Closing Remarks and Adjournment
The Chair reminded the NISPPAC that the next full meeting would be in late July. With that, the meeting adjourned at 3:09 p.m.

Summary of Action Items:

A) **The Chair requested that the PCL Working Group address, at the next working group meeting, Industry's current capabilities, as well as, any other options available, that would help address the issue of supporting small industrial facilities with the introduction of the new SWFT technology.**

B) **Members of the NISPPAC are to provide formal responses with regard to the proposed changes to the Directive within 30 days.**

C) **Industry will provide a draft definition of "organization" within 30 days.**

D) **Per the Chair, following the next meeting of the FOCI Working Group, the issues involving FOCI will be reevaluated at a later date.**

E) **The NISPPAC members are to review the proposed amendments to the bylaws and provide formal comments within 30 days. Following Article 9 of the bylaws, a vote to approve the proposed bylaws will occur at the next meeting of the NISPPAC.**

F) **The Chair reintroduced the ODAA Working Group, under the name, "Certification and Accreditation Working Group" in order to work the policy/guidance addressed in the ISL in a manner that meets the needs of protecting information, while supporting Industry's ability to perform on Government contracts. In addition, the group is to identify those examples that DSS needs in order to better understand where the ISL is posing a challenge.**

G) **The ODAA will provide a metrics update at the next meeting of the NISPPAC.**

Appendix 1 – Ms. Smith's PCL Working Group Presentation
Appendix 2 – Ms. Denison's PCL Working Group Presentation
Appendix 3 – Mr. Mansfield's PCL Working Group Presentation
Appendix 4 - Mr. Pannoni's FOCI Working Group Presentation
Appendix 5 - Proposed amendments to the NISPPAC Bylaws
Appendix 6 - Mr. Cole's ODAA Presentation
Appendix 7 - Mr. Jarvie's Combined Industry Presentation

Appendix 1
Ms. Smith's PCL Working Group Presentation

Timeliness Performance Metrics for DOD's Industry Personnel Includes Initiation, Investigation, & Adjudication Time

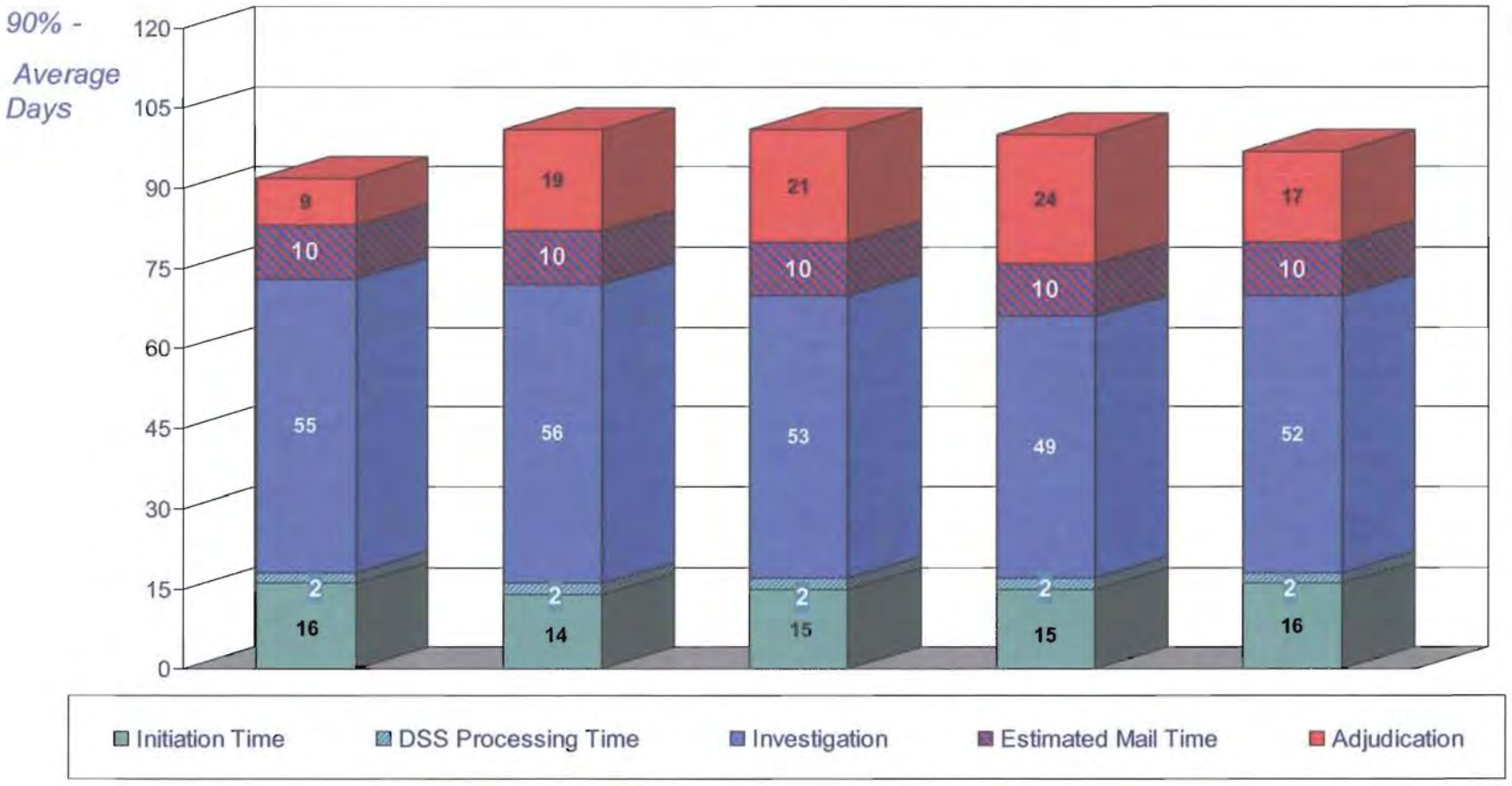
Reported Clearance Decisions Made During the 1st Qtr FY 09

- All Initials – All 27,817 cases: 134 day average cycle time
  - Fastest 80% cases: 86 day average
  - Fastest 90% cases: 97 days

  - TS Initial – All 5,314 cases: 159 day average cycle time
    - Fastest 80% cases: 111 day average
    - Fastest 90% cases: 120 days
  - Secret – All 22,503 cases: 128 day average cycle time
    - Fastest 80% cases: 80 day average
    - Fastest 90% cases: 92 days

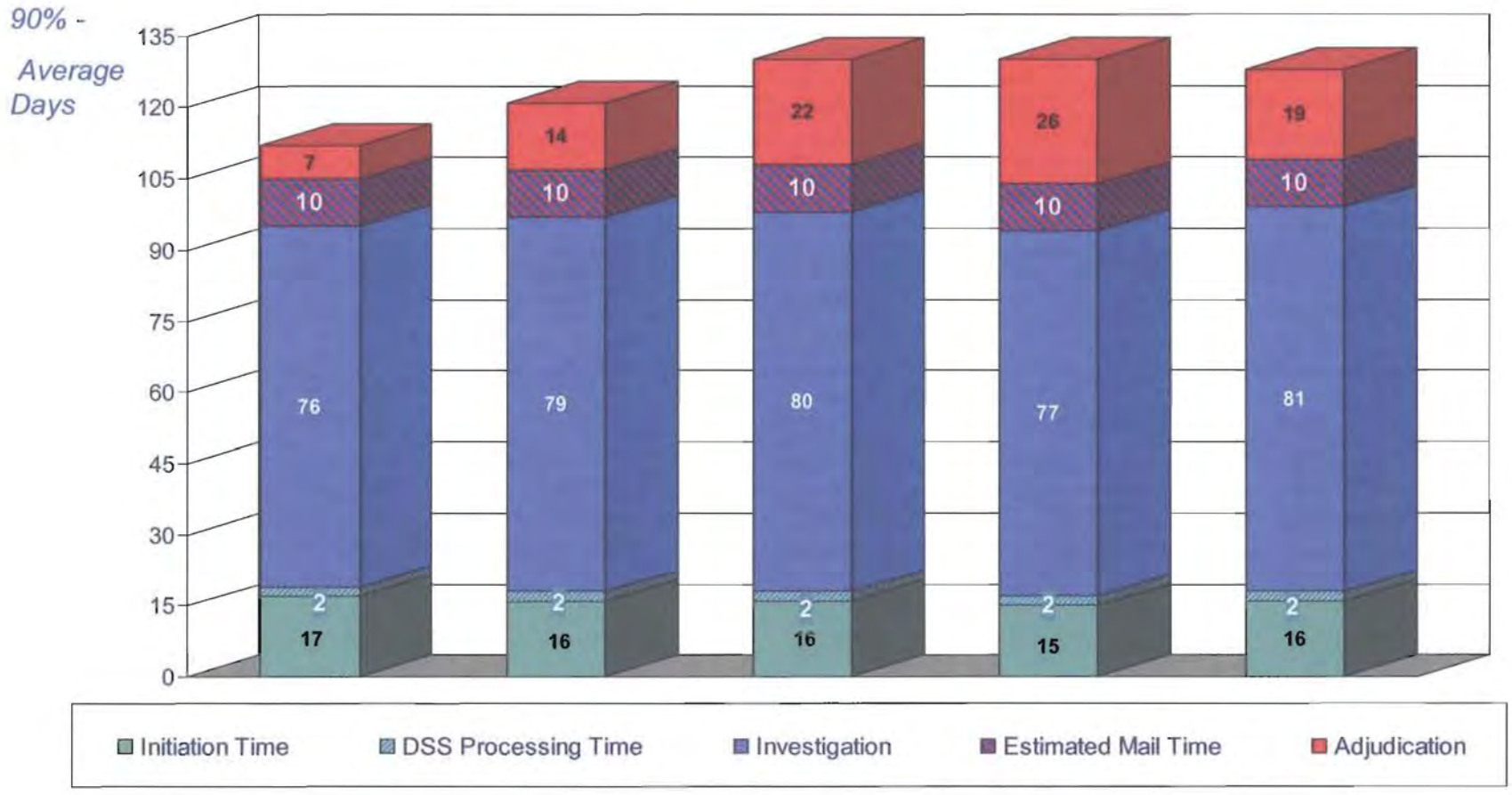
- TS PR – All 9,839 cases: 183 day average cycle time
  - Fastest 80% cases: 122 day average
  - Fastest 90% cases: 136 days

Industry's Average Timeliness Trends for 90% Initial Top Secret and All Secret/Confidential Security Clearance Decisions



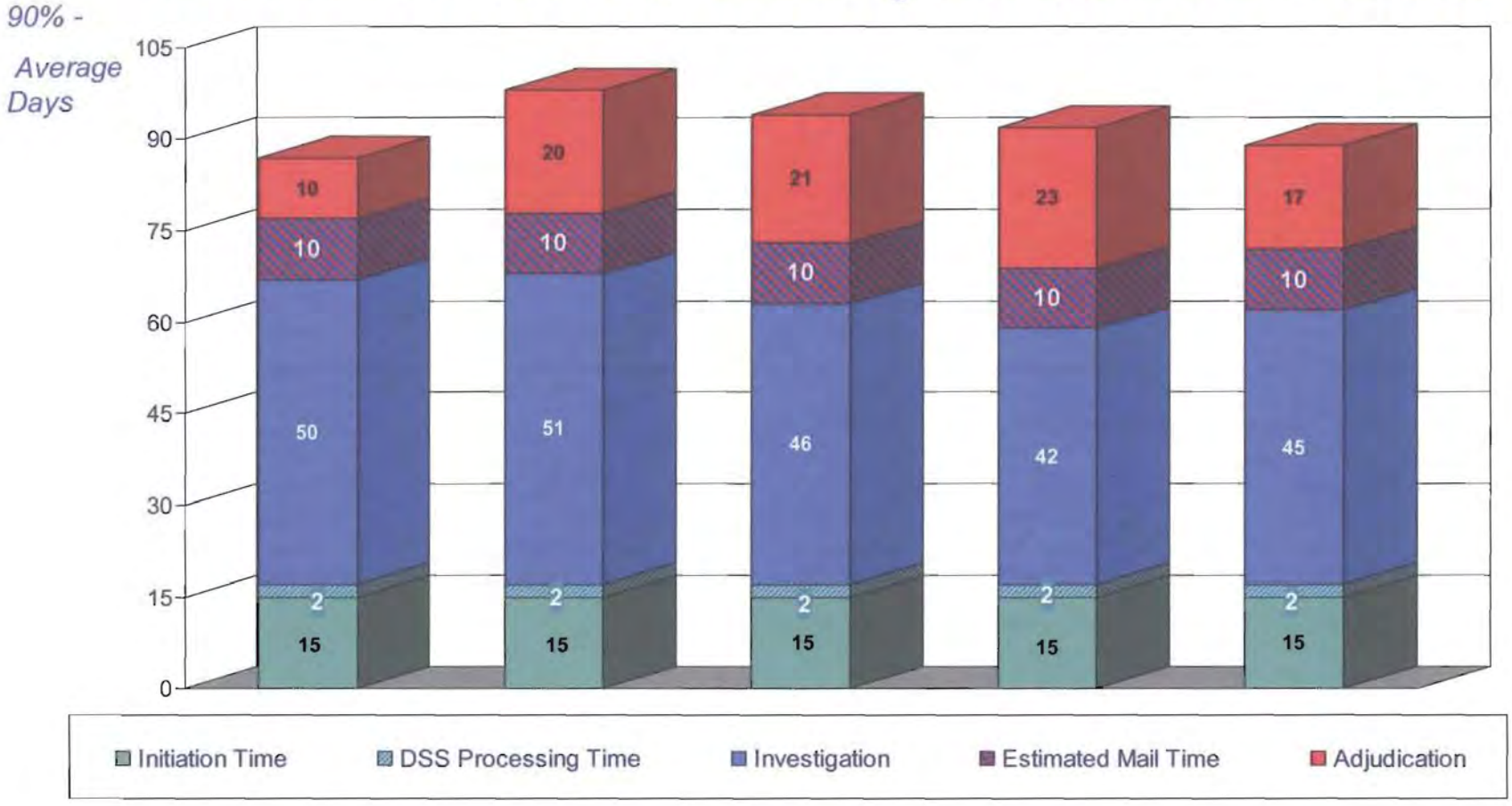
Adjudications actions taken:	Oct 08	Nov 08	Dec 08	Jan 09	Feb 09
100% of Reported Adjudications as of March 25, 2009:	11,868	6,741	9,208	10,318	9,875
Average Days for the first 90%	92 days	101 days	101 days	100 days	97 days

Industry's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



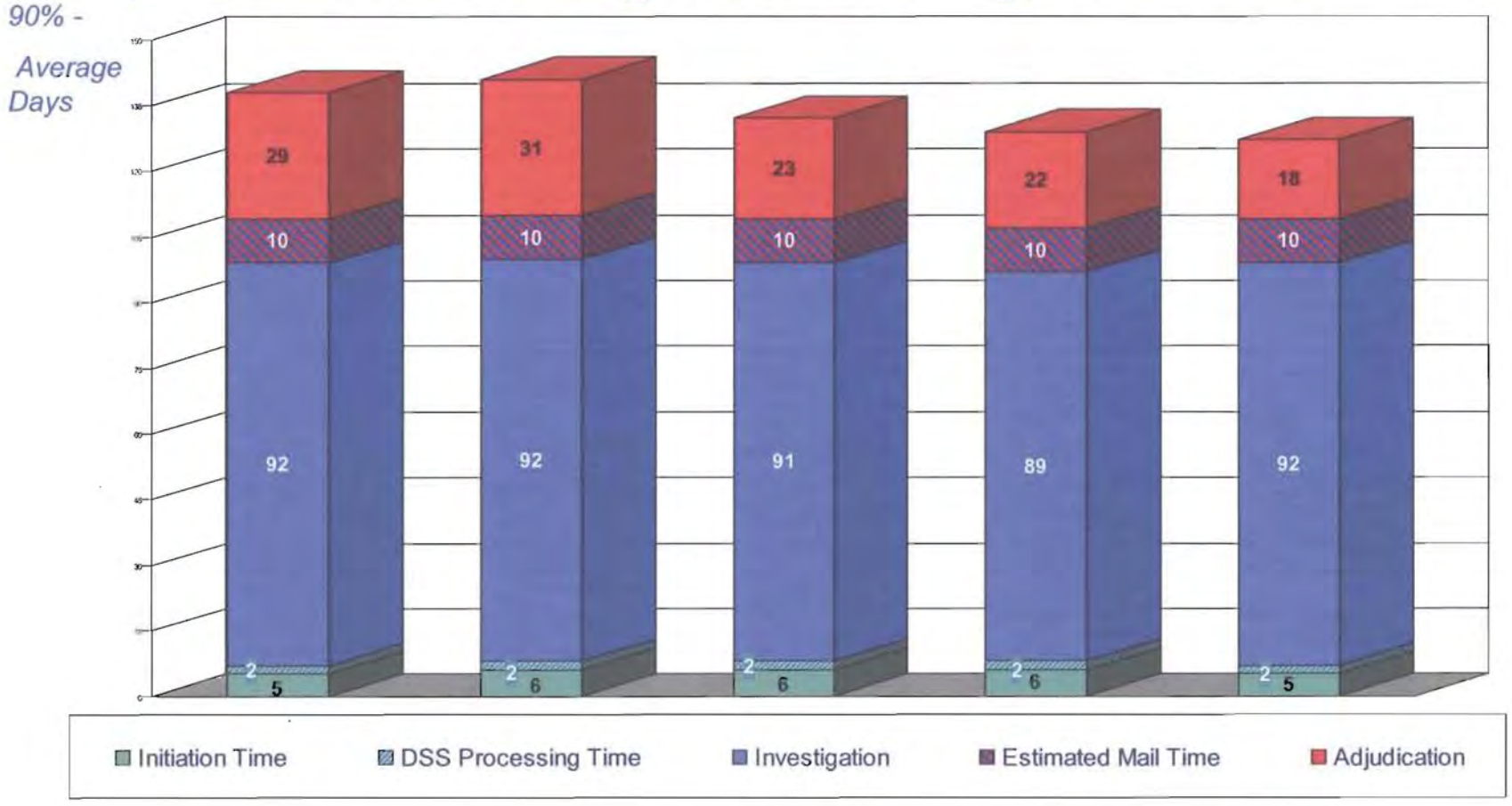
Adjudications actions taken:	Oct 08	Nov 08	Dec 08	Jan 09	Feb 09
100% of Reported Adjudications as of March 25, 2009:	2,450	1,086	1,778	2,231	2,134
Average Days for the first 90%	112 days	121 days	130 days	130 days	128 days

Industry's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



Adjudications actions taken:	Oct 08	Nov 08	Dec 08	Jan 09	Feb 09
100% of Reported Adjudications as of March 25 2009:	9,418	5,655	7,430	8,087	7,741
Average Days for the first 90%	87 days	98 days	94 days	92 days	89 days

Industry's Average Timeliness Trends for 90% Top Secret Reinvestigation Security Clearance Decisions



Adjudications actions taken:	Oct 08	Nov 08	Dec 08	Jan 09	Feb 09
100% of Reported Adjudications as of March 25 2009:	4,471	2,252	3,116	3,408	3,070
Average Days for the first 90%	138 days	141 days	132 days	129 days	127 days

Appendix 2
Ms. Denison's PCL Working Group Presentation

SF-86, Questionnaire for National Security Positions, July 2008 Version

- On January 17, 2009, DoD implemented required Agency Use Block (AUB) fields to enable submission of the July 2008 version of the SF 86 for Industry users.

- On January 16, 2009, DSS posted guidance with changes in completing Requests for Investigations on the the JPAS website.

DISCO

FY09 ADJUDICATION INVENTORY

CASE TYPE	FY 08				FY 09		Delta (Q1FY09 vs Feb09)
	Q1	Q2	Q3	Q4	Q1	Feb-09	
NACLC	11,449	488	240	1,953	4,721	3,344	-29%
SSBI	9,337	5,625	30	354	1,448	1,342	-7%
SBPR	4,899	3,752	5,973	757	974	1,109	14%
Phased PR	8,945	4,923	4,210	330	1,690	2,246	33%
TOTAL PENDING	**34,630**	**14,788**	**10,453**	**3,394**	**8,833**	**8,041**	**-9%**

Overall reduction of 9% for NACLC, SSBI, SBPR and Phased PR case types from 1Q FY09 to Feb 09.

Source: DISCO Manual Counts

INDUSTRY CASES AT OPM

FY09 INVESTIGATION INVENTORY

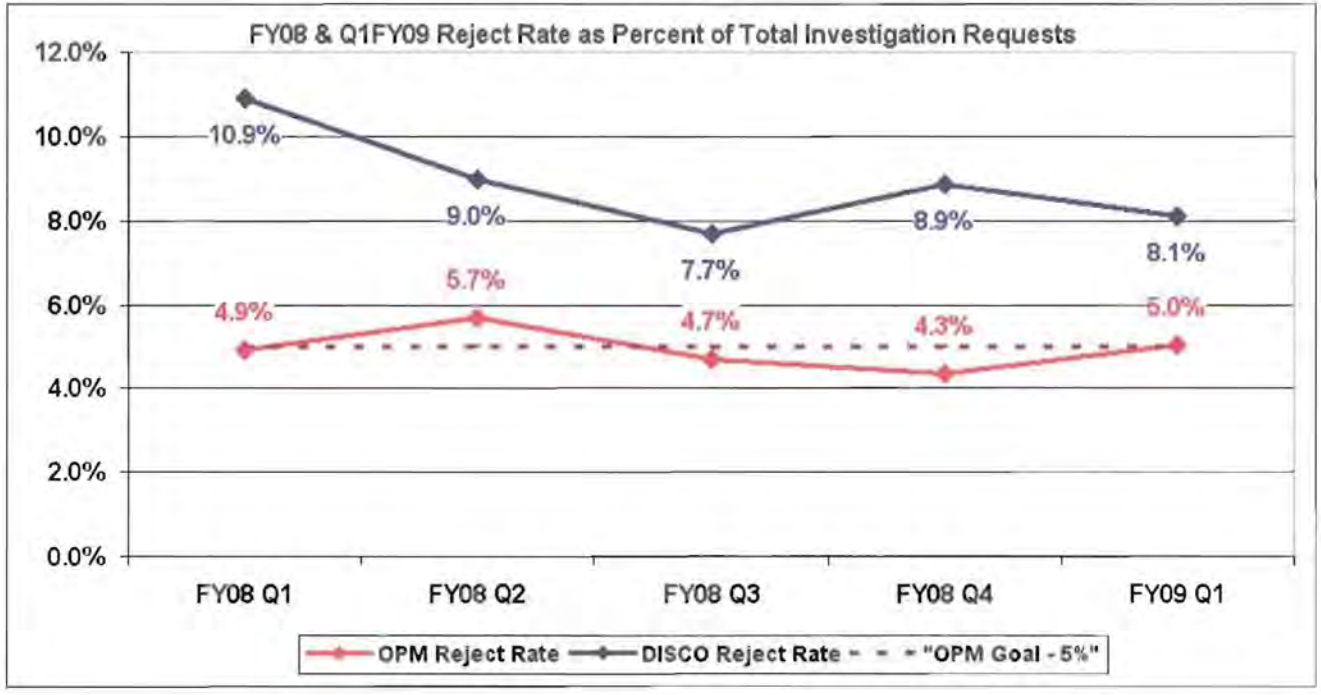
CASE TYPE	FY 08				FY 09		Delta (Q1FY09 vs Feb09)
	Q1	Q2	Q3	Q4	Q1	Feb-09	
NACLC	29,575	25,085	22,077	15,561	13,209	14,072	7%
SSBI	14,110	8,796	7,404	6,720	6,626	6,728	2%
SSBI-PR	11,761	9,943	5,639	4,167	3,772	3,578	-5%
Phased PR	7,711	7,749	6,734	6,408	5,430	3,728	-31%
TOTAL PENDING	**63,157**	**51,573**	**41,854**	**32,856**	**29,037**	**28,106**	-3%

Overall reduction of 3% for NACLC, SSBI, SBPR and Phased PR case types from Q1 FY09 to Feb 09.

Source: OPM Customer Support Group

QUARTERLY REJECT RATES

(Initial & Periodic Reinvestigation Requests)



- **Q1 FY09: DISCO received 44,834 investigation requests**
  - **Rejects:** Total of 5,882 (13.1%) of incoming investigation requests rejected back to FSOs
    - DISCO rejected 3,624 (8.1%) investigation requests to FSOs for re-submittal
    - OPM rejected 2,258 (5.0%) investigation requests to DISCO (and then to FSOs) for re-submittal
- **Note – Case rejection and re-submittal time is not reflected in timeliness.**
  - When a case is re-submitted, the timeline restarts for the PSI/PCL process.
- **For additional guidance please review *"Applicant Tips for Successful e-QIP Submission"* located on the on the DSS.mil JPAS site**

Source: JPAS / OPM IRTPA Monthly Reports

REJECTS
Reasons and Category

TOP REASONS FOR REJECTION

Source – "Analysis of Defective SF86 Submissions" PERSEREC Working Paper 09-03

Section	*Reason for Rejection*	*Number of Subjects*	*% of Subjects (N=4,994)*
12: People Who Know You Well	Incomplete address	1,159	23.2
13-15: Your Spouse	Incomplete name for current spouse	969	19.4
14-15: Relatives - In-Laws	Missing in-law's data	929	18.6
14-15: Relatives	Incomplete address for relative	888	17.8
20: Selective Service Record	Incomplete Selective Service Number	857	17.2
11: Employment Activities	Incomplete address	699	14.0
11: Employment Activities	Explain commute between home and work	657	13.2
11: Employment Activities	Incomplete Phone number	655	13.1
11: Employment Activities	Add employer	612	12.3
13-15: Your Spouse	Clarify living arrangement: are you living with someone in a spouse-like relationship or is the person a roommate?	583	11.7
12: People Who Know You Well	Add the name of another person who knows you well	529	10.6
9: Where You Have Lived	Incomplete address.	520	10.4
14-15: Relatives	Incomplete citizenship data on foreign born relative	520	10.4
14-15: Relatives - In-Laws	Missing in-law's citizenship data	492	9.9

CATEGORIES

- Smaller / Non-possessing, Category E / Secret-cleared

	% of Requests	% of Rejects
A / AA	22.30%	8.80%
B	6.90%	5.90%
C	8.50%	8.40%
D	27.20%	27.70%
E	35.10%	49.20%

FY09 INDUSTRY CLEARANCE SUBMISSIONS VS PROJECTIONS

- OMB performance goal is +/- 5%
  - Feb 09 Status: At the close of February, Industry clearance submissions were **6.5**% below overall Industry/DSS projections.
  - Historically, case submissions trend downward during winter months and peak during spring and summer months.

FY09 Projection	Weekly Projected	Year to Date	% of Projection
182,315	3,506	3,278	**93.5%**

Appendix 3
Mr. Mansfield's PCL Working Group Presentation

Defense Security Service

Security Systems Program Status

Office of the Chief Information Officer

April 7, 2009

Agenda

Secure Web Fingerprint Transmission System (SWFT)

- **Current & Future System**
- **New Features**
- **System Configuration**
- **Transition**
- **Questions**

Current & Future System

There are still four major SWFT business functions (future in red):

- Capture - Fingerprint images captured electronically.
  - Facility Security Officer (FSO) captures fingerprint images and demographic information
- Upload - Electronic file uploaded to DSS server
  - FSO signs onto an https web site and uploads captured fingerprint images and demographic data, or
  - FSO's backend server uploads capture fingerprint images directly via secure web services
- Store - Electronic file stored temporarily
  - Captured fingerprint images and demographic data are then stored in the SWFT system
- Release - Electronic file release to OPM
  - Using data from a daily release file provided by JPAS to determine which fingerprint to release
  - Captured fingerprint images and demographic data are automatically and manually released from the SWFT system to OPM

New Features

- Industry users will be able to securely transmit from their systems to SWFT via secure web services
- Store in excess of 15,000 fingerprint submissions
- Data analysis to identify records for automatic and manual release to OPM
- Notification to Industry users regarding their transmission status
- Metrics reporting capability
- Account Management that allows: Account creation, Password management, and Multiple user roles

Systems Configuration

- The SWFT application, web site, and data will be hosted at DSS Headquarters at Braddock Place
- The backup site will be hosted in Monterey, CA and connected to the production site via a VPN
  - Data replication between sites will be performed without operator intervention
- VPN connection to allow vendor to perform system administration and troubleshooting tasks

Transition Pilot to Production

- Once the system goes live in July 2009 only the new SWFT will be accessible
- No user information or data will be migrated from the pilot system
- All user information will be recreated by the DSS SWFT administrators
- Industry users will be contacted to resubmit any outstanding EFTs

Questions?

Appendix 4
Mr. Pannoni's FOCI Working Group Presentation

Foreign Ownership, Control, or Influence (FOCI) Working Group Update

NISPPAC, April 7, 2009

General

- Working Group convened twice
- Purpose to evaluate the NISP FOCI process and develop recommendations for improvement
- Representation

  --- Army, DOD, DHS, ODNI, FBI, State, DSS, Navy, Air Force, Treasury, DOE, DTSA, NSA, ISOO, Industry

When is a U.S. company considered under FOCI?

- If a foreign interest has the power to direct or decide matters affecting the management or operations of a company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts (paraphrased from 2-300.a NISPOM)

Focus of Effort

- Review & Evaluation of FOCI Process
  - ID actual/potential FOCI factors
  - Tools to mitigate foreign interest involvement
  - Monitoring changed conditions
  - Reporting requirements

- Recommendations to Improve the Process

Recommendations

- Issue a Material Change Matrix for standardization of what constitutes a change of real importance/great consequence
- NISP Implementing Directive revision to address NID process
- NISPOM revision to clarify the purpose of NIDs pertinent to national security interests
- Database of NID POCs

Electronic FOCI (eFOCI)

- Review and demonstration of DOE eFOCI system provides an efficient means for meeting FOCI reporting requirements
- DOD is implementing eFOCI on a 'phased approach' and is planning to have all DSS elements operational by Sept 30, 2009
- Should eliminate preponderance of redundant reporting requirements

Ancillary Concern

- Some Executive Branch agencies continue to require completion of SF 328 data for purposes other than NISP FOCI determinations, despite the Form's provisions that it is authorized for the NISP
- An example is requiring the information for a risk assessment as part of an acquisition initiative/effort.

Future Efforts

- Recommend the FOCI working group reconvene after changes to the NISP implementing directive and promulgation of the Material Change Matrix to evaluate the effectiveness of the changes.

Questions?

Contact:

Greg Pannoni
Associate Director, Operations and Industrial Security
Telephone: 202-357-5047
E-mail: Greg.Pannoni@nara.gov

Appendix 5
Proposed amendments to the NISPPAC Bylaws

Formatted: Right

National Industrial Program Policy Advisory Committee (NISPPAC)

Bylaws (As amended in April, 2009)

Deleted: May 2007

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, (the Order) establishes the NISPPAC as an advisory committee acting through the Director, Information Security Oversight Office (ISOO), who serves as the Chairman of the Committee, and who is responsible for implementing and monitoring the NISP, developing directives implementing the Order, reviewing agency implementing regulations, and overseeing agency and industry compliance. The framework for the Committee's membership, operations, and administration is set forth 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).

Deleted: E.O. 12829, as amended,

Article 3. Membership

A. **Primary Membership.**

The Order 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 those executive branch departments and agencies (including the Chairman) most affected by the NISP and eight non-government representatives of

Deleted: Executive Order 12829, as amended,

Deleted: from industry

contractors, licenses, grantees involved with classified contracts, licenses, or grants. 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 their 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 advance written notification to 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.

D. **Term of Membership.** The term of membership for Government representatives shall be four years. When renominated by the head of their agency, a representative of a Government agency may be selected to serve successive four year terms. The term of membership for industry representatives shall be four years. The terms of industry

Formatted: Right

Deleted: 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.

Deleted: his or her

Deleted: the

Deleted: written approval of

Deleted: 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.

Deleted: three

Deleted: .

Deleted: with the terms of initial members ending on September 30, 1996.

Deleted: his or her

Deleted: three-

Deleted: Commencing in fiscal year 1998,

Deleted: t

representatives shall be staggered so that the terms of two industry representatives are completed at the end of each fiscal year. 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 the 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. **Security Clearance.** If it becomes necessary to hold a classified meeting, members and alternates in attendance must possess a current security clearance at or above the level of the meeting's classification. Clearance certification shall be provided in advance of the meeting 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 presentations, 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

Formatted: Right

Deleted: 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.

Deleted: M

Deleted: Secret

Deleted: or above, and c

Deleted: to

Deleted:

Formatted: Right

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 a notice in the Federal Register at least 15 calendar days prior to each meeting.

Deleted: five

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 full or partial closing 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 a closed session. Notices of closed meetings will be published in the Federal Register at least 15 calendar days in advance.

Deleted: all or just part of

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 a brief outline of

Deleted: n

Formatted: Right

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, 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 National Industrial Security Program Operating Manual 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.

Deleted: member

Deleted: NISPOM

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 certified minutes of the previous meeting. 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.

Deleted: At that time the minutes will be corrected, as necessary, and approved by the membership and certified by the Chairman.

G. **Minutes.** The Committee's Executive Secretary shall prepare minutes of each meeting, which will be certified by the Designated Federal Official (DFO) within 90 calendar days. Copies of the minutes will be distributed to each Committee member once certified. Minutes of open meetings will be accessible to the public. 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

Deleted: and

Deleted: copies

Deleted: available

Deleted: upon request.

Formatted: Right

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 a portion(s) of a meeting, 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 may note that oral comment from the public is excluded and in such circumstances invite written comment as an alternative. Also, members of the public may submit written statements to the Committee at any time.

Deleted: will

Deleted: will

Deleted: Me

I. **Sub-committee Meetings.** The Chairman may establish a sub-committee(s), to include sub-groups or working groups. Sub-committees shall brief the members of the NISPPAC on its work, and any recommendations of a sub-committee shall be presented to the NISPPAC for deliberation.

Formatted: Bullets and Numbering

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 an industry or Government representative.

Deleted: d

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 cast are in favor of, or are opposed to, a particular motion; (4) Government and Industry Majority. Results when the majority of the votes cast, 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 the Order, the Committee Chairman is the Director, ISOO. The Chairman will: (1) call meetings of the full Committee; (2) set the meeting agenda; (3) determine a quorum; (4) open, preside over and adjourn meetings; and (5) certify meeting minutes. The Chairman also serves as the Committee's DFO, a position required by the FACA.

B. **Designated Federal Officer.** The FACA requires each advisory committee to have a DFO and an alternate, one of whom must be present for all meetings. The Director and Associate Director, Operations and Industrial Security, ISOO, are, respectively, the DFO and alternate for the NISPPAC. Any meeting held without the DFO or alternate present will be considered as a subgroup or working group meeting.

Formatted: Right

Deleted: ed

Deleted: casted, including

Deleted: Executive Order 12829, as amended

Deleted: of the Information Security Oversight Office

Deleted:

Deleted: and

Deleted: ,

Deleted: esignated Federal Officer

Deleted: esignated Federal Officer (D

Deleted:)

Deleted: nformation Security Oversight Office

Deleted: esignated

Deleted: ederal

Deleted: fficer

Formatted: Right

Deleted: nformation Security Oversight Office

C. **Executive Secretary.** The Executive Secretary shall be a member of the staff of the ISOO 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; (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.

Deleted: including subgroup and working group activities that are presented to the full Committee;

D. **Committee Staff.** The staff of the ISOO 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.

Deleted: nformation Security Oversight Office

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.

Formatted: Right

Article 8. Committee Expenses and Cost Accounting.

Committee expenses, including travel and per diem of non-Government members, will be borne by the ISOO 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.

Deleted: nformation Security Oversight Office

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 the Order and be agreed to 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.

Deleted: Executive Order 12829, as amended.

Deleted:

Deleted: b

Appendix 6
Mr. Cole's ODAA Working Group Presentation

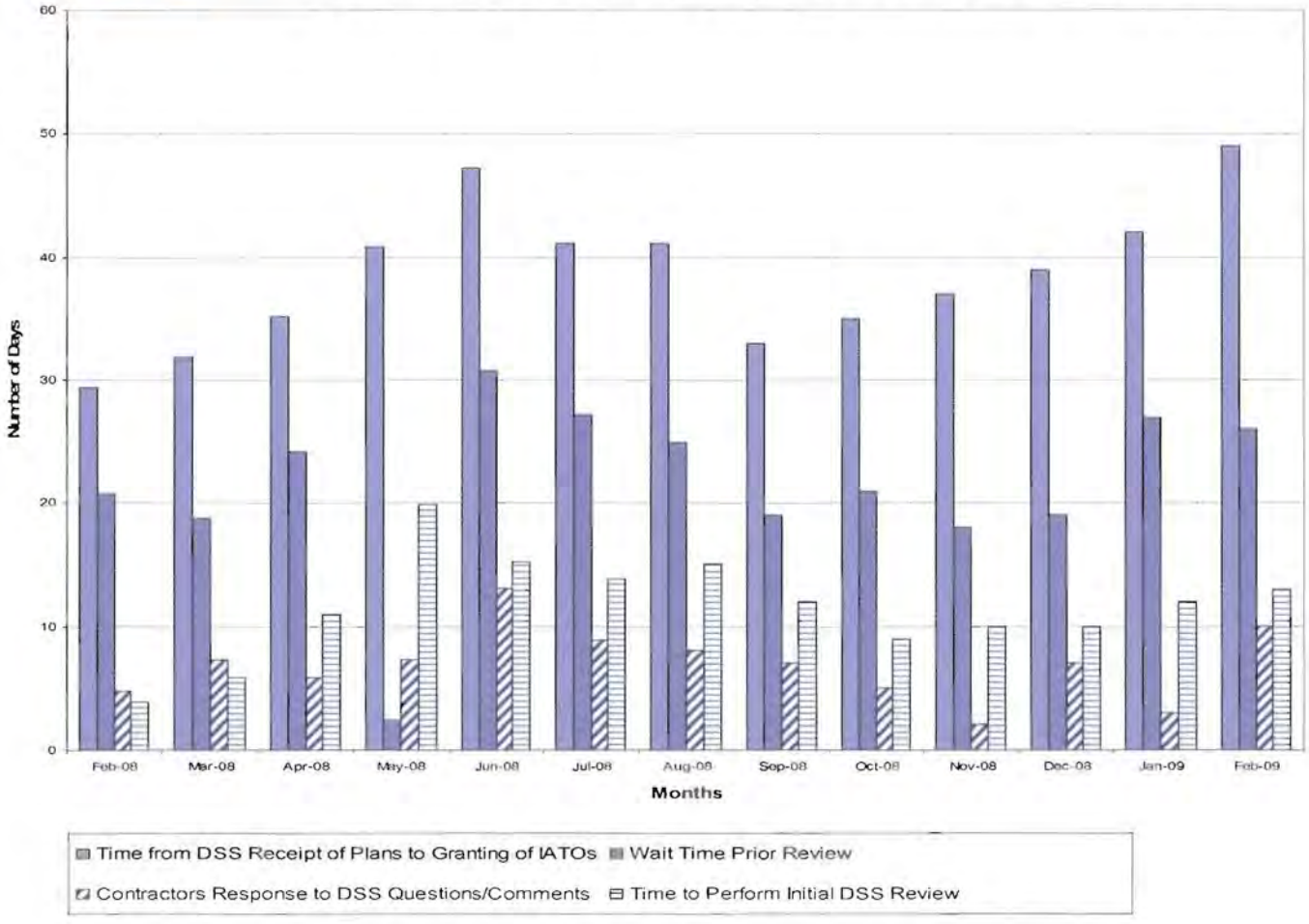
Defense Security Service

Industrial Security Field Operations Office of the Designated Approving Authority (ODAA)

April 2009

ODAA Improving Accreditation Timeliness and Consistency

ODAA Metrics for # Days to Process Plan Submissions

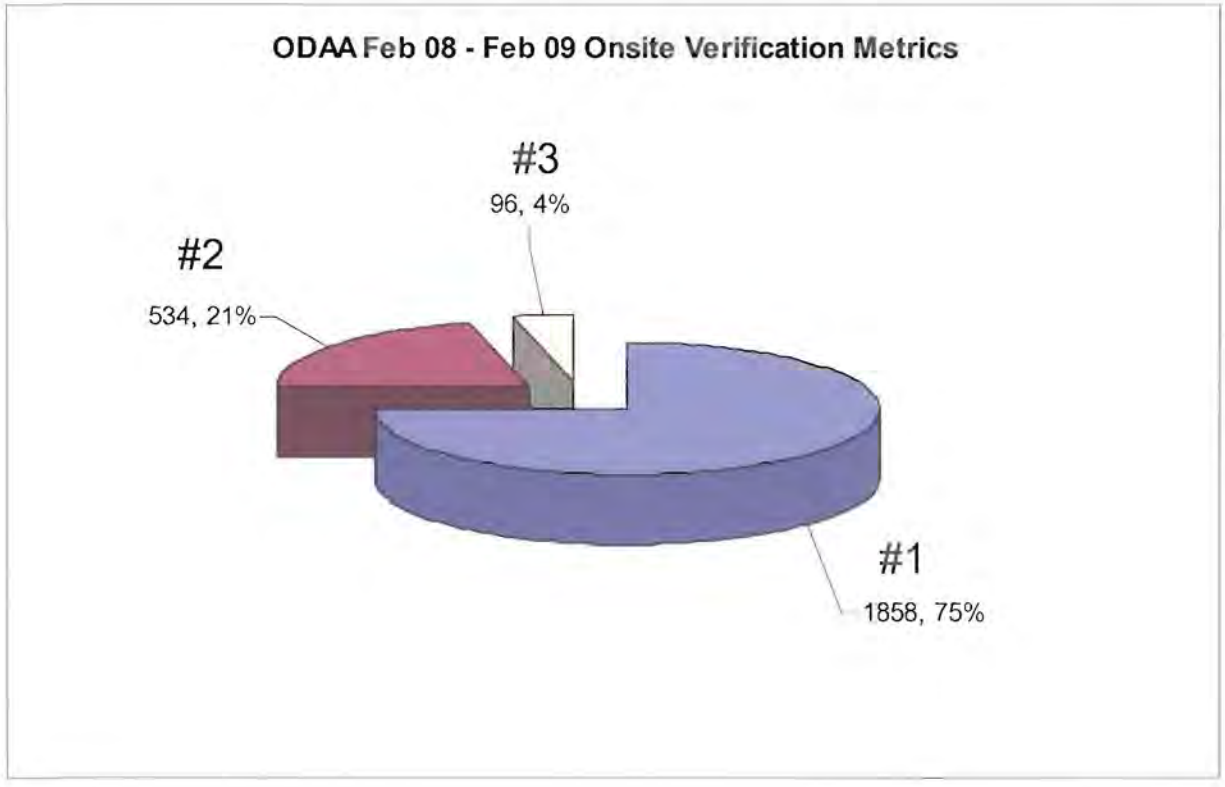


During the Past Year Feb 2008 – Feb 2009

- Average number of days to receive an IATO after receipt of a submission is 39 Days
- Average waiting time before a review process is initiated is 21 Days
- Average number of days for the review time to be completed is 12 Days

ODAA Metrics and Organization

On-site Verification Stats (25% Required Some Level Modifications)



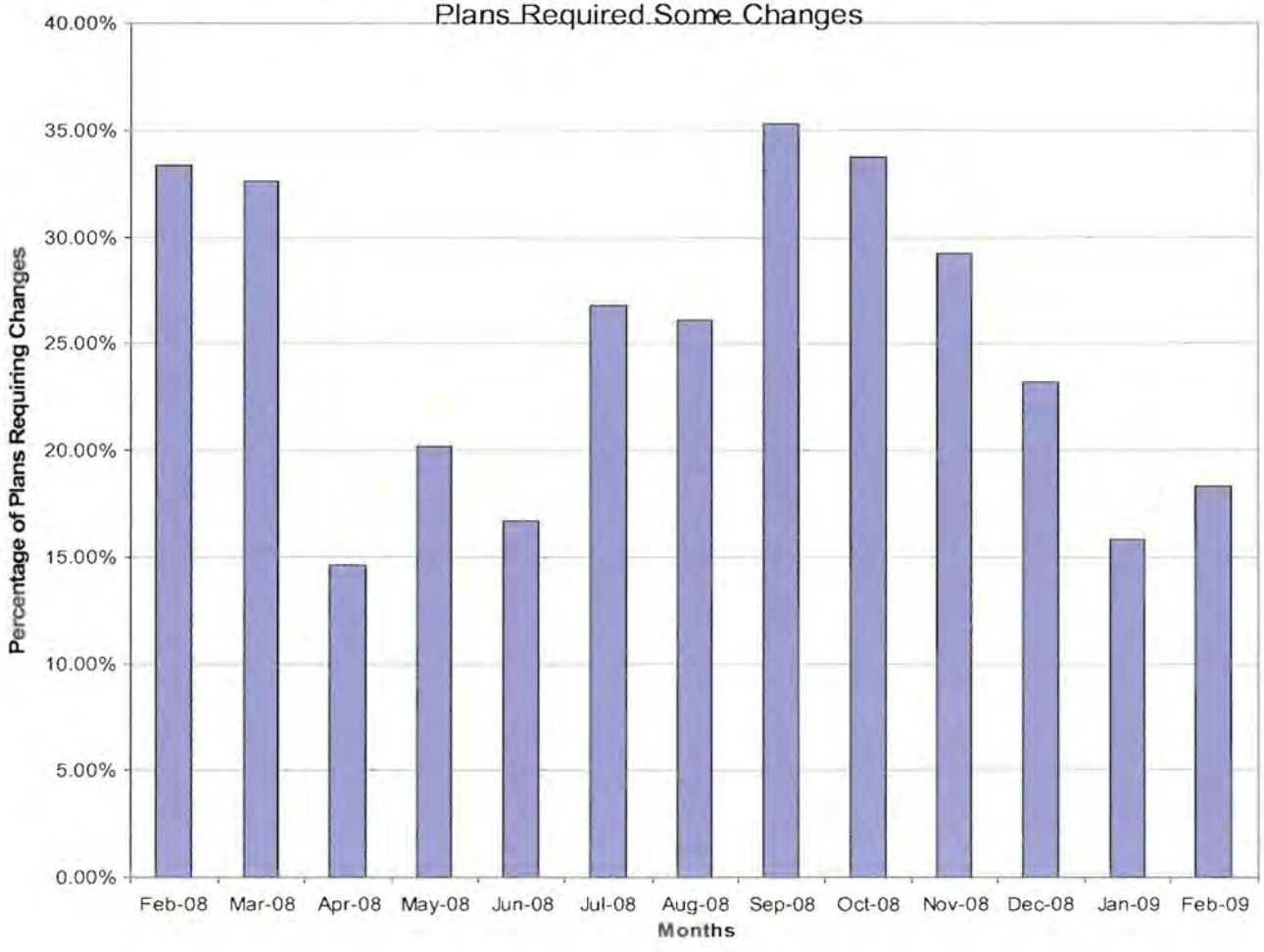
#1. No discrepancies discovered during on-site validation.

#2. Minor discrepancies noted and corrected during on-site validation.

#3. Significant discrepancies noted which could not be resolved during on-site validation.

ODAA Metrics
Security Plan Reviews

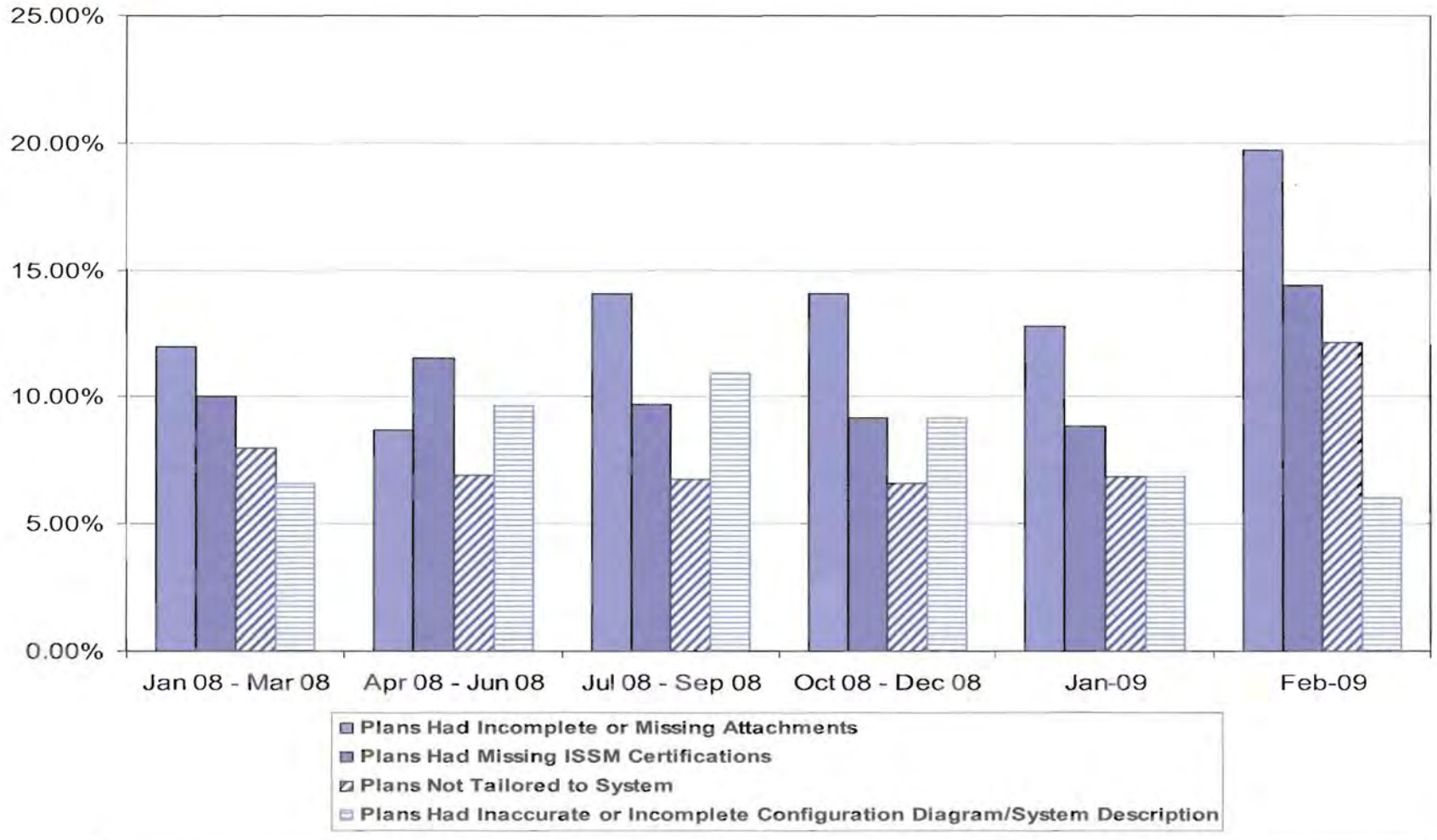
Review Questions and/or Comments, Errors and Corrections Noted



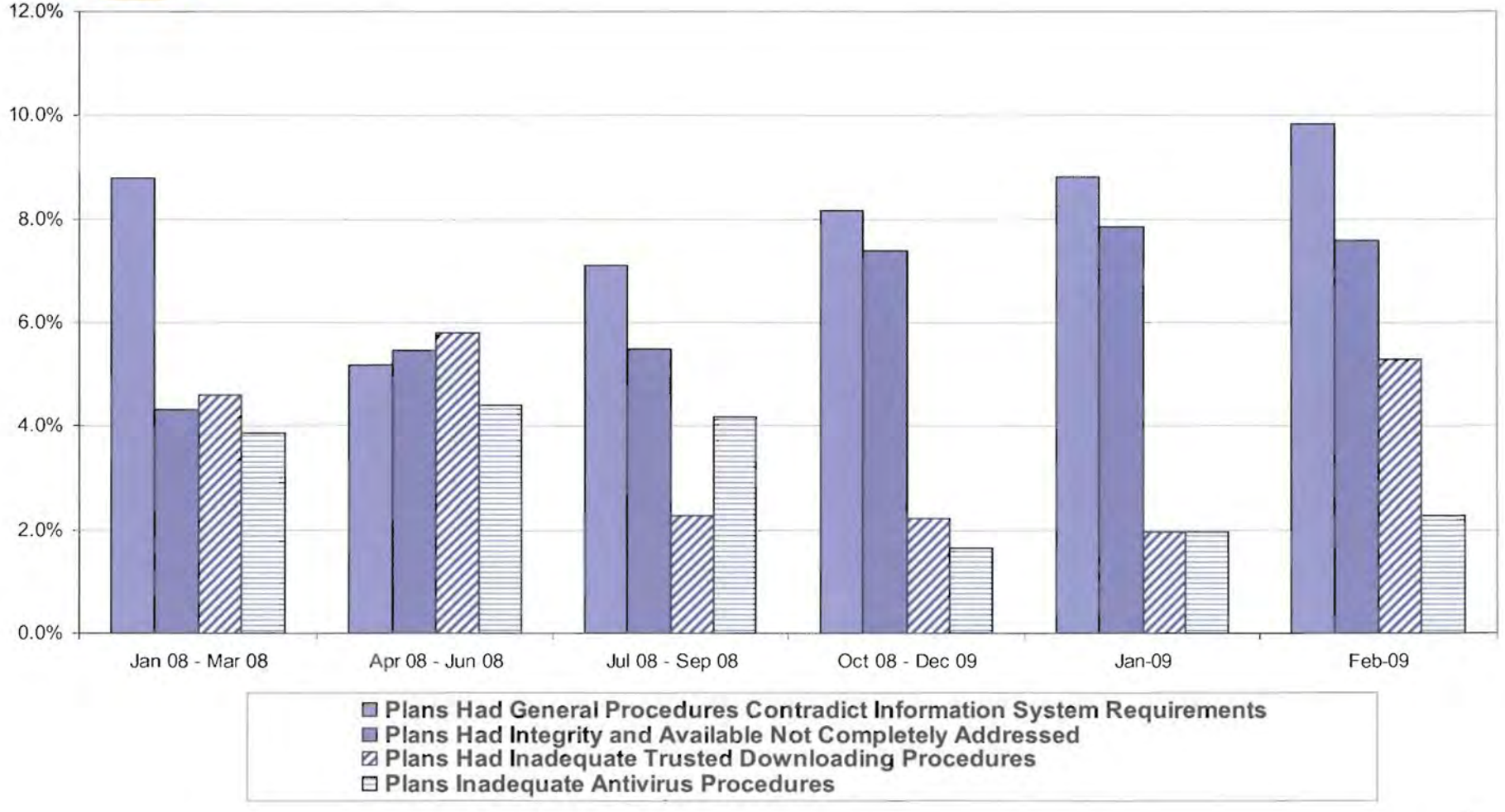
Of the 1700 plans received from Feb 08 – Feb 09:

- On average 25.1 % of all plans submitted required changes prior to the On-site Verification for ATO

ODAA Metrics
Security Plan Reviews Common Errors
Part One



ODAA Metrics
Security Plan Reviews Common Errors
Part Two



DSS ISFO Accreditation Policies and Procedures Update

- ISL 2009-01 March 5, 2009

Implements DSS ODAA "Manual for the Certification and Accreditation of Classified Systems under the NISPOM" and DSS ODAA Standardization of Baseline Technical Security Configurations"

- Time frame for compliance: New systems and re-accreditations
- Technical Settings are "baseline", document non-compliance
- DSS procedures coordinated and approved within DoD and Services

NISPOM Chapter 8 planned redraft

- Based on DoD, DNI, and Federal C&A policies and procedures
- Based on NIST 800-53 and draft CNSS 12-53
- Benchmark analysis completed (NISPOM, DNI, DIACAP, NIST, JAFAN controls)
- Greater emphasis in cyber network inspection and vulnerability partnership assessments

DSS ISFO Accreditation Policies and Procedures Update

- DSS ISFO C&A Training Initiative
- DSS ISFO C&A Work Shops
- Overall Process and Purpose of Changes
  - Risk management approach leveraging DoD, DNI, and other Federal efforts within IT security
  - Standardize processes and documents
  - Enhance computer security controls equivalent with today's threats
    - External and insider

Appendix 7
Mr. Jarvie's Combined Industry Presentation

NISPPAC
Industry Presentation

7 April 2009

Industry Members/NISPPAC

Member	Company	Term Expires
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

Industry Members/MOU

AIA	Scott Conway
ASIS	Ed Halibozek
CSSWG	Randy Foster
ISWG	Mitch Lawrence
ITAA	Richard “Lee” Engel
NCMS	Paulette Hamblin
NDIA	Fred Riccardi

NISPPAC Ad Hoc Working Group

- Foreign Ownership Control and Influence (FOCI)
  - Material change
  - Corporate submission
  - National Interest Determination (NID) process

NISPPAC Ad Hoc Working Group

- Personnel Security Clearance Processing
  - Consistent and synchronized metrics
  - Process for continuous improvement

NISPPAC

- National Industrial Security Program (NISP)
  - Industrial Security Letter Implementation
    - Office of the Designated Approval Authority
      - Process Guide
      - Configuration Guide
  - National Industrial Security Program Operating Manual

NISPPAC Reports

(Industry concerns 15 May 2008/ 20 November 2008)

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

*previously discussed

Information Sharing - Threat

Institutionalized Process:

- Information
- Communication methodology
- Feedback