NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

SUMMARY MINUTES OF THE MEETING

The NISPPAC held its 35th meeting on Wednesday, March 24, 2010, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, NW, Washington, DC. William J. Bosanko, Director, Information Security Oversight Office (ISOO), chaired the meeting, which was open to the public. The following minutes were finalized and certified on July 13, 2010.

The following members/observers were present:

- William J. Bosanko (Chairman)
- Daniel McGarvey (Department of the Air Force)
- Lisa Gearhart (Department of the Army)
- George Ladner (Central Intelligence Agency)
- Stephen Lewis (Department of Defense)
- Drew Winneberger (Defense Security Service)
- Richard Hohman (Office of the Director of National Intelligence)
- Richard Donovan (Department of Energy)
- Christal Fulton (Department of Homeland Security)
- Sean Carney (Department of the Navy)
- Dennis Hanratty (National Security Agency)
- Darlene Fenton (Nuclear Regulatory Commission)
- Kimberly Baugher (Department of State)
- Chris Beals (Industry)
- Scott Conway (Industry)
- Shawn Daley (Industry)
- Richard Lee Engel (Industry)
- Sheri Escobar (Industry)
- Vincent Jarvie (Industry)
- Frederick Riccardi (Industry)
- Marshall Sanders (Industry)
- Merton Miller (Office of Personnel Management) – Observer

I. Welcome, Introductions, and Administrative Matters

The Chairman greeted the membership and called the meeting to order at 10:00 a.m. After introductions, the Chairman directed attention to Deborah Smith, Office of Personnel Management (OPM), and recognized her service to the NISPPAC and her impending retirement.

II. Old Business

The Chairman requested that Greg Pannoni, Designated Federal Officer (DFO), ISOO review the action items from the last meeting.

ACTION: The Chair stated that there was a request to examine how to better support smaller companies. There are two options: (1) use one of the three NISPPAC meetings as a focus meeting for small company solutions and solicit issues of concern from small companies; or (2) hold a NISPPAC meeting outside of the Washington DC area to create greater involvement from

smaller companies. The Chair stated that these two options would be pursued within the provisions of the FACA.

Mr. Pannoni stated that the Federal Advisory Committee Act (FACA) does not restrict the options of holding a NISPPAC meeting specially designated for smaller companies or a meeting outside of the Washington, DC, area. He stated that the NISPPAC meeting, scheduled for November 17, 2010, is a possible candidate for a focus meeting dedicated to smaller companies. Also, he stated that in 2011 a NISPPAC meeting may be held outside the Washington, DC, area by partnering with an industry-led gathering such as the National Classification Management Society Annual Training Seminar or one of the Industrial Security Awareness Council Seminars.

ACTION: The Chair stated that the NISPPAC Charter has been renewed and the bylaws will require further amendment. The Chair stated that through the FACA review process, which is managed by the General Services Administration, it was determined that the Chair should not serve as the Designated Federal Officer (DFO) of the NISPPAC. The new DFO will be Mr. Pannoni, and the alternate DFO will be David Best, ISOO. An updated version of the bylaws to reflect this change will be provided to the members and subsequently a vote will be taken.

Mr. Pannoni stated that the NISPPAC Bylaws were further amended to reflect that the DFO is the Associate Director, Operations and Industrial Security, ISOO, rather than the Chairman. The Chairman stated that a formal vote must be taken to approve the amendment to the bylaws. He stated that under the amendment Mr. Pannoni would be the DFO and the alternate DFO would be the Senior Program Analyst, Operations and Industrial Security, ISOO, who currently is David Best. The Chairman called for a vote on the amended bylaws; a vote was taken and passed by unanimous decision. He stated that the bylaws will be available online at the ISOO website.

ACTION: The Chair stated that he would send a letter to the heads of Government agencies requesting appointment letters designating their Government representative to the NISPPAC. He stated that if a response has not been received by the next NISPPAC meeting, the Government agency would be downgraded to "Observer" status. The Chair requested that members respond within the next two weeks with contact information and courtesy copy information.

Mr. Pannoni stated that a memorandum was sent to government agencies represented on the NISPPAC, requesting them to provide the names of the nominees to serve as members on the committee by April 16, 2010. The Chairman stated that concerns were raised by various members regarding the bylaws, which state the agency head will nominate the agency's member. He stated that the memorandum was addressed to the senior agency official designated under Executive Order 12829, as amended, "National Industrial Security Program," but drafted to preserve the intent of having the agency heads approve the nominations.

ACTION: The Chair stated that a new ad hoc working group would be formed to address the issue of non-GSA approved containers still in use by Government and Industry and their plans for ensuring that the October 1, 2012, deadline for discontinuing the use of these containers is met.

Mr. Pannoni stated that ISOO received a request from Congress to review the status of replacing non-General Service Administration (GSA) approved containers and as a result, formed an ad hoc working group. He stated that the group was formed for a single meeting and that almost all government agencies and industry were well on their way to having all containers replaced by the October 1, 2012, deadline. He stated that one agency advised that it believes that all of its Non-GSA containers had been replaced but would provide confirmation in the coming months. Another agency reported having a substantial number of non-GSA approved containers in use and would be providing ISOO its plan to address replacing these containers sometime next week.

After a review of the action items, Mr. Pannoni reported that the amendment to 32 C.F.R. Part 2004, "National Industrial Security Program Directive No. 1," was finalized and ready to be signed by the Archivist of the United States by the end of the week for publication in the Federal Register. He stated that the amendment addressed the National Interest Determinations (NID) and provided specific guidance as to how a NID was processed. The Chairman stated that once the amended directive was published, an electronic copy would be provided to the membership and also posted on the ISOO website.

III. Working Group Updates

A) Personnel Security Clearance (PCL) Working Group Report[1]

Ms. Smith and Kathleen Branch, Defense Security Service (DSS), provided the PCL Working Group report. Ms. Smith stated that data has been updated to reflect the first quarter of fiscal year (FY) 2010. She stated that end-to-end metrics for Department of Defense (DoD) industry personnel are based on the adjudicative decisions and date as reported by DSS to OPM through a daily upload to the Personnel Investigative Processing System (PIPS). She stated that PIPS tracked every event from the time a subject is initiated in the Electronic Questionnaires for Investigations Processing (e-QIP) system until the date of adjudication is reported. She stated that the query used to develop the metrics was based on the billing code the Defense Industrial Security Clearance Office (DISCO) uses to submit industry investigations to OPM.

Ms. Smith reported the number of cases processed in the first quarter of FY 2010 for initial clearances at all levels and commented that there was an increase from the fourth quarter of FY 2009. She also reported the average number of days for completion of all initial Top Secret (TS) and all Secret/Confidential investigations and the average for the fastest 90 percent completed. These metrics were further divided into the numbers for each clearance level. She stated that there was an overall reduction in the average number of days for the fastest 90 percent of all investigations from the previous quarter. Furthermore, she provided metrics for all Top Secret Periodic Reinvestigations (TS-PR) and for the fastest 90 percent completed. She commented that, during the quarter, the number of days for adjudication for all types of cases was reduced by eight days.

Ms. Smith stated that, as of August 20, 2009, DISCO began receiving investigation results electronically from OPM. She stated that until August, OPM had estimated

[1] See appendix 1 for Ms. Smith's presentation and appendix 2 for Ms. Branch's presentation.

10 days for mail time, but now, since systems transmit electronically, the adjudication time starts once transmission is complete. Therefore, the 10-day estimate was eliminated. Next, she provided monthly combined metrics for January 2010, on the fastest 90 percent of all initial TS and all Secret/Confidential investigations completed with a breakdown of timeliness for each phase of the clearance process: case initiation, DSS processing, investigation, and adjudication. She stated that the initiation time represented the period from certification of the e-QIP until the date of receipt at OPM; the investigation time represented the period from the date of receipt of a complete and acceptable case at OPM until the electronic transmission to DISCO; and the adjudication time represented the time from receipt at DISCO until adjudication. She provided metrics on the fastest 90 percent of investigations at each individual clearance level and for TS-PR.

Finally, Ms. Smith addressed concerns expressed by industry over the number of case submissions by providing a trend line for FY 2007, 2008, 2009, and cases received so far in 2010. She stated that the Single Scope Background Investigations (SSBI) have increased by approximately 2,000 cases each year since 2007 and require more time and resources to investigate and adjudicate. National Agency Checks with Law and Credit (NACLC), which represent Secret investigations, have been reduced by approximately 2,000 cases from 2007 to 2009. She stated that it seems that the backlog was eliminated but the decrease in NACLC's is reciprocal to the increase in SSBIs, which require more time to complete.

She reported that the newly revised Standard Form 86 "Questionnaire for National Security Positions" (SF 86) was approved by the Office of Management and Budget and OPM was working to merge all the changes from the SF 86 into PIPS for scheduling and e-QIP for data collection by December 2010. Ms. Smith stated that this included the "branching questions," which were designed to gather more information on a subject's background to help the investigation move faster. She yielded to Merton Miller, OPM, on the changes in the Clearance Verification System (CVS). Mr. Miller stated that more options for data points relating to reciprocity have been added into the system to revise and streamline the process. He stated that the CVS is much more user friendly and easier to navigate. Frederick Riccardi, Industry, asked Mr. Miller about the process for reciprocity and electronic delivery of adjudications. Mr. Miller responded that the system was performing successfully and the only limitations that would occur were based on the agency capability for processing the electronic cases.

Ms. Branch provided metric data for DISCO adjudication inventory, which was from the end of first quarter FY 2008 through February 2010. She stated that the data reflected that there was an 80 percent reduction in the backlog of adjudication inventory for DISCO across this timeframe. She continued with metrics on industry cases with pending investigations at OPM and stated that there was a reduction of almost 60 percent in total pending inventory since the end of first quarter FY 2008. Scott Conway, Industry, asked about the steady state of DISCO. Ms. Branch responded that even with the current backlog DISCO is at a steady state and directed a question to Ms. Smith regarding the status of OPM's steady state. Ms. Smith responded that OPM has no backlog and was at a steady state. Mr. Riccardi commented that the overall reduction of submissions may be a result of certain defense programs being delayed or cancelled. The Chairman commented that the reduction in pending cases is a small portion of the overall

reduction in cases and that it was important to highlight the overall trend as well. Beth Patridge, Argon ST, asked whether the projected submissions were matching actual submissions. Drew Winneberger, DSS, responded that projected submissions were 18 percent higher than actual submissions, Shawn Daley, Industry, asked whether there was a backlog at the Defense Office of Hearings and Appeals. Ms. Branch was unable to give a definite answer. Mr. Conway stated that due to the short adjudication times most likely there would not be a backlog.

Ms. Branch moved to rejection rates for initial and periodic reinvestigations and noted a contrast between rejection rates from DISCO and from OPM. She stated that in this FY OPM's rejection rate has increased while DISCO's has decreased. She stated that the difference in the rejection rate would be closely monitored and added that 83 percent of OPM rejections were due to missing documents, specifically fingerprint cards. She stated that DISCO has many new people and it is possible that things were being caught by OPM that DISCO may have missed. Ms. Smith stated that, in the Joint Personnel Adjudication System (JPAS), the fax releases did not always transmit correctly. Finally, Ms. Branch provided the percentage of rejects based on the size of a company's cleared facility, which showed that smaller companies and facilities made up the majority of the rejections. The Chairman thanked Ms. Smith and Ms. Branch for their update and all those who participated in the working group.

B) Certification and Accreditation (C&A) Working Group Report[2]

David Cole, DSS, provided the C&A Working Group report. Mr. Cole stated that DSS is the government entity responsible for approving a cleared contractor's information systems. He stated that the Office of the Designated Approving Authority (ODAA) has been changing many of its processes and updating how things are done. He indicated that these improvements would be reflected in the metrics. He provided the average timeframe for plan reviews from March 2009 through February 2010. He commented that the current averages were most likely the norm for the foreseeable future and that most of the delays were from DSS, due to more time being spent on inspections of contractor facilities rather than processing security plans. Mr. Cole was asked whether the metrics could be divided by region, and he responded that this was possible and was already being provided to regional managers. Multiple questions were raised on the delay in reviewing security plans. Mr. Cole responded that the delay was due to a lack of staff and DSS planned to add 60 Information System Security Professional (ISSP) positions in the immediate future and 176 in the next several years. Vincent Jarvie, Industry asked if the 60 ISSPs were available in the current timeframe. Mr. Cole responded that the staffing plan was through 2013, but he hoped to have most onboard fairly quickly due to an increasing need.

Next, Mr. Cole provided metrics on the timeliness of granting Interim Approval to Operate (IATO) and reiterated that the average number of days would be fairly consistent as with the averages for processing security plans. He continued with metrics regarding on-site inspections after a system received an IATO and stated that there was a five percent increase in systems given an Approval to Operate (ATO) and a decrease in the

[2] See appendix 3 for Mr. Cole's presentation.

overall amount of discrepancies of systems. Nineteen percent of the systems were found to have discrepancies. Next, Mr. Cole provided metrics covering discrepancies found during on-site inspections that prevented granting an ATO. He stated that most discrepancies were related to the technical configuration requirements because the technical standard was released last year and most systems may not have been configured to the standard when the on-site inspection occurred. He commented that, in the next 180 days, there would be a significant difference in the type of discrepancies and that metrics would continue to improve. He stated that the lack of data reported from December 2009 and January 2010 was due to industry shutdowns from the holidays and time off. Finally, Mr. Cole presented metrics on the review of security plans and common errors found in plans. He stated that the most frequently found errors have been decreasing as a result of greater interaction between system managers and ISSPs and the use of templates provided by DSS to industry to draft plans. He also commented that DSS has a proposal to create an electronic system for the ODAA process that would address most of these errors before the review.

Ms. Patridge asked whether data was collected on Protection Level (PL) 1, PL-2, and PL-3. Mr. Cole responded that the ODAA system does not collect data in that manner. Sean Carney, Department of the Navy, asked whether violations were a result of security plans being poorly implemented and maintained after the approval of the plans or because more inspections were being conducted. Mr. Cole responded that the metrics represent the receipt of the security plan and on-site inspections. He stated that there is a review of the plans prior to annual on-site inspections and he could not comment on whether violations were increasing or decreasing, but speculated that, since there has been a significant focus and heightened awareness on security violations, the numbers may have increased. Sheri Escobar, Industry, raised concerns over the approval to sanitize systems that were used to process classified information and the difficulties faced in receiving approval from the ISSPs with regard to data spills. Mr. Cole responded that spills represented the majority of security violations and that, if a procedure was developed for contractors to address spills approved by the Government Contracting Activity/sponsor and it was included with the security plan, this would shorten the time period in receiving approval to sanitize the system. The Chairman commented that the challenges of consistency regarding information security during spills affect both Government and industry.

IV. New Business

The Chairman stated that, on December 29, 2009, the President issued Executive Order 13526, "Classified National Security Information" (CNSI) which replaces E.O. 12958, as amended. He stated that sections 1.7, 3.3, and 3.7 were effective immediately and the remainder of the Order is effective on June 27, 2010. He continued by stating that an administrative Executive Order regarding Original Classification Authority (OCA) delegations and a Presidential memorandum giving further direction for the implementation of the Order were also issued on December 29, 2009. He stated that the memorandum emphasized having agencies regularly update their regulations and security classification guides. He stressed that government agencies also need to provide updated guidance for contractors and their activities.

The Chairman specifically highlighted some major changes and impacts of the Order, which were as follows: derivative classifiers must be identified by name and position, or by personal

identifier, on each derivatively classified document, and they must receive periodic training on the use of classified markings; classified addenda or unclassified versions of documents must be used whenever possible to facilitate information sharing; documents derivatively classified from multiple sources must include a list of classified sources with the document. He further offered to the NISPPAC the opportunity to receive a more complete slide briefing presented by himself or members of ISOO, if requested. He stated that ISOO was required to issue a revision to the Order's implementing directive 32 C.F.R. Part 2001 (the Directive), which would be finalized before June 27, 2010. He stated that typically the Directive is not subject to public rulemaking process review due to the unique nature of the information conveyed and the urgency for implementation guidance. He assured the membership that there will be as much interagency coordination as possible.

The Chairman discussed Controlled Unclassified Information (CUI) reform and the establishment of the Presidential Task Force on CUI. He stated that the Task Force was chaired by the Department of Homeland Security and the Department of Justice, which produced 40 recommendations to the President and that there was an ongoing effort to draft an executive order for consideration by the President. He stated that there is a clear need for reform but there is no intention to require a clearance process, need-to-know, or non-disclosure agreements as with the classification system. Also, he expressed dismay over issuances and policies for CUI, such as the notion of a CUI need-to-know concept, being formulated by agencies before national guidance is issued. Finally, the Chairman discussed the ongoing effort to support State, Local, Tribal, and Private Sector entities that are not covered by the NISP but receive classified information to be brought fully into the policy framework. The Chairman yielded to Stephen Lewis, DoD, for his update on the National Industrial Security Program Operating Manual (NISPOM).

A) DoD Update

Mr. Lewis stated that significant changes have been proposed for the NISPOM to incorporate the concerns of industry members, NISP signatories, and to address the changes in E.O. 13526. He stated that the initial draft was being coordinated amongst NISP Cognizant Security Agencies and ISOO and the draft would be subsequently forwarded to the remainder of the NISPPAC for comment and review. Mr. Daley, Industry, asked if the draft would be forwarded on April 5 or later. The Chairman and Mr. Lewis jointly responded that it would take some time after April 5 to prepare the coordination draft for the remainder of the NISPPAC. Mr. Lewis stated that workshops and working groups would be held to discuss the changes and comments received and would be limited to NISPPAC members and/or their designees. Mr. Lewis continued, stating that DoD is working on a complete re-write of the Industrial Security Regulation (ISR), which will affect DoD Components and the other 23 agencies that use DoD industrial security services. Mr. Carney asked for clarification on the difference between the NISPOM and NISP Manual, Volume 2. Mr. Lewis explained that, due to changes in DoD standards for publications, the NISPOM, which levies security requirements on cleared contractors, will be redesignated as the NISP Manual, Volume 1, and the ISR, which provides required industrial security procedures for government activities, will be issued as NISP Manual Volume 2.

B) Combined Industry Presentation[3]

Mr. Jarvie provided the Combined Industry Presentation. He thanked all the members involved in the NISP, the Industrial Security Working Group, and various associations, for their constant hard work in the past months. Mr. Jarvie thanked and recognized Ms. Smith for her contributions to the NISPPAC. Mr. Jarvie stated that industry is committed to the laws and regulations that govern the NISP, the partnership between industry and Government, and he was pleased that industry was and will be solicited for comments and responses to revisions to the NISPOM. Mr. Jarvie yielded to Mr. Riccardi over industry concerns about the Federal Acquisitions Regulation (FAR). Mr. Riccardi stated that industry would like to see a single FAR clause that would address industry concerns about information security and CUI. He stressed that reciprocity needs to take place in the information-sharing environment and that a single universal training package for all users should be accepted and implemented. Mr. Jarvie stated that industry is working to create a single level of uniform information sharing through the Defense Industrial Base Sector Coordinating Council and the Defense Security Information Exchange (DSIE). He thanked Mr. Riccardi and continued, stating that the Federal Bureau of Investigation (FBI) would sponsor industry access to the Secret Internet Routing Protocol Network (SIPRNET). He commented that the Defense Federal Acquisition Regulation Supplement on safeguarding unclassified information would be under the public rulemaking process and a public meeting would be held on April 22, 2010.

Mr. Jarvie stated that many agencies require industry to print copies of an employee's JPAS records in order to gain access to an installation or special access program, and according to Industrial Security Letter (ISL), 2010-01 industry was prohibited from printing and releasing these records. Richard Hohman, Office of the Director of National Intelligence (ODNI) responded that ODNI would have to know which government activities were requiring this. Mr. Lewis reiterated that it was also contrary to DoD policy for agencies to require the printing of an employee's JPAS record. The Chairman commented that it may be a site-specific issue, and Mr. Lewis asked industry representatives to provide specific examples to allow DSS and DoD to address the issue. A question was raised as to how NISPPAC members can be better notified when an ISL was going to be released. Subsequent to the meeting, DoD, DSS and ISOO developed a process to allow NISPPAC members to comment on ISLs prior to issuance.

C) Cyber Intrusion Reporting[4]

Mike Gordon, Industry presented on the DSIE and ISL 2010-02 on reporting requirements for cyber intrusions. Mr. Gordon stated that the DSIE is a collaborative environment that shares threat information developed under the same auspices as the Network Security Information Exchange. He stated that there were two levels of information sharing in the DSIE: strategic and tactical. He stated that the recent ISL expands reporting under NISPOM 1-301. He is concerned that industry would be reporting hundreds of thousands of events under the ISL, rather than focusing on those that provide valuable information to those who need it. He stated that industry was working on interpreting the ISL so adverse threat information reporting was achieved

[3] See appendix 4 for Mr. Jarvie's presentation.
[4] See appendix 5 for Mr. Gordon's presentation.

without reporting every minor event. He commented that there is not a secure communication path from industry to the FBI and DSS, which negatively affects the ability of those entities to do their jobs. Also, he stated that ISL 2010-02 was focused more on the corporate information security officer rather than the traditional relationship with facility secure clearance officers; so, industry is building a data flow processes to ensure that information moves quickly and accurately to the necessary parties. Finally, he stated that smaller companies are greatly impacted by this ISL since they do not possess the same amount of expertise, technical capability, or financial resources as the larger companies.

V. General Open Forum/Discussion

Mark Leavitt, FBI, discussed the issue of the insider threat from hiring individuals that do not require a security clearance. He specifically discussed the need for greater "due diligence" with regard to receiving information on the previous employment of people terminated as a result of security violations when those individuals seek employment with another company. He asked whether or not something could be done to improve the process to surface this type of information so that companies were not hiring people with a history of security violations. Mr. Riccardi responded that, when the CUI policy is finalized, a process similar to the Personnel Reliability Program may be developed to address this issue. Gina Otto, ODNI, responded that it is an issue within the hiring process. William Marosy, OPM, responded that there is less and less cooperation from private sector entities to assist in suitability investigations.

VI. Closing Remarks and Adjournment

The Chairman stated that the next two NISPPAC meetings are scheduled for Wednesday, July, 21, 2010, and Wednesday, November 17, 2010, from 10:00 a.m. to 12:00 p.m. He expressed his sincere thanks to all. The meeting was adjourned at 11:56 a.m.

List of Appendices

Appendix 1 – Ms. Smith's PCL Working Group Report Presentation
Appendix 2 – Ms. Branch's PCL Working Group Report Presentation
Appendix 3 – Mr. Cole's C&A Working Group Report Presentation
Appendix 4 – Mr. Jarvie's Combined Industry Update Presentation
Appendix 5 – Mr. Gordon's Cyber Intrusion Reporting Presentation

Appendix 1
Ms. Smith's PCL Working Group Report Presentation

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

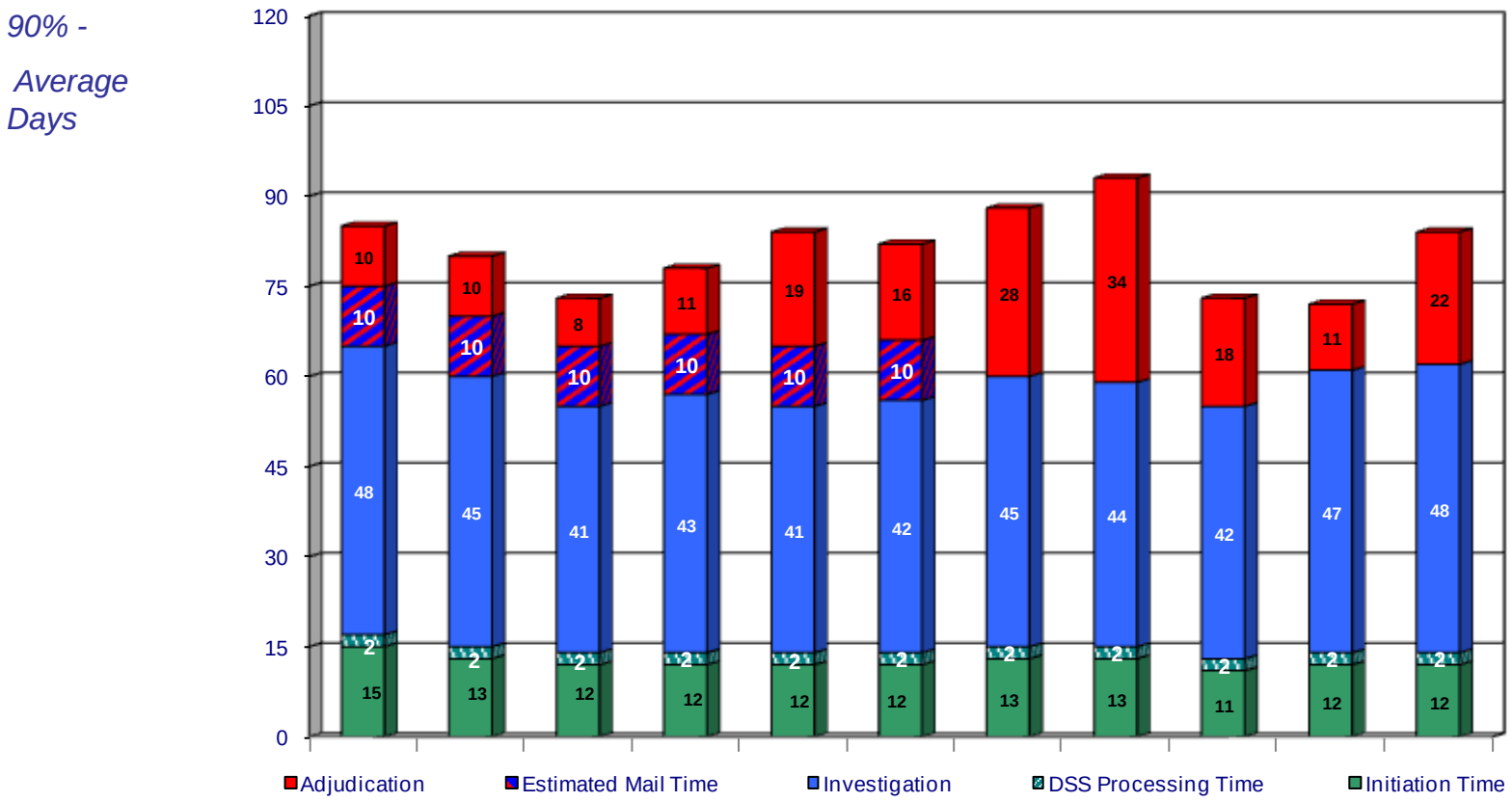
Reported Clearance Decisions Made During the 1st Qtr FY 10

- All levels of Initial clearances – 31,439 cases average 99 days End-to-End time (Initiation through Adjudication)
  - Fastest 80% average 71 days
  - Fastest 90% average 78 days
    - Top Secret Initial – All 6,709 cases: 134 day average cycle time
      - » Fastest 80% average 107 days
      - » Fastest 90% average 114 days
    - All Secret/Conf – All 24,730 cases: 89 day average cycle time
      - » Fastest 80% average 64 days
      - » Fastest 90% average 69 days
- TS Periodic Reinvestigation – All 5,360 cases: 149 day average cycle time
  - Fastest 80% average 104 days
  - Fastest 90% average 114 days

***The adjudication timelines include collateral adjudication by DISCO and SCI adjudication by other DoD adjudication facilities**

Data reflective of reported adjudicative decisions as of January 4, 2010

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

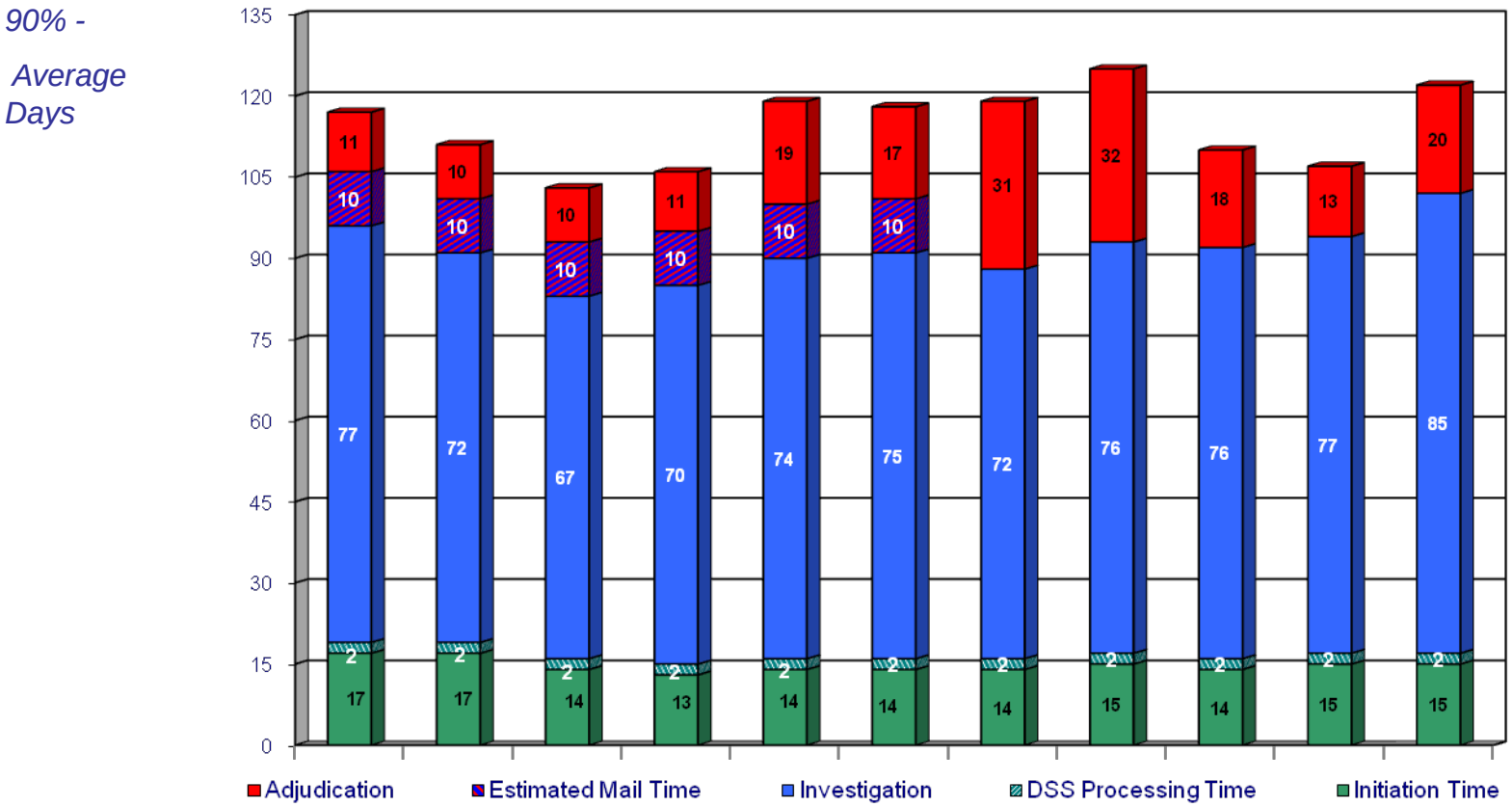


* - 10 day estimated mail time removed in September 2009 as Industry began eDelivery on August 20, 2009

Adjudications actions taken:	Mar 09	Apr 09	May 09	Jun 09	Jul 09	Aug 09	Sept 09	Oct 09	Nov 09	Dec 09	Jan 10
100% of Reported Adjudications:	12,957	10,577	10,059	9,470	9,582	10,324	9,624	9,352	12,738	9,350	7,604
Average Days for the fastest 90%	85 days	80 days	73 days	78 days	84 days	82 days	88 days	93 days	73 days	72 days	84 days

Slide has been updated with reported adjudicative decisions made during September 2009 through January 2010. Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested. The time span for the rejections may not be included in the above metrics

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

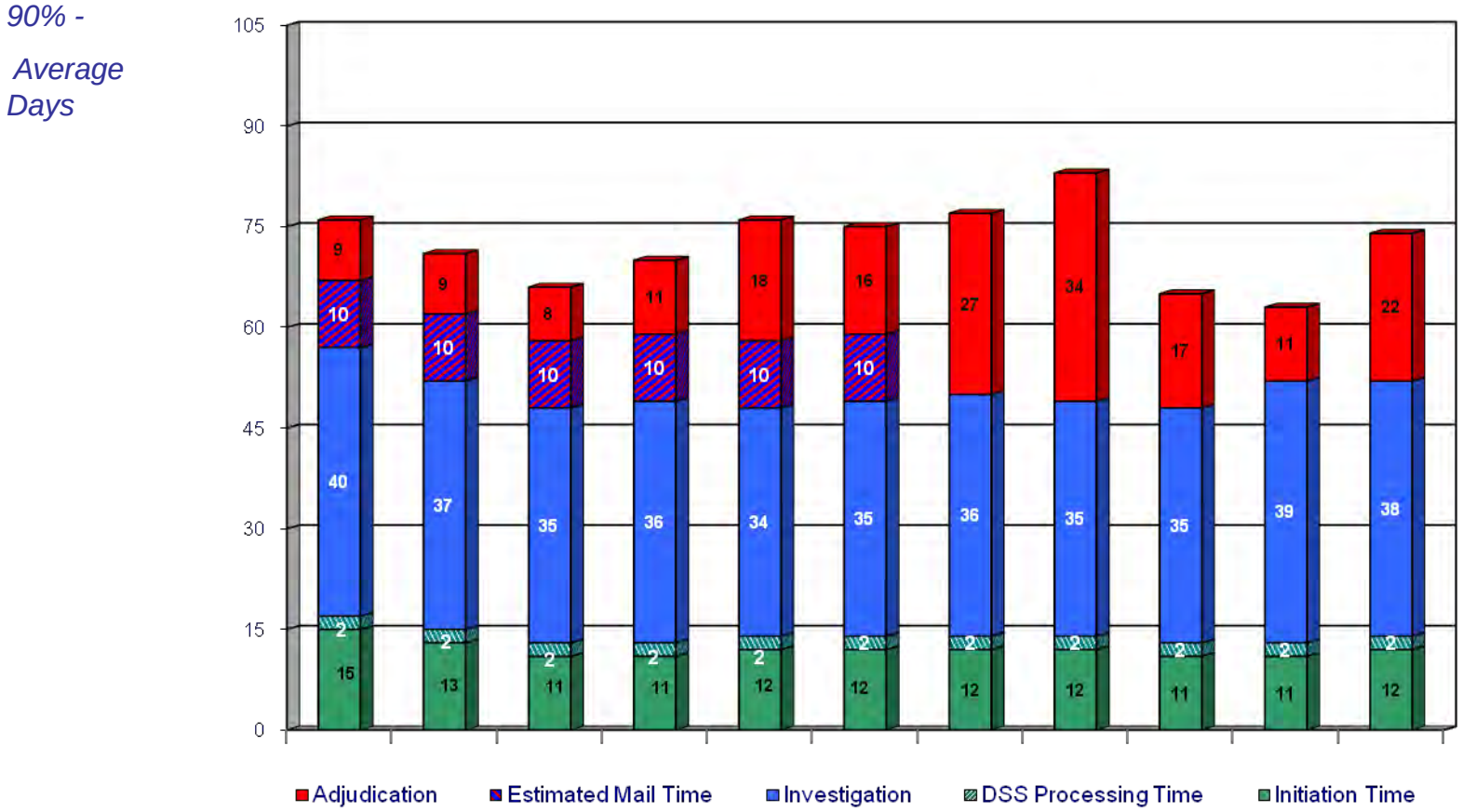


* - 10 day estimated mail time removed in September 2009 as Industry began eDelivery on August 20, 2009

Adjudications actions taken:	Mar 09	Apr 09	May 09	Jun 09	Jul 09	Aug 09	Sept 09	Oct 09	Nov 09	Dec 09	Jan 10
100% of Reported Adjudications:	3,092	2,409	2,136	1,998	1,873	1,936	2,467	2,225	2,454	2,028	1,641
Average Days for the fastest 90%	117 days	111 days	103 days	106 days	119 days	118 days	119 days	125 days	110 days	107 days	122 days

Slide has been updated with reported adjudicative decisions made during September 2009 through January 2010. Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested. The time span for the rejections may not be included in the above metrics

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

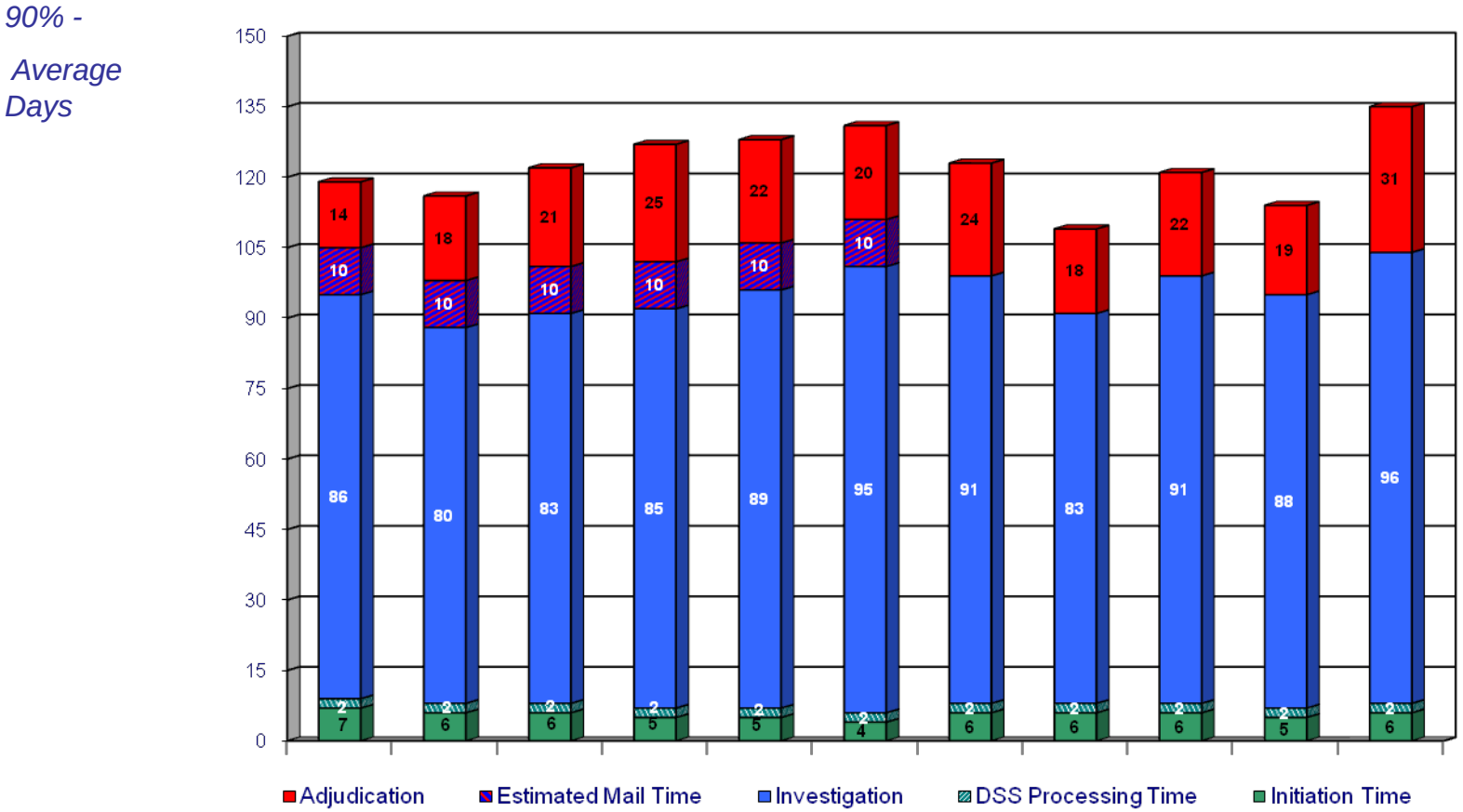


* - 10 day estimated mail time removed in September 2009 as Industry began eDelivery on August 20, 2009

Adjudications actions taken:	Mar 09	Apr 09	May 09	Jun 09	Jul 09	Aug 09	Sept 09	Oct 09	Nov 09	Dec 09	Jan 10
100% of Reported Adjudications:	9,865	8,168	7,923	7,472	7,709	8,388	7,157	7,127	10,284	7,322	5,963
Average Days for the fastest 90%	76 days	71 days	66 days	70 days	76 days	75 days	77 days	83 days	65 days	63 days	74 days

Slide has been updated with reported adjudicative decisions made during September 2009 through January 2010. Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested. The time span for the rejections may not be included in the above metrics

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



* - 10 day estimated mail time removed in September 2009 as Industry began eDelivery on August 20, 2009

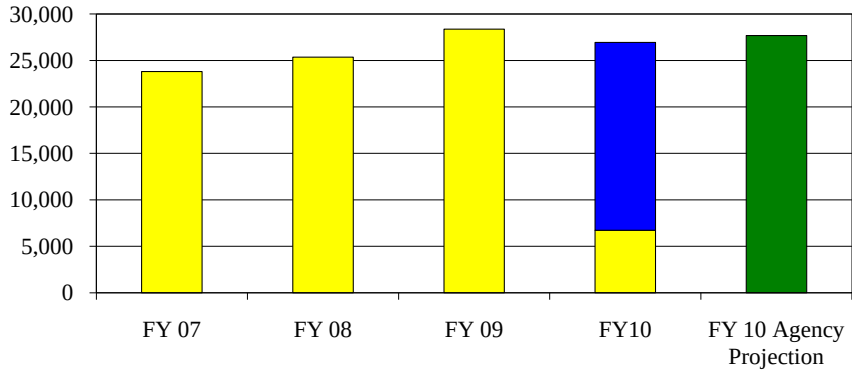
Adjudications actions taken:	Mar 09	Apr 09	May 09	Jun 09	Jul 09	Aug 09	Sept 09	Oct 09	Nov 09	Dec 09	Jan 10
100% of Reported Adjudications:	3,729	2,210	1,891	1,812	1,989	2,063	2,419	2,206	1,486	1,602	1,322
Average Days for the fastest 90%	119 days	116 days	122 days	127 days	128 days	131 days	123 days	109 days	121 days	114 days	135 days

Slide has been updated with reported adjudicative decisions made during September 2009 through January 2010. Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested. The time span for the rejections may not be included in the above metrics

DISCO Scheduled Trends

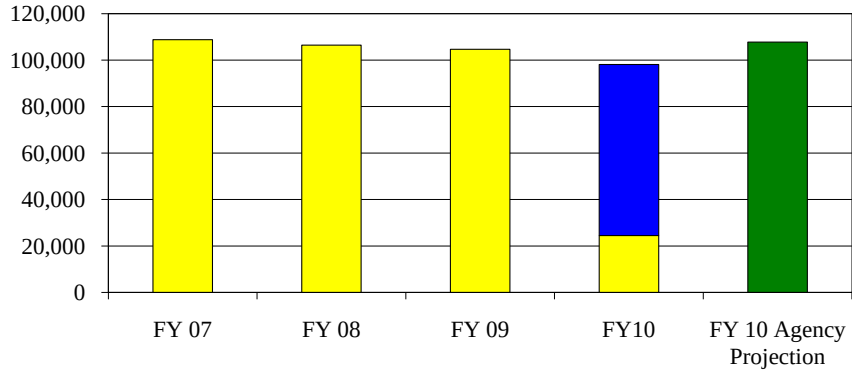
Single Scope Background Investigation (SSBI)

FY 07:	**23,805**
FY 08:	**25,363**
FY 09:	**28,375**
***FY 10:**	**6,735**
OPM est. FY10:	**26,940**
Agency proj. FY10:	**27,674**
Variance:	**-3%**



National Agency Check with Law and Credit (NACLC)

FY 07:	**108,772**
FY 08:	**106,445**
FY 09:	**104,638**
***FY 10:**	**24,528**
OPM est. FY10:	**98,112**
Agency proj. FY10:	**107,769**
Variance:	**-9%**



**** FY 10 data complete as of 12/31/09- 25% of the year elapsed***

FY 10 flat line projection for the remainder of the current fiscal year

Appendix 2
Ms. Branch's PCL Working Group Report Presentation

DISCO

FY10 ADJUDICATION INVENTORY

CASE TYPE	FY 08				FY 09				FY 10		Delta Q1 FY08 vs Feb FY10
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Feb-10	
NACLC	11,449	488	240	1,953	4,721	1,815	4,187	7,292	1,411	4,372	-62%
SSBI	9,337	5,625	30	354	1,448	634	1,102	1,608	450	1,389	-85%
SSBI-PR	4,899	3,752	5,973	757	974	340	756	488	123	516	-89%
Phased PR	8,945	4,923	4,210	330	1,690	495	346	208	53	581	-94%
Total Pending	**34,630**	**14,788**	**10,453**	**3,394**	**8,833**	**3,284**	**6,391**	**9,596**	**2,037**	**6,858**	**-80%**

Overall reduction of 80% for NACLC, SSBI, SBPR and Phased PR case types from Q1 FY08 to Feb FY10.

Source: DISCO Manual Counts

INDUSTRY CASES AT OPM

FY10 INVESTIGATION INVENTORY

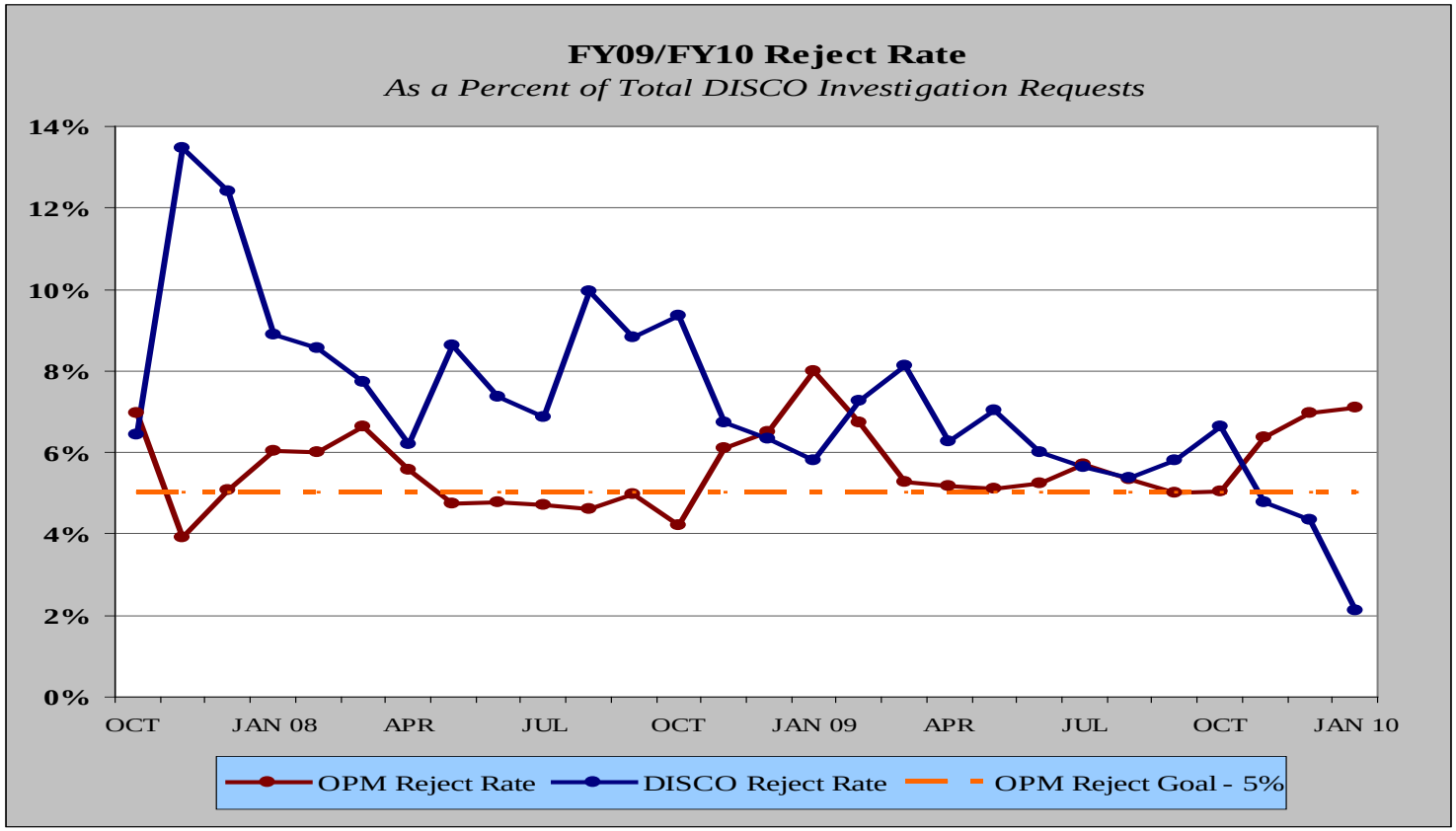
Case Type	FY 08				FY 09				FY 10		Delta Q1 FY08 vs Feb FY10
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Feb-10	
NACLC	29,575	25,085	22,077	15,561	13,209	13,982	13,900	12,307	11,730	11,616	-61%
SSBI	14,110	8,796	7,404	6,720	6,626	6,687	6,944	6,561	6,782	6,542	-54%
SSBI-PR	11,761	9,943	5,639	4,167	3,772	4,160	4,692	3,703	4,096	4,336	-63%
Phased PR	7,711	7,749	6,734	6,408	5,430	2,771	2,476	2,640	3,158	3,402	-56%
Total Pending	**63,157**	**51,573**	**41,854**	**32,856**	**29,037**	**27,600**	**28,012**	**25,211**	**25,766**	**25,896**	**-59%**

Overall reduction of 59% for NACLC, SSBI, SBPR and Phased PR case types from 1Q FY08 to Feb FY10.

Source: OPM Customer Support Group

REJECT RATE

Initial and Periodic Reinvestigation Requests



- **FY10 (close of January): DISCO received 49,116 investigation requests**
  - **Rejects –** A total of **5,614 (11.4%)** of incoming investigation requests rejected back to FSOs
    - DISCO rejected **2,505 (5.1%)** investigation requests to FSOs for re-submittal
    - OPM rejected **3,109 (6.3%)** investigation requests to DISCO (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.

Source: JPAS / OPM IRTPA Monthly Reports

REJECTS

DISCO Front-End Statistics

Facilities where rejects most often occur – October 09 through January 10

- Smaller Category D / Non-possessing Category E / NACLC
  - *Percent of overall case rejections by facility category and case type*

	NACLC	SSBI	TSPR	Overall % by Category
A/AA	*7%*	*7%*	*7%*	*7%*
B	*4%*	*6%*	*7%*	*5%*
C	*5%*	*8%*	*13%*	*7%*
D	***29%***	***24%***	***33%***	***29%***
E	***55%***	***55%***	***38%***	***52%***
	100%	*100%*	*100%*	*100%*

Appendix 3
Mr. Cole’s C&A Working Group Report Presentation

Defense Security Service

Industrial Security Field Operations Office of the

Designated Approving Authority (ODAA)

March 2010

Defense Security Service

Overview

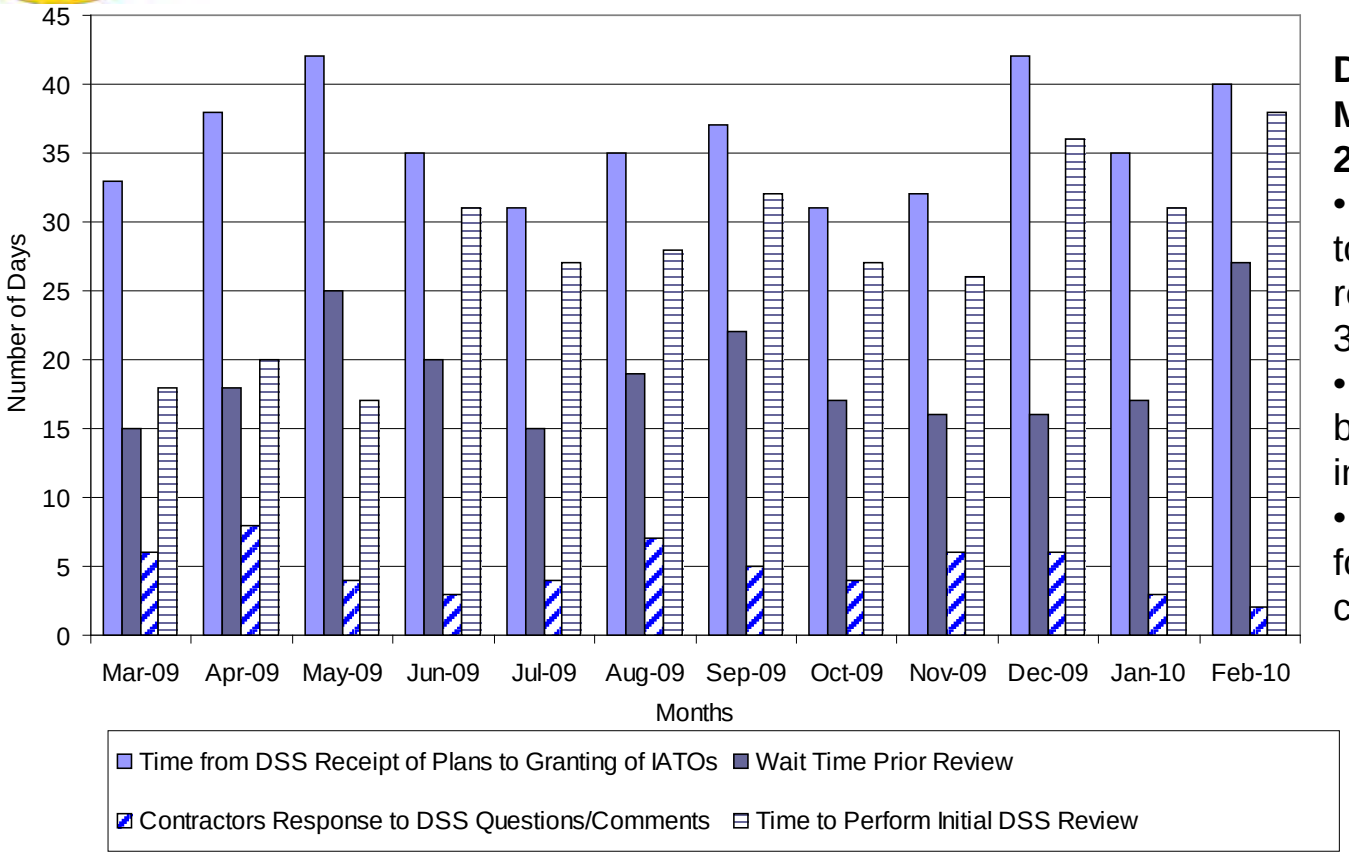
- Certification & Accreditation (C&A)
- C&A Metrics

Certification & Accreditation

- DSS is the Government entity responsible for approving cleared contractor information systems to process classified data.
- Ensures information system security controls are in place to limit the risk of compromising national security information.
- Provides a system to efficiently and effectively manage a certification and accreditation process.
- **Ensures adherence to national industrial security standards.**

ODAA Improving Accreditation Timeliness and Consistency

ODAA Metrics for # Days to Process Plan Submissions

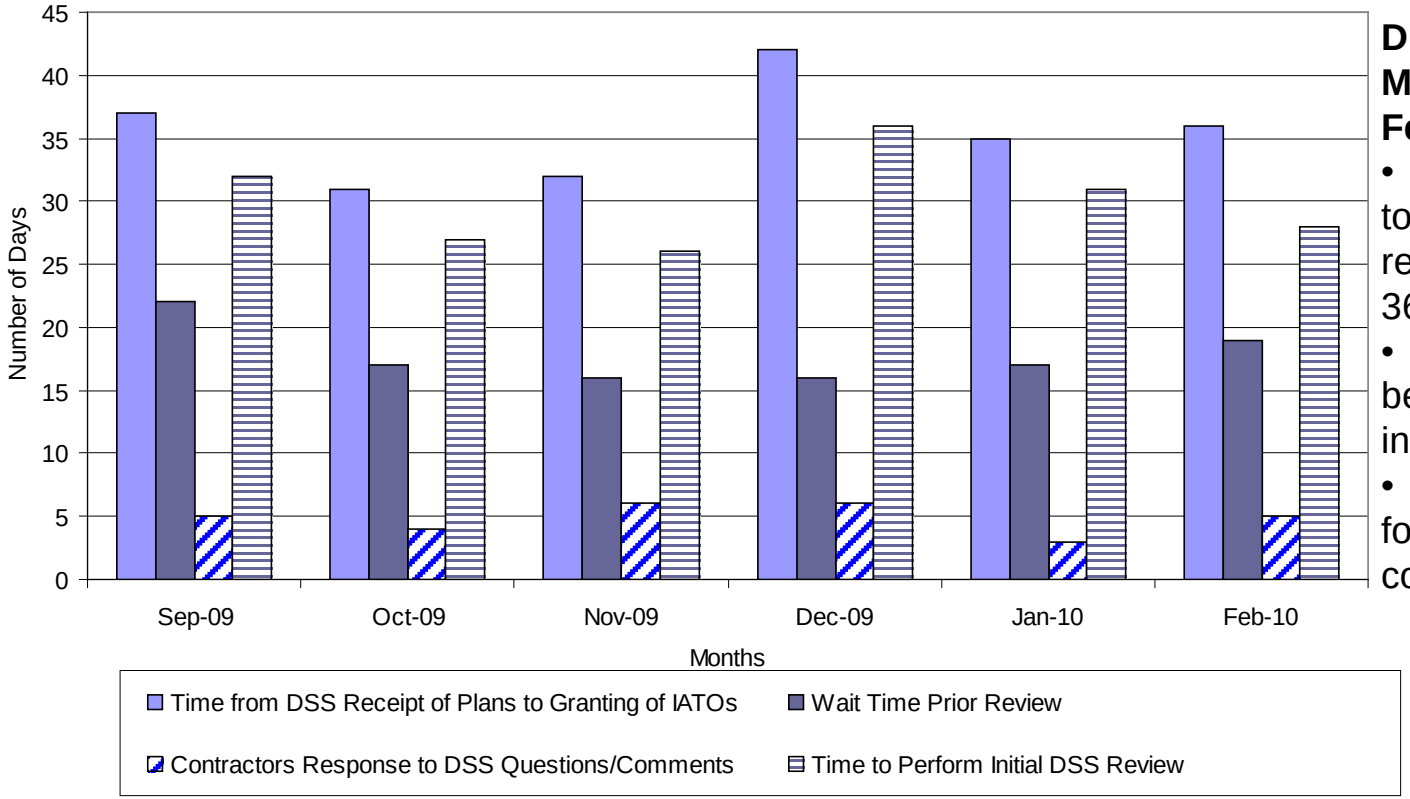


During the Past Year March 2009 – February 2010

- Average number of days to receive an IATO after receipt of a submission is 36 Days
- Average waiting time before a review process is initiated is 19 Days
- Average number of days for the review time to be completed is 28 Days

ODAA Improving Accreditation Timeliness and Consistency

ODAA Metrics for # Days to Process Plan Submissions

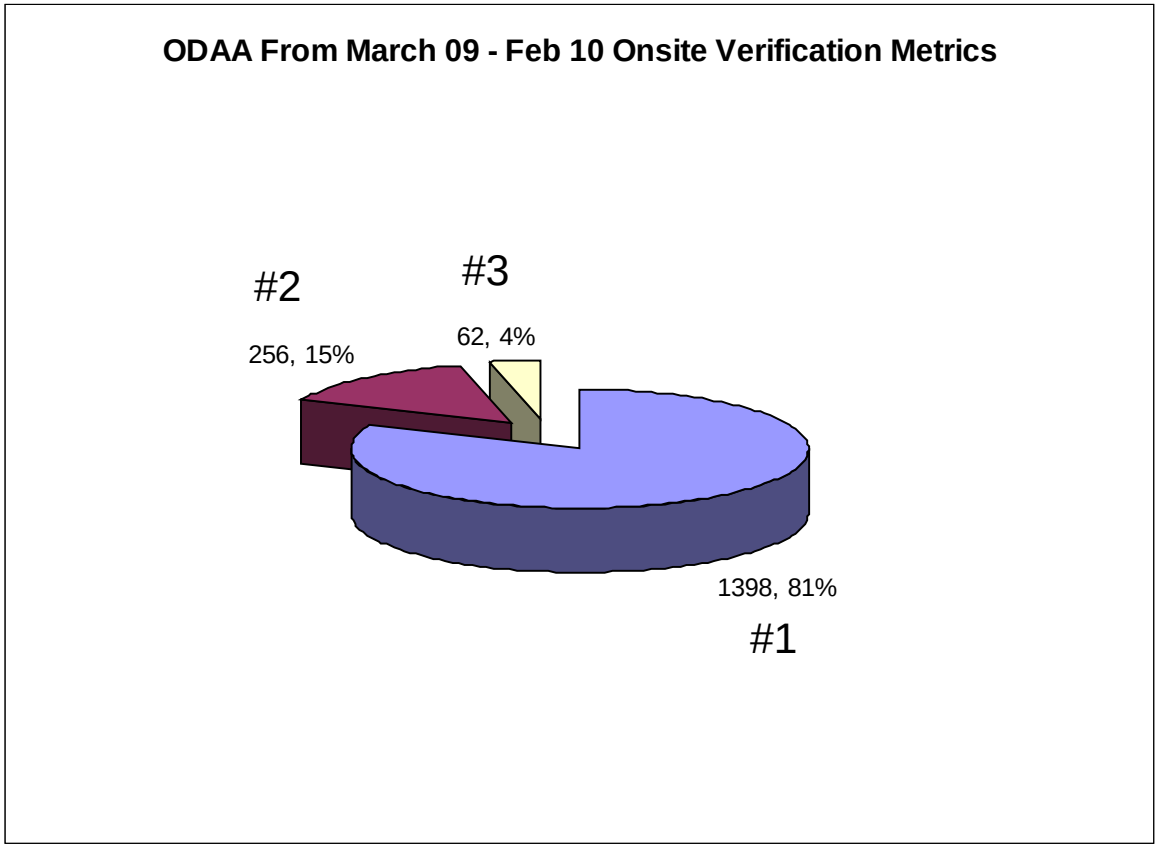


During the Past Six Months Sept 2009 – February 2010

- Average number of days to receive an IATO after receipt of a submission is 36 Days
- Average waiting time before a review process is initiated is 18 Days
- Average number of days for the review time to be completed is 30 Days

ODAA Metrics and Organization

On-site Verification Stats (15% Required Some Level Modifications)

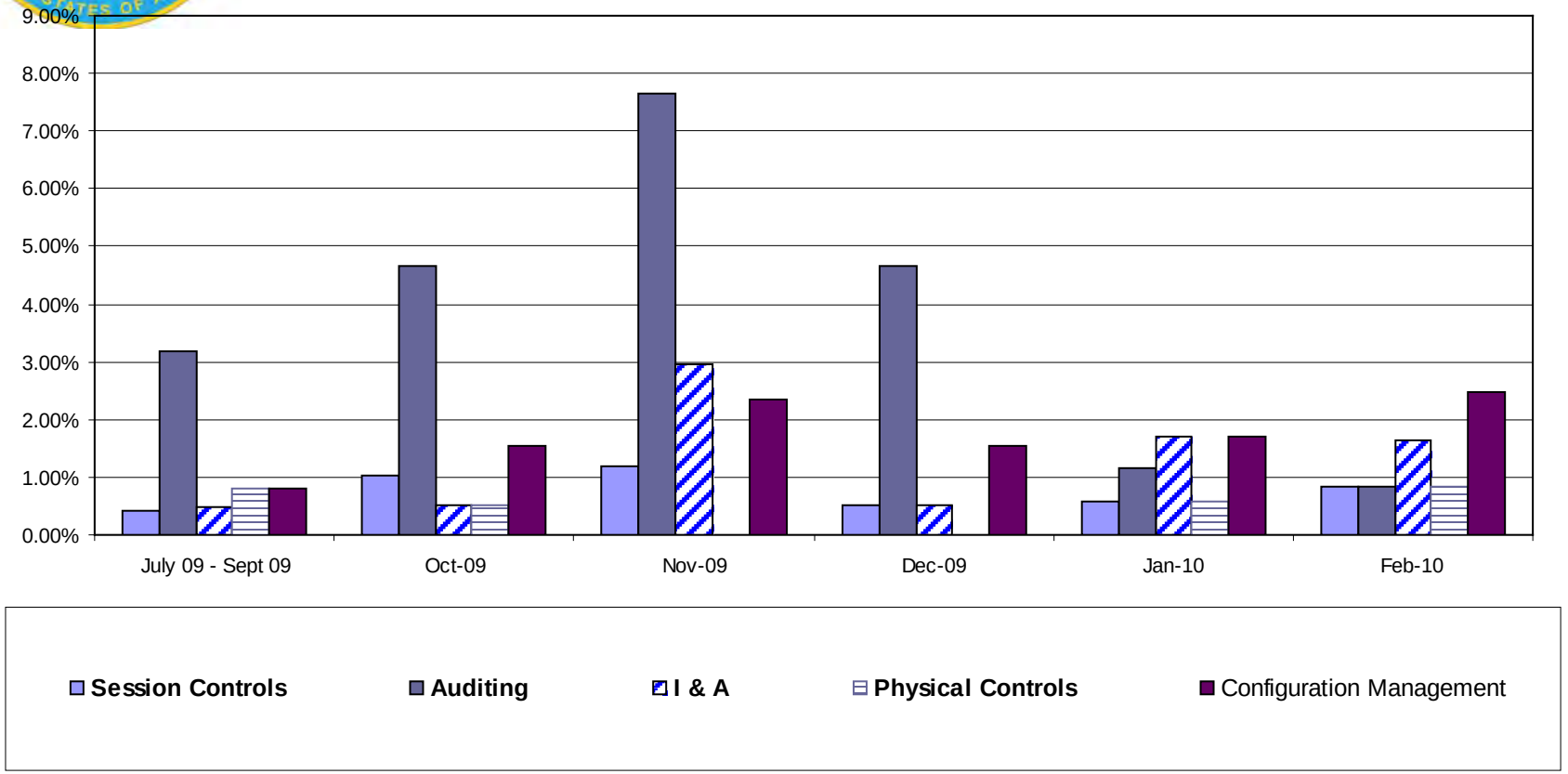


#1. No discrepancies discovered during on-site validation.

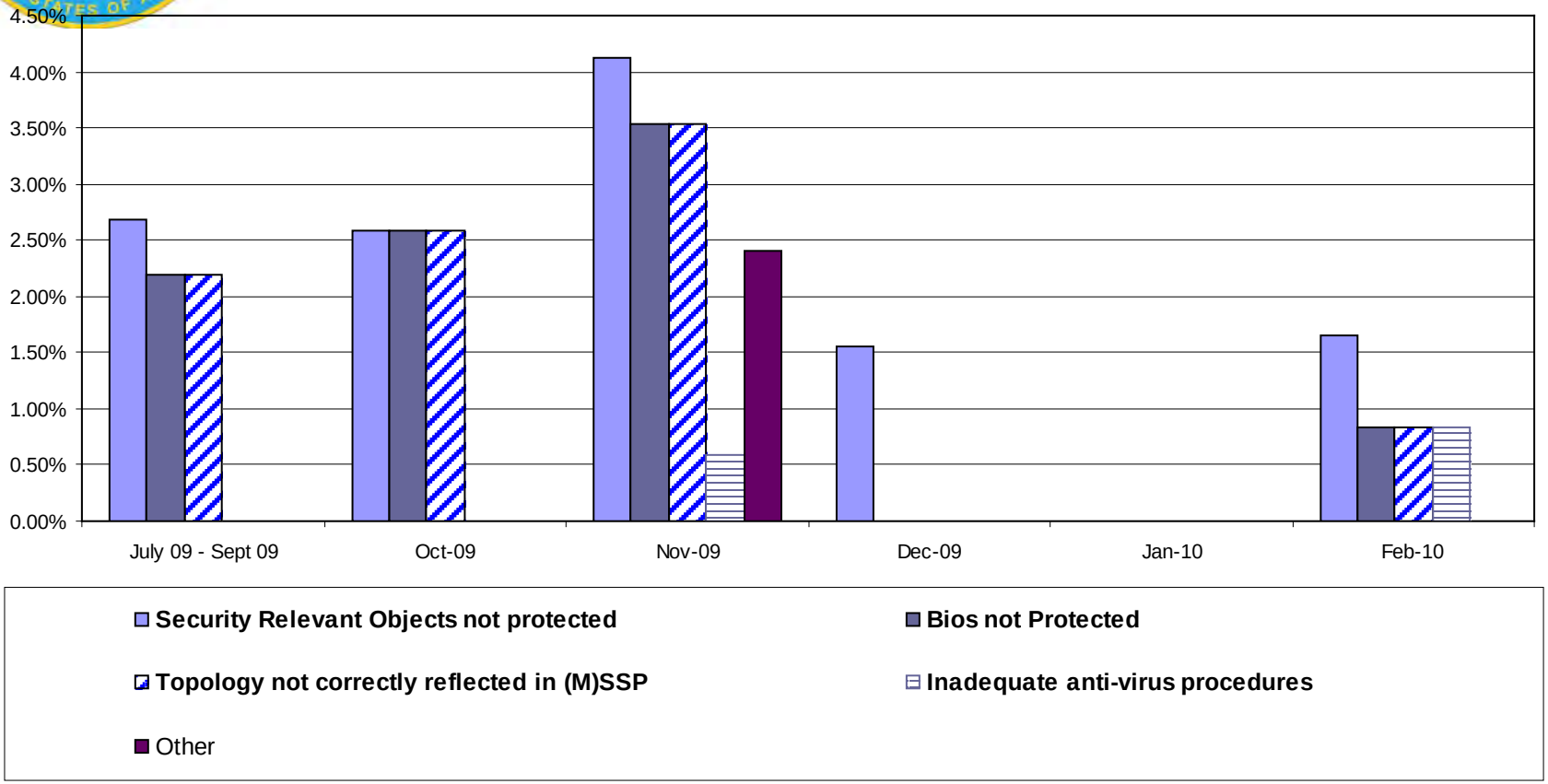
#2. Minor discrepancies noted and corrected during on-site validation.

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

ODAA Metrics
Onsite Plan Reviews Discrepancies
Part One

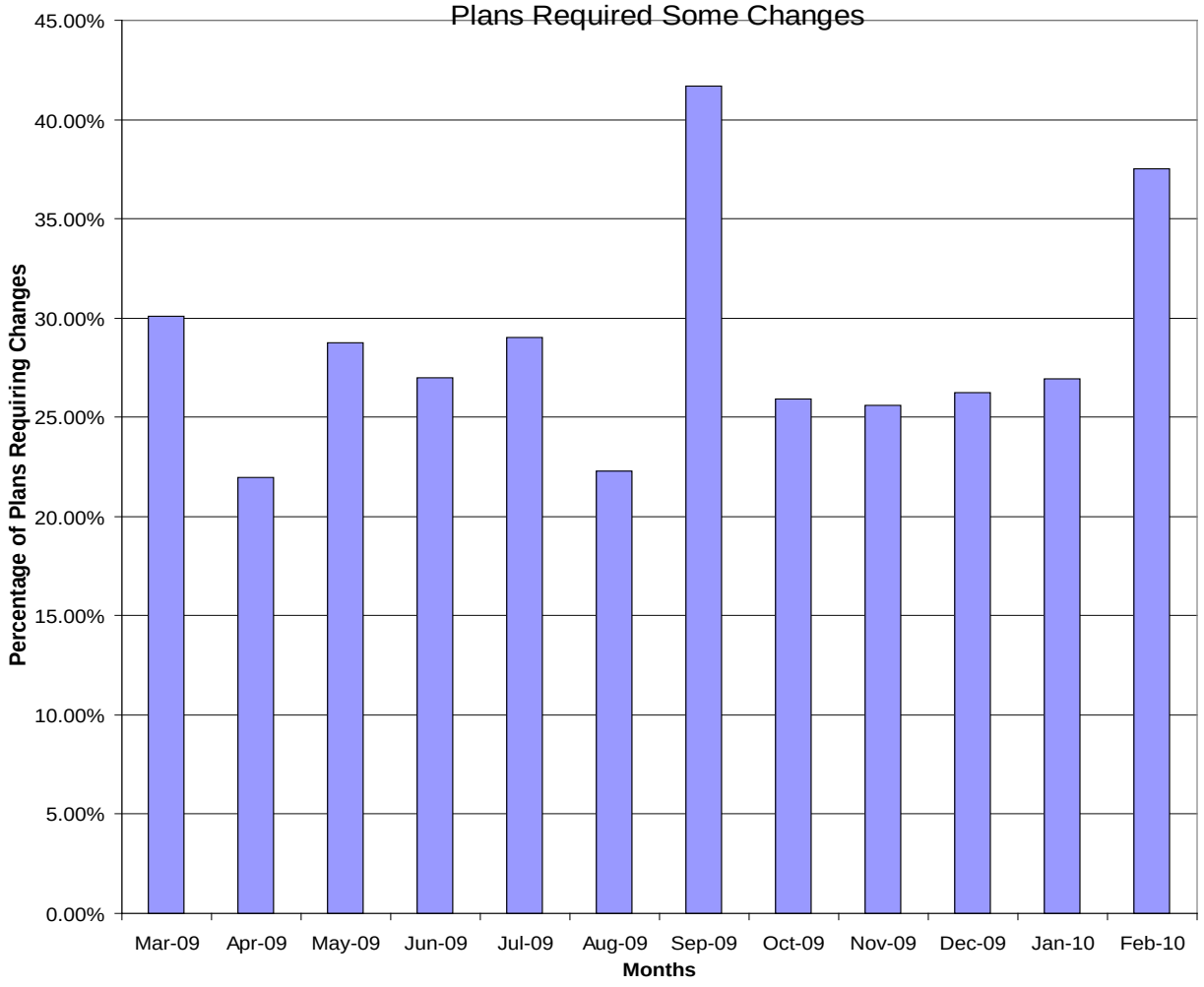


ODAA Metrics
Onsite Plan Reviews Discrepancies
Part Two



ODAA Metrics
Security Plan Reviews

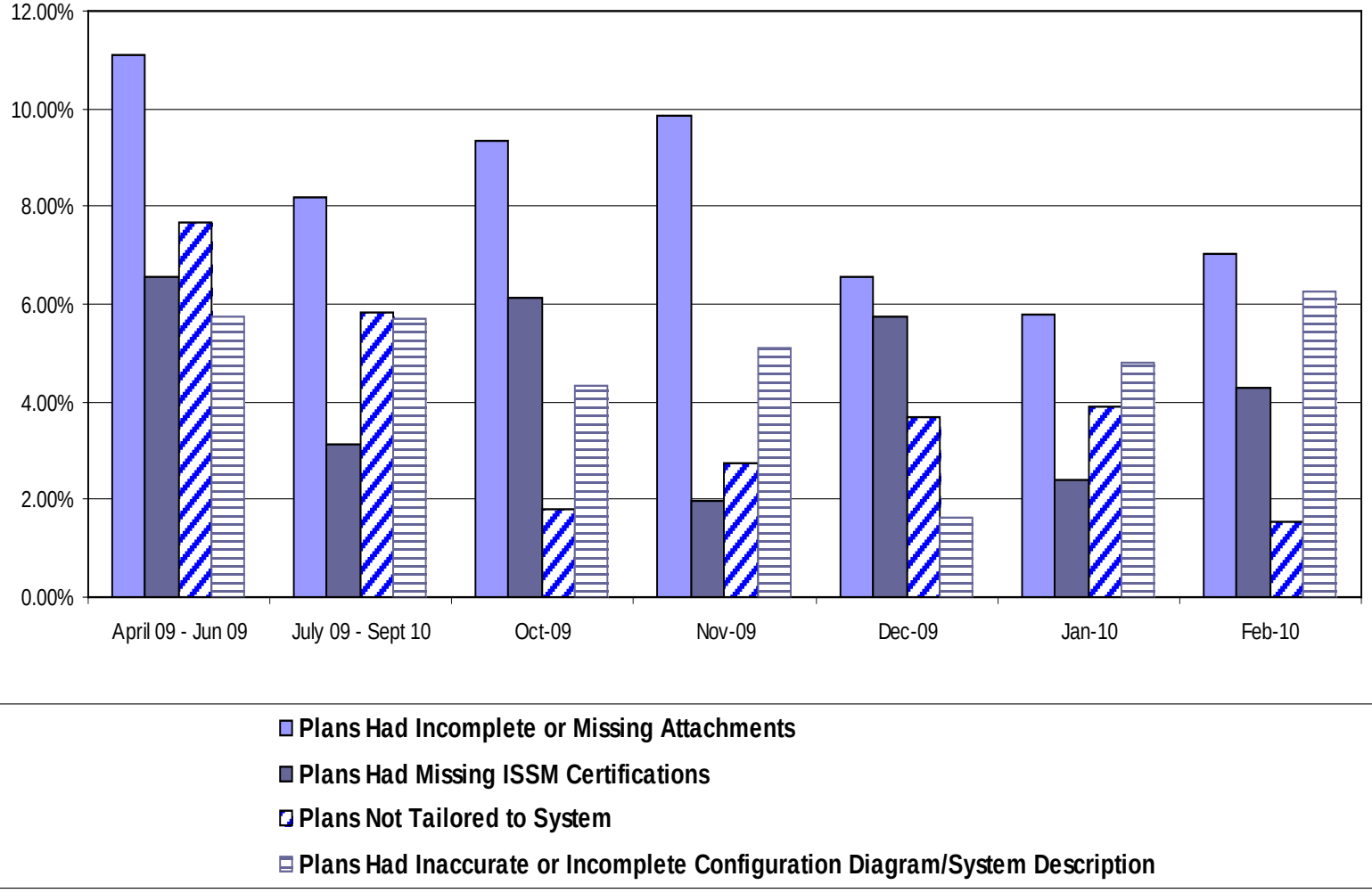
Review Questions and/or Comments, Errors and Corrections Noted



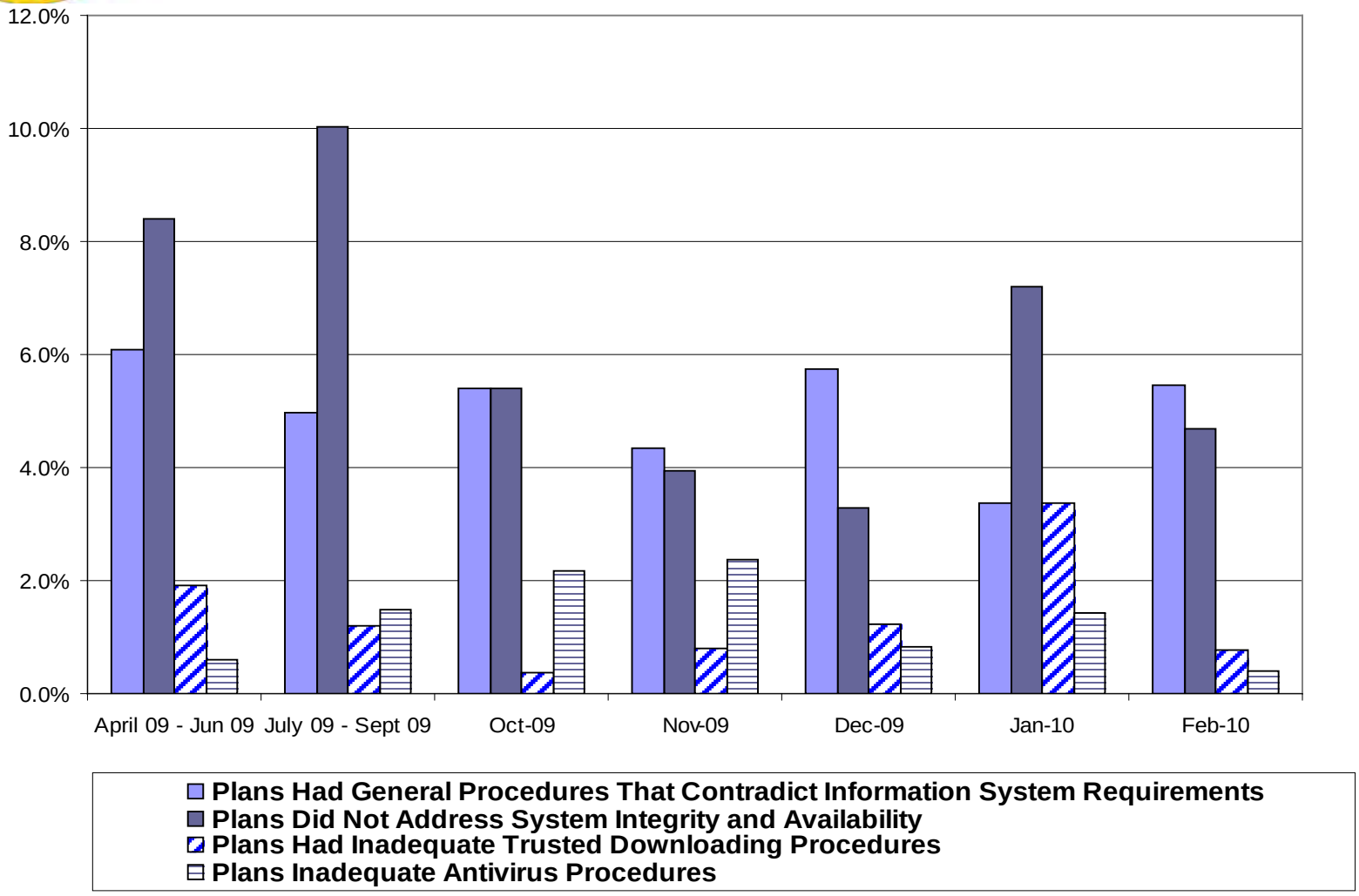
Of the 2400 plans received from Mar 09 – Feb 2010:

- On average 28.57% 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



Appendix 4
Mr. Jarvie’s Combined Industry Update Presentation

NISPPAC
Industry Presentation

24 March 2010

Industry Members/NISPPAC

Member	Company	Term Expires
“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
Frederick Riccardi	ManTech	2013
Shawn Daley	MIT Lincoln Labs	2013

Industry Members/MOU

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

NISPPAC Ad Hoc Working Groups

- Personnel Security Clearance Processing
  - Consistent and synchronized metrics
  - Process for continuous improvement
- Certification & Accreditation
- Foreign Ownership Control & Influence (FOCI)

NISPPAC

- National Industrial Security Program Operating Manual – revision by USG in progress
  - August 27th 2009 – Initial discussion with Industry
    - Hosted by the ISOO
    - General outline of topics provided by OSD
    - Industry provided results of data call
      - Numerous items for consideration provided to USG
      - Industry working priorities

NISPPAC

- National Industrial Security Program Operating Manual – revision by USG in progress
  - Industry review of revised language
    - Time period for review
    - Assess Impact
    - Coordinate and provide comments

NISPPAC

(Industry concerns 15 May 2008/ 20 November 2008/ 07 April 2009/ 22 July 2009/ 8 October 2009)

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

Information Sharing - Threat

Institutionalized Process:

- Information
- Communication methodology
- Feedback

Proposed Defense Federal Acquisition Regulation

- DFARS 252.204–7XXX, Basic Safeguarding of Unclassified DoD
- Information Within Industry & DFARS 252.204–7YYY, Enhanced
  - Safeguarding and Cyber Intrusion Reporting of Unclassified DoD Information Within Industry
- Safeguarding requirements apply to any unclassified DoD information that has not been cleared for public release
- Includes cyber incident reporting for information subject to the following:
  - Critical program information
  - ITAR & EAR requirements
  - FOIA Exempt & FOIA withheld information
  - CUI &PII
- Will multiple contract requirements proliferate across government resulting in inconsistent policies, safeguarding standards and increased costs within government and industry?

Policy – Industrial Security Letters (ISLs)

- ISL 2010-01 January 28, 2010
  1. (NISPOM 1-204) Cooperation with Federal Agencies and Officially Credentialed Representatives of Those Agencies.
  5. (NISPOM 6-104a) Release of JPAS records.

Policy – Industrial Security Letters (ISLs)

- ISL 2010-02 February 22, 2010
  - Reporting Requirements for Cyber Intrusions (NISPOM 1-301)

Appendix 5
Mr. Gordon’s Cyber Intrusion Reporting Presentation

DEFENSE INDUSTRIAL BASE

CRITICAL INFRASTRUCTURE PROTECTION

SECTOR COORDINATING COUNCIL

Defense Security Information Exchange (DSIE)

NISPPAC on ISL 2010-2

Reporting Requirements for Cyber Intrusions

DIB
DEFENSE INDUSTRIAL BASE
CRITICAL INFRASTRUCTURE PROTECTION
SECTOR COORDINATING COUNCIL

DSIE Concept of Operations

- DSIE formed using the same CONOPS as the Network Security Information Exchange NSIE
- The DSIE is the information sharing organization for the DIB to collectively share cyber threat and warning information between members of the DIB SCC. The Strategic Committee works with the SSA on the SSP and other Strategic Cyber issues
- The DSIE organizationally is an industrial committee of the NDIA. As such, it acts as the Cyber Sub-Council of the DIB Sector Coordinating Council.
- Information sharing should be on two levels
  - Strategic (higher level, policy issues)
  - Tactical (near real time threat and warning sharing)

DIB
DEFENSE INDUSTRIAL BASE
CRITICAL INFRASTRUCTURE PROTECTION
SECTOR COORDINATING COUNCIL

Membership in the DIB SCC

- Open to any existing industry association member predominately representing significant defense industrial base business interests. “Core” member associations include
  - Aerospace Industries Association (AIA)
  - American Society for Industrial Security (ASIS)
  - Industrial Security Working Group (ISWG)
  - National Classification Management Society (NCMS)
  - National Defense Industrial Association (NDIA)
- Council members must possess an authoritative knowledge of defense industrial base industrial capabilities and infrastructure protection requirements
- The DSIE Strategic Committee members must be members of the NDIA.

ISL Changing Roles & Responsibilities

- ***Drives far more reporting then originally intended by NISPOM 1-301***
  - **Large expansion into Unclassified data**
- ***Requires APT attribution by CDCs***
- ***Centralized Secure Incident Handling / Communication Processes***
- ***Shifts Industry interface to FSOs from CISO & CIRT***

Reporting Sample per CDC
24 hour period: **• 90K+ scan events** **• 40K+ pdf files** **• 2M spam** ***20K man hours without substantial automation***

DSIE Position

- **ISL impacts incident reporting**
  - **FBI advises reporting based items which lead to prosecution**
  - **Data requires incident filtering**
  - **Impact to small suppliers**
- **Industry provides unclassified protection through enterprise mechanisms**
  - **Contractual**
  - **Shareholder value**
  - **Employee privacy**
- **Effective collaborative reporting mechanisms already in place**