6/03/2011

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

SUMMARY MINUTES OF THE MEETING

The NISPPAC held its 38th meeting on Thursday, March 3rd 2011, 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 June 3, 2011.

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)
- Valerie Heil (Department of Defense)
- Gina Otto (Office of the Director of National Intelligence)
- Drew Winneberger (Defense Security Service)
- Richard Donovan (Department of Energy)
- Christal Fulton (Department of Homeland Security)
- Darlene Fenton (Nuclear Regulatory Commission)
- Dennis Hanratty (National Security Agency)
- Sean Carney (Department of the Navy)
- Michael Hawk (Department of State)
- Rosalind Baybutt (Industry)
- Chris Beals (Industry)
- Scott Conway (Industry)
- Shawn Daley (Industry)
- Sherry Escobar (Industry)
- Frederick Riccardi (Industry)
- Marshall Sanders (Industry)
- Michael Witt (Industry)
- William Marosy (Office of Personnel Management) – Observer

I. Welcome, Introductions, and Administrative Matters

The Chair greeted the membership and called the meeting to order at 10:00 a.m. After introductions, he reminded everyone that the meeting was being recorded and was open to the public. He also reminded the members that copies of the minutes from the November 17, 2010, meeting and copies of today's presentations were in their packets.

II. Old Business

Greg Pannoni, Designated Federal Officer, ISOO, reported on the status of the five action items from the previous meeting. First, the Office of the Director of National intelligence (ODNI) agreed to provide an update on the status of the government clearance reform, which was on the agenda for today's meeting. Next, the Chair requested that metric data regarding the causes for extensions to an Interim Approval To Operate (IATO) and efforts to resolve issues pertaining to the designation of integrity and availability requirements for information systems security plans be included in the Certification &Accreditation (C&A) working group report. Also, the Defense Security Service (DSS) will report on Industry's progress in replacing non-GSA-approved security containers., and finally, the Department of Defense (DoD) will report on whether the Defense Federal Acquisition Regulation (DFAR) permits random drug testing of contractor personnel.

III. Working Group Updates

A) Personnel Security Clearance (PCL) Working Group Report

William Marosy, Office of Personnel Management (OPM), announced that effective February 1, 2011, Kathy Dillaman, OPM, retired as the Director of the Federal Investigative Service, with, Merton Miller selected as her successor. Mr. Marosy proceeded with his presentation (appendix 1) on timeliness performance metrics for clearance decisions for the first quarter of fiscal year (FY) 2011.

He noted that there has been a slight increase in volume of incoming cases from the fourth quarter of FY 2010 and the first quarter of FY 2011. He also noted that for all initial Top Secret, and all Secret and Confidential clearances, the average time for the completion of the fastest 90 percent decreased from 97 days to 87 days between November 2010 and December 2010. He further noted that for December 2010, there was a noticeable decrease in the adjudication timeliness for initial Top Secret cases. Regarding Secret/Confidential clearance decisions for the same period, he noted that the initiation phase remains below the 14-day requirement, with investigations averaging 36 days and adjudications 29 days respectively. He articulated that a large portion of these cases are handled through automated processes that involve less field work, which results in shorter timelines.

For Top Secret reinvestigations, Mr. Marosy mentioned that there has been an increase in submissions, of about 500–1000 per month, due largely to the use of the Electronic Questionnaire for Investigations Processing. He briefed that in December 2010, the average investigative time was 102 days, and the average adjudicative time was 54 days. Mr. Marosy then addressed the declining use of the Phased Periodic Reinvestigation (PR) product noting that he has been working with Jim O'Heron at the Defense Industrial Security Clearance Office (DISCO) to identify a cause for the decline; he will report on those trends at the next NISPPAC meeting.

Helmut Hawkins, DSS, provided an update (appendix 2) on metrics regarding the FY2011 inventory of Single Scope Background Investigation/ National Agency Check with Local and Credit Checks (SSBI/ NACLC) and PR adjudications. Mr. Hawkins noted that there was a 27 percent decrease in the number of SSBI/NACLC adjudications between October 2010 and January 2011. Regarding PRs, Mr. Hawkins explained that the dramatic decrease of 94 percent in total PR adjudications from October 2010 to February 2011 can be explained as a possible aberration resulting from the way the coding is done on SSBI's in the Case Adjudication and Tracking System (CATS). He noted an increase of 23 percent for NACLC, SSBI, SBPR, and Phased PR case types from October 2009 to February 2011. Mr. Hawkins commented on the FY 2011 reject rates at DISCO for the period of November 2010 to January 2011 explaining that, prior to January 2011, a contractor compiled the data from the Joint Personnel Adjudication System (JPAS), but this data did not comprise all the reject data because about half the cases were handled internally by DISCO and these would not have been included in the JPAS data. He stated that, at the next NISPPAC meeting, the Defense Industrial Security Clearance Office (DISCO) will present both sets of data so that the overall rejection rate is reflected. In response to a comment by Stan Sims, DSS, regarding the cause of the rejects, Mr. Hawkins stated that of the nearly five percent OPM reject rate, 63 percent was due to fingerprint issues; 19 percent was due to problems with releases, and six percent was due to lack of place of birth on forms. For submissions processed by DISCO, the principal reasons for rejections are: (1) missing or incorrect Social Security number; (2) missing or incorrect alien registration number for foreign born relatives; (3) lack of signed release(s); (4) missing scope information (employment, etc.); and (5) lack of specific cost data in financial reporting. In response to a comment regarding where the rejects are occurring, Mr. Hawkins provided that the vast majority of rejections come from small companies, with category "D" companies accounting for 30 percent of the rejections and category "E" companies accounting for 57 percent of the rejections. Scott Conway, Industry, commented that we need to include data from the Defense Office of Hearings and Appeals (DOHA) in future reports of denial metrics in order to get a more accurate picture. He suggested that DOHA should be invited to participate in the PCL working group and at the NISPPAC meetings.

The Chair commented that, while there has been progress in the last quarter with regard to adjudications, he expressed concern about the on-going relocation of DISCO.
Mr. Sims responded that DISCO has lost over 85 percent of its adjudication staff in the consolidation of the Central Adjudication Facilities to Fort Meade, Md. Citing the use of mandatory overtime and extra training to ensure that DISCO stays on track in meeting timelines, Mr. Sims stressed that, although Industry could experience some delays, they would be kept to a minimum.

B) Government Clearance Reform Update

The Chair introduced Mr. Charles Sowell, ODNI, to update the NISPPAC on the efforts of the Joint Suitability and Security Clearance Reform Team. Mr. Sowell provided a brief overview (appendix 3) of the Joint Reform Team organization, its authorities, its missions, as well as providing an orientation to its major functional areas. He noted that security executive agent support is provided by the ODNI. This support includes planning, monitoring, and reporting for 51 executive branch-wide and intelligence community-specific, special reform projects, as well as interfacing with the Performance Accountability Council. Mr. Sowell explained the timelines developed for clearance reform and how the endeavor resulted in the development of a strategic framework that drives current efforts. The efforts have brought about the recent removal of DoD from the Government Accountability Office "high risk" list, where it was placed in 2005. Mr. Sowell described the transformed process, which includes validating needs, eApplication (a new Standard Form (SF) 86), automated records check, eAjudicate, enhanced subject interviews, and expandable, focused investigations through continuous evaluation. Mr. Sowell indicated that timeliness has significantly improved over the last five years while the focus on quality has been maintained and reciprocity and transparency have improved. His discussion of the performance measures showed that the end-to-end timelines for the fastest 90 percent of all initial and Top Secret PR investigations in the fourth quarter of FY 2010 meet the Intelligence Reform and Terrorism Prevention Act requirements and the Office of Management and Budget goals.

He then provided an update on the status of the Joint Reform Team Interagency Working Group revision of the Federal Investigation Standards (FIS) to improve the cost, quality, and timeliness of investigations. The updated FIS model consists of five tiers that reflect the difference in formats and investigative scope for public trust positions (tiers two and four) as well as those for sensitive and national security positions (tiers one, three, and five). He reiterated that the goal of the FIS updates is to resolve some of the policy conflicts that currently exist between Intelligence Community Directive 704 and the 1997 federal investigative standards.

In response to an inquiry from Ms. Baybutt as to why Industry numbers seem to be highest, Mr. Sowell stated that the reason was unclear. However, subsequent comments from Mr. Sims and Mr. Hawkins suggested that differences in the processes used to monitor the submissions by the Agencies and Industry definitely impacted the timelines. Mr. Sims stated that most Agencies conduct a pre-screening of submissions on the front-end so these submissions are a lot cleaner and can be put through the e-adjudication process (currently 28–34 percent of investigations), and he noted that only four percent of Industry submissions are adjudicated electronically. Mr. Hawkins added that the e-adjudications are limited to NACLC's and that SSBI's and other more in-depth investigations are not eligible for electronic processing. Mr. Conway suggested that this information should be in the metrics reported to the PCL working group. Mr. Sims pointed out that DSS sends all investigations with substantial issues to DOHA, which significantly lengthens the adjudicative timeline.

C) Certification and Accreditation (C&A) Working Group Report

Randy Riley, DSS, reported (appendix 4) on the Industrial Security Field Office, Office of the Designated Approval Authority (ODAA) metrics, on behalf of the NISPPAC C&A working group. After a review of the ODAA's C&A responsibilities, Mr. Riley presented the metrics showing the number of days to process information systems plan submissions for the period of February 2010 through January 2011. During that period, 3,859 Interim Approvals to Operate (IATO) were granted within an average of 28 days after submission. The average number of days from an IATO to a formal Approval to Operate (ATO) was reported at 84 days.

Ms. Baybutt commented about a working group discussion regarding System Security Plans (SSP) being rejected prior to their being entered into the formal DSS review process. Mr. Riley acknowledged that some plans are sent back to the Information Systems Security Managers (ISSM) because they do not include critical information needed for the review process, but that the ODAA works with ISSMs to expedite corrections. It is rare that this issue would cause a plan to be sent to the back of the queue where the review process would have to be restarted. Mr. Pannoni commented that the metrics need more refinement in this area to show the total number of plans that were submitted and how many plans made it into the queue that in turn started the clock for IATO/ATO approval. John Haberkern, DSS, commented that it is important to understand what differentiates a rejection from a denial; however, it is a process than may take a little more time to fine tune. Mr. Riley agreed the ODAA is responsible for collecting data to answer those questions. Specifically, he indicated that, for January 2011, 317 IATOs were granted within an average of 21 days after submission, and the IATO to ATO approvals averaged 82 days.

The metrics for reviews of SSPs indicated that between February 2010 and January 2011, 4,906 plans were reviewed and that on average 36.9 percent of all the plans submitted required some changes prior to the on-site verification for an ATO. The review revealed that the common errors encountered during plan reviews included incomplete or missing attachments and certifications, and integrity and availability issues that were not addressed. In response to a comment from Mr. Pannoni regarding a breakdown of the "other" category, which constituted 20 percent of the total number of errors, Mr. Sims indicated that the review process was manual and that the collection of the data in such detail would be very manpower intensive. However, he indicated that DSS would examine if it could get better clarity for the report. The Chair commented it was important to know where the errors are coming from so we can start to reduce them over a period of time. Tony Ingenito, Industry, and Vince Jarvie, Industry, both commented on the importance of identifying the type of company where the errors are coming from so that training can be adjusted to help mitigate the problems. Mr. Riley then reported on the 3,662 on-site verifications conducted by ODAA between February 2010 and January 2011, and noted that over 24 percent of the systems that were reviewed required some type of modification to receive an ATO. Specifically, he noted that 814 (22.2 percent) of the systems had some minor discrepancy that was resolved during the on-site validation and that 73 systems (2 percent) had significant discrepancies that could not be resolved during the on-site. He noted that, for the period of October 2010 through January 2011, the most common discrepancies found during on-site reviews included security relevant objects that were not being protected and the system topology not being accurately reflected in the SSP. In response to a comment from Mr. Pannoni regarding the need for more detail on where the discrepancies are occurring, Mr. Riley agreed that the ODAA should be able to get more granularity as it improves its processes.

Sheri Escobar, Industry, inquired as to what would be done if we determine that the small companies contribute to the majority of the discrepancies? Ms. Escobar elaborated, stating that Government and Industry continue to push the problems back and forth to each other, but nothing gets done. Reiterating her point, she opined that if everyone agrees it is the category “D” and “E” companies that are the problems, then solutions need to be found through NISPPAC working groups or other ways, and we must focus on how to help these small companies improve their processes. In response, Mr. Sims commented that it still needs to be determined if it is the small companies, and if so there will be ways to address the problems and work within the Government to get solutions to help the small companies. Mr. Pannoni opined that there is a framework that can address the issues, such as the National Classification Management Society (NCMS) chapter meetings that could provide the venues for focused educational efforts. The Chair commented that this is an agenda item for the next meeting in New Orleans especially since there will be a higher percentage of small companies present at the meeting.

Mr. Riley finished his presentation by reviewing the three general reasons for an IATO extension: (1) the on-site review did not result in an ATO; (2) DSS had to postpone an onsite review; or (3) the contractor had to postpone the onsite review. Regarding the “Integrity and Availability not available” error, Mr. Riley showed a before and after sample of the checklist that is being changed to enable the default of “not contractually imposed,” which should apply to 99 percent of the NISP contractors.

IV. New Business

A) Defense Security Service Update

Mr. Sims advised of his new role as the Director of DSS. He noted that in the last two days he hosted both Government and Industry stakeholders meetings where several of the same issues being presented here today were discussed. He explained that during both meetings he presented his vision for DSS and his intention to fundamentally change how DSS will be doing business. He emphasized that DSS collaboration and communication with its Government and Industry partners will become paramount and that everything will be transparent so that DSS's partners fully understand the dynamics that we face. He emphasized that he is proactive in getting things fixed, believes in the team approach, and considers Industry a key part of the team. He stated he has emphasized to his staff that he wants to conduct oversight as an advisory and assistance type of function. Mr. Sims provided a recap of central themes from the stakeholders meeting, specifically emphasizing the importance of the "Voice of Industry Survey", and stressing the importance of ensuring that the respondents give honest efforts, without fear of reprisals, because these surveys are taken seriously by the DSS leadership. In response to Industry feedback faulting the current security review rating system as being too subjective, Mr. Sims announced that there is a new numeric-based rating system being presented to Industry, and while it may have problems at first, with feedback it will be fixed. He cited as an example, electronic fingerprinting and stated that DoD was taking the lead and is forming a working group, which will include Industry, to develop a plan to meet the FY 2013 implementation requirement.

Mr. Sims acknowledged the need to get more Industry-oriented threat data through DSS' Counterintelligence (CI) efforts. He mentioned that the DSS CI office has produced threat analyses for specific companies and has received positive feedback on the results. He also noted that DSS is trying to capture threat information from the intelligence agencies that might impact Industry. Mr. Sims highlighted his plan to make the DSS website a "one stop shop" that provides more links and accessibility to information that Industry needs. Regarding National Interest Determinations (NID), Mr. Sims, stated that DoD is leading the effort to fix the NID process and highlighted the need for coordination of policies and procedures across all the Cognizant Security Authorities to ensure Industry is not adversely impacted by the process.

Mr. Sims then solicited Industry's support for the annual Personnel Security Investigations (PSI) survey, which is provided to Industry each year to help forecast PSI requirements. Emphasizing its importance, Mr. Sims, emphasized that the survey directly impacts how DSS resources manpower for processing clearances and that it is essential to have a 100 percent response to the survey. He also appealed for Industry participation in the Wounded Warrior Program and cited successful accomplishments by

Industry. Mr. Sims concluded his update by indicating that in his 88 days on the job he has identified areas where DSS can do better and that he is working with his staff to affect necessary change.

The Chair commented that both Government and Industry look forward to working with Mr. Sims in his new position and then requested an update on how Industry is doing with the replacement of non-GSA approved containers. In response, Sharon Irwin, DSS, reported that about 2,500 non-GSA approved containers have been replaced since October, 2010, and that DSS will report at the next meeting regarding the number of non-GSA- approved containers that still need to be replaced. Mr. Sims commented that the information is being collected as DSS conducts its security reviews, and the Chair requested an in-depth report at the fall meeting.

B) JPAS Status Update

The Chairman introduced George Angelovic, Defense Manpower Data Center (DMDC), to report (appendix 5) on efforts regarding the use of Public Key Infrastructure (PKI) on JPAS and on the elimination of the fax option for submitting forms to DISCO and OPM. After providing an overview, Mr. Angelovic provided an update on the status of public key enabling for the JPAS system. Phase 1 which began in June 2010, gathered requirements from DSS and Industry to address security issues regarding JPAS access. Using a multi-phased approach, JPAS became Common Access Card (CAC)-enabled on January 19, 2011. Users can now login to JPAS using either a username or password or a previously issued CAC. In June 2011, the testing of the personal identification verification (PIV) card begins. When this is complete, the PIV will provide another means to login to JPAS. Phase III will enable the use of Industry-issued/DoD-approved PKI devices.

Mr. Angelovic then explained that the use of the fax server option within JPAS, which allows submission of signature pages associated with an SF 86, will end on May 1, 2011. The fax option is very manpower-intensive and costs the Government almost one million dollars a year to operate. The use of the scan and upload method, which is currently available for submission of signature pages, will become the required standard for submitting the SF 86 certification and authorization forms. Mr. Angelovic mentioned some of the benefits of this change include: (1) removal of an unsecure submission method and an improvement in the protection of Personally Identifiable Information (PII); (2) resolution of data quality issues that required manual processes; and (3) elimination of a 25 percent delay rate for fax submissions. He then provided an update on changes to the timeout policies, stating that the Joint Adjudication Management System timeout will go from four hours to 30 minutes, and that the Joint Clearance & Access Verification System timeout will go from 45 minutes to 15 minutes. These changes will help mitigate significant security vulnerabilities to the network, web servers, and PII data, as well as enhance compliance with DoD and Defense Information Systems Agency computer use policies. Finally, Mr. Angelovic summarized on-going communication and outreach efforts to keep stakeholders apprised of the changes occurring within the DMDC. Mr. Sims noted that DSS would be providing links to the DMDC website to make it easier to get to the needed information.

C) DoD Update

Valerie Heil, DoD, provided an update regarding implementation of Section 845 of the National Defense Authorization Act of 2011, which requires the Secretary of Defense to provide plans and guidance regarding covered entities that are authorized to safeguard classified national security information and not under foreign ownership, control or influence mitigation measures. The report is due to Congress in October 2011 and Ms. Heil noted that DoD and DSS will work with the NISPPAC working groups to issue NISP Operating Manual (NISPOM) changes that address the new requirements. Ms. Heil discussed the NISPOM revisions and thanked everyone who provided inputs and noted that the January 25, 2011, ad-hoc working group meeting resulted in the identification of the need for a significant rewrite of the safeguarding section. Mr. Sims asked about changes to the timeline for getting the rewrite published, and Ms. Heil stated that DoD is planning for a public release for comments in the fourth quarter of FY 2011. She further explained that the document would also go through the DoD internal approval process at the same time and stressed that the NISPPAC members would have one final opportunity for review of the document. Mr. Sims commented on the time it is taking to get the new NISPOM published and encouraged a tighter timeline to review the proposed changes. The Chair commented on the need to validate the requirement that the NISPOM be published in the Federal Register, citing the ISOO Implementing Directive as an example by noting that it was not published in the Federal Register prior to release. The Chair highlighted the criticality in getting the NISPOM published and suggested that the DoD process should be expedited, asserting that it is important to have the document published as soon as possible. Mr. Sims concurred with the Chair's comments regarding an expedited DoD coordination process. Ms. Heil detailed what remains in the coordination process and reiterated that efforts are being made to get the NISPOM update approved. The Chair again commented that it might be prudent to approve what we currently have, rather than to continue to wait to get other sections coordinated. Finally, in response to the action item from the last meeting on whether the DFAR permits random drug testing of contractor personnel, Ms. Heil commented that the issue is under evaluation and assessment within DoD and expects an answer by the June NISPPAC meeting.

Note: Since the March NISPPAC meeting, the DoD representative to the NISPPAC responded that DFARS clause 252.223-7004 clearly requires the contractor to institute and maintain a program to identify illegal drug users in applicable contracts and the phrase "appropriate alternatives" does not present an option to avoid drug testing. If Industry NISPPAC members believe that there is an issue with the meaning of the clause, they should formally raise the issue to the Office of the Director, Defense Procurement and Acquisition Policy with a request for revision of the clause.

D) Combined Industry Presentation

Scott Conway, Industry, presented the combined industry presentation (appendix 6). After a review of Industry members of the NISPPAC, and Memorandum of Understanding (MOU) organizations, Mr. Conway explained the roles and responsibilities of the NISPPAC Industry members in support of the various working groups and NISPOM review teams. Mr. Conway specifically noted Industry's efforts as part of the DoD Special Access Program (SAP) Manual Review Team, and Ronald Hopkins, DoD, shared details regarding the plan to incorporate revised SAP guidance into the Special Security Information section (Attachment D) of the NISPOM.
Mr. Conway highlighted the following areas of interest for Industry: (1) efforts to enhance information sharing, specifically regarding getting threat information through the Defense Industrial Base (DIB) processes and framework; (2) C&A process timelines with specific concerns regarding when the clock for the review process actually starts and with the processes for reaccreditation of expiring systems; (3) PCL reform, with specific concerns regarding continuous monitoring as JPAS transitions to PKI; (4) industrial security policy modernization and Controlled Unclassified Information implementation with specific concerns regarding revisions, updates, and implementation issues; (5) implementation of an information technology (IT) security strategy that includes developing DFAR clauses regarding IT security relating to the DIB-wide environment; (6) increased focus on insider threat and associated problems resulting from the Wiki Leaks that has brought increased focus on CI and that has highlighted related gaps in the governance process; (7) cost and impact of data spills and the associated need to review the advanced persistent threat requirements; (8) impact on staffing levels related to the relocation of DISCO and the possibility of temporary delays in clearance processing; and (9) the future of the NISPOM Supplement and the need for consistent national policy for special security requirements. In response to a comment from Gina Otto, ODNI, regarding updates to the current insider threat efforts at a future NISPPAC meeting, the Chair commented on government efforts pertaining to insider threat that may be of interest to the NISPPAC, and he stated that DSS is a model with standards and oversight in the executive branch.

V. General Open Forum/Discussion

No items were discussed.

VI. Closing Remarks and Adjournment

The Chair noted that the next NISPPAC meeting will be on Monday June 20, 2011, from 1:00 to 3:00 p.m., at the Hilton Riverside Hotel in New Orleans, Louisiana, in conjunction with the NCMS Annual Training Seminar. He reminded members to begin their travel planning as soon as possible and solicited agenda items for the meeting by May 16, 2011. Finally, he noted that the last meeting for this calendar year is scheduled for November 16, 2011. The Chair adjourned the meeting at 12:15 p.m.

Summary of Action Items

(1) DoD will formally request representation of DOHA in the NISSPAC's PCL working group processes in order to better understand clearance appeal processes and timeliness issues.

(2) DSS will clarify the rejection and denial processes in regard to the review and approval of SSPs.

(3) Industry will work with Government to identify methodologies and capabilities to assist small and medium sized companies, identified as submitting PCL requests and system accreditation packages that are continually rejected, with resources to eliminate their problematic actions.

(4) ISOO requested an update from DoD at the November 2011, NISPPAC meeting on the number of non-GSA approved security containers in Industry that require replacement.

(5) ISOO will coordinate the presentation on the "Governance of the Insider Threat" at the November 2011 NISPPAC meeting.

(6) Government and Industry members were requested to provide agenda items for the June NISPPAC meeting in New Orleans, by May 16, 2011. Additionally, the working group reports should provide enhanced metrics relating to small and medium sized companies.

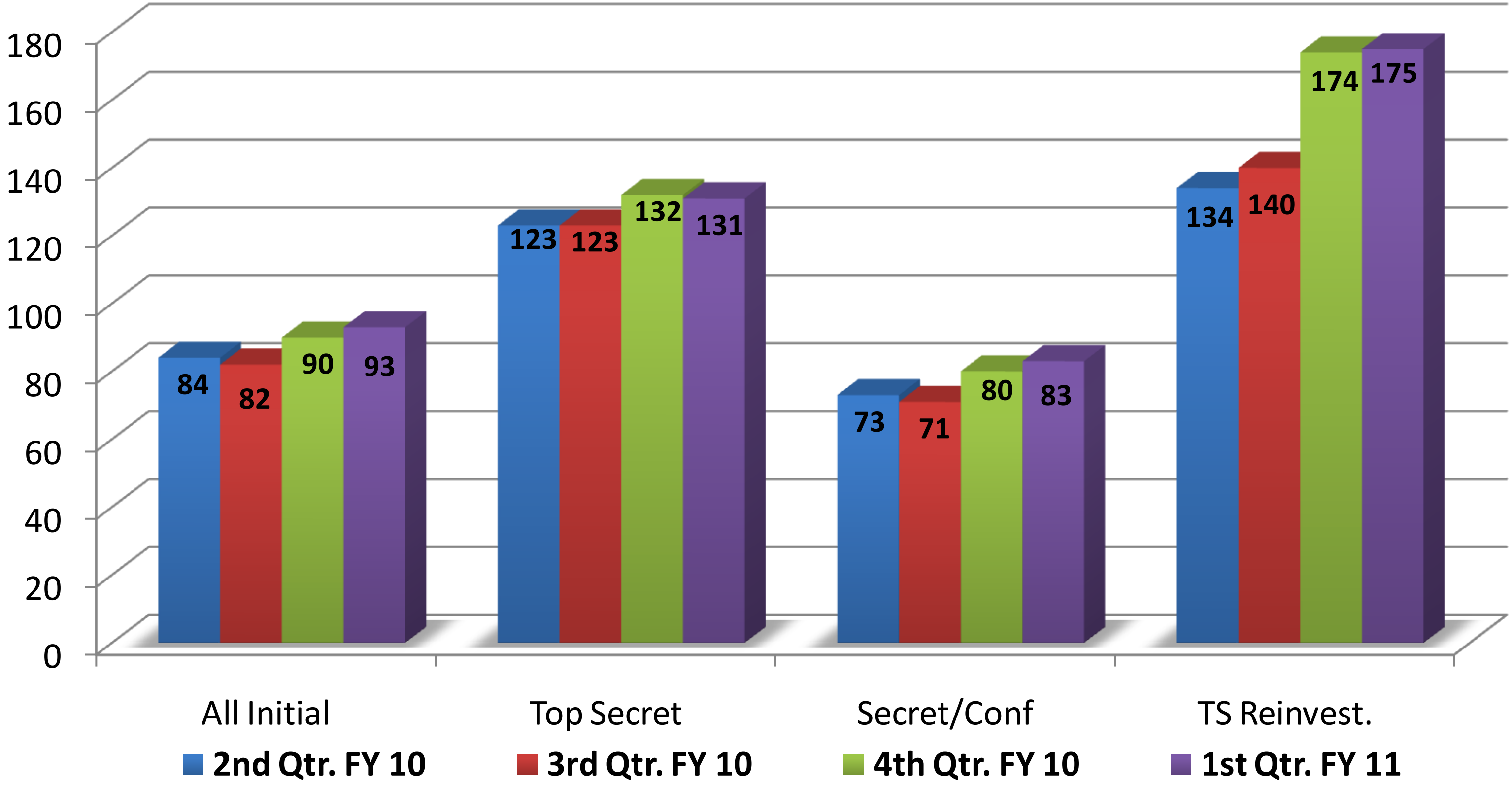
(7) Industry will provide an update on its progress in nominating two new members to represent Industry from October 1, 2011, to September 30, 2015.

(8) OPM and DISCO will report on trends relating to a decline in the submission of Phased PRs.

Appendix 1- OPM PCL Presentation

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

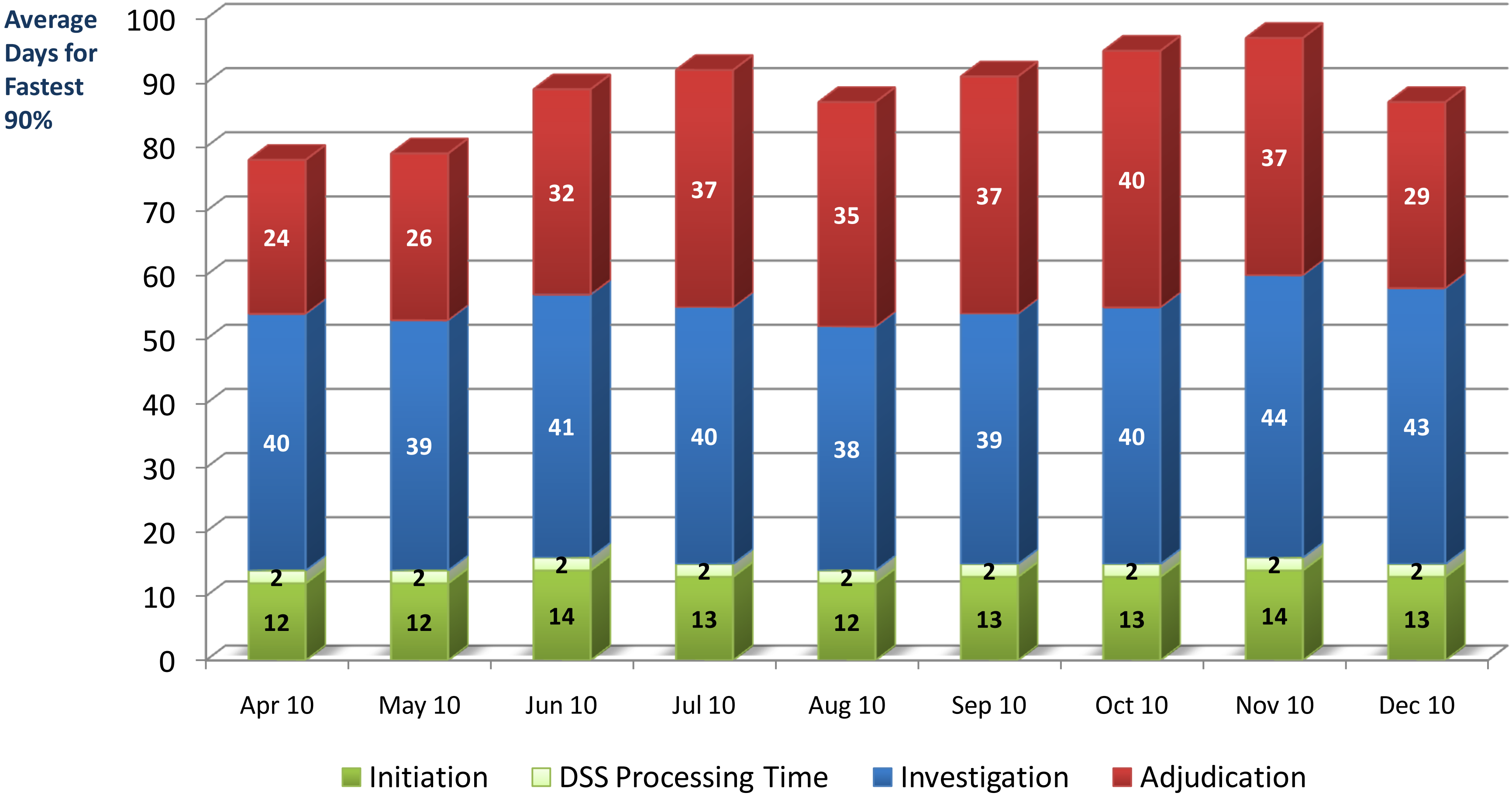
Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 2nd Q FY10	23,143	5,210	17,933	4,611
Adjudication actions taken – 3rd Q FY10	25,027	5,422	19,605	5,320
Adjudication actions taken – 4th Q FY10	25,446	5,247	20,199	4,051
Adjudication actions taken – 1st Q FY11	29,639	6,766	22,873	6,894

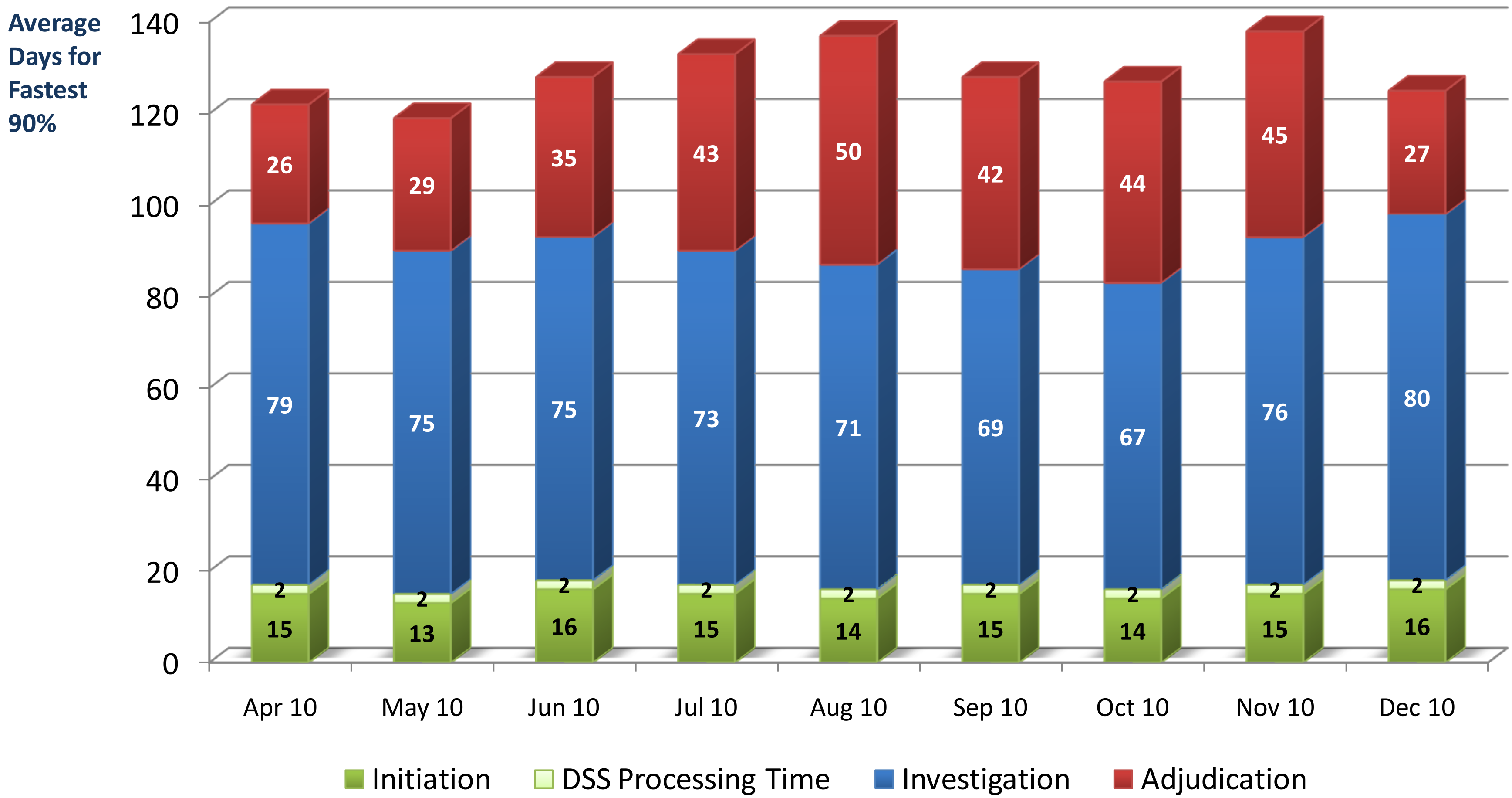
*The adjudication timelines include collateral adjudication by DISCO and SCI adjudication by other DoD adjudication facilities

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



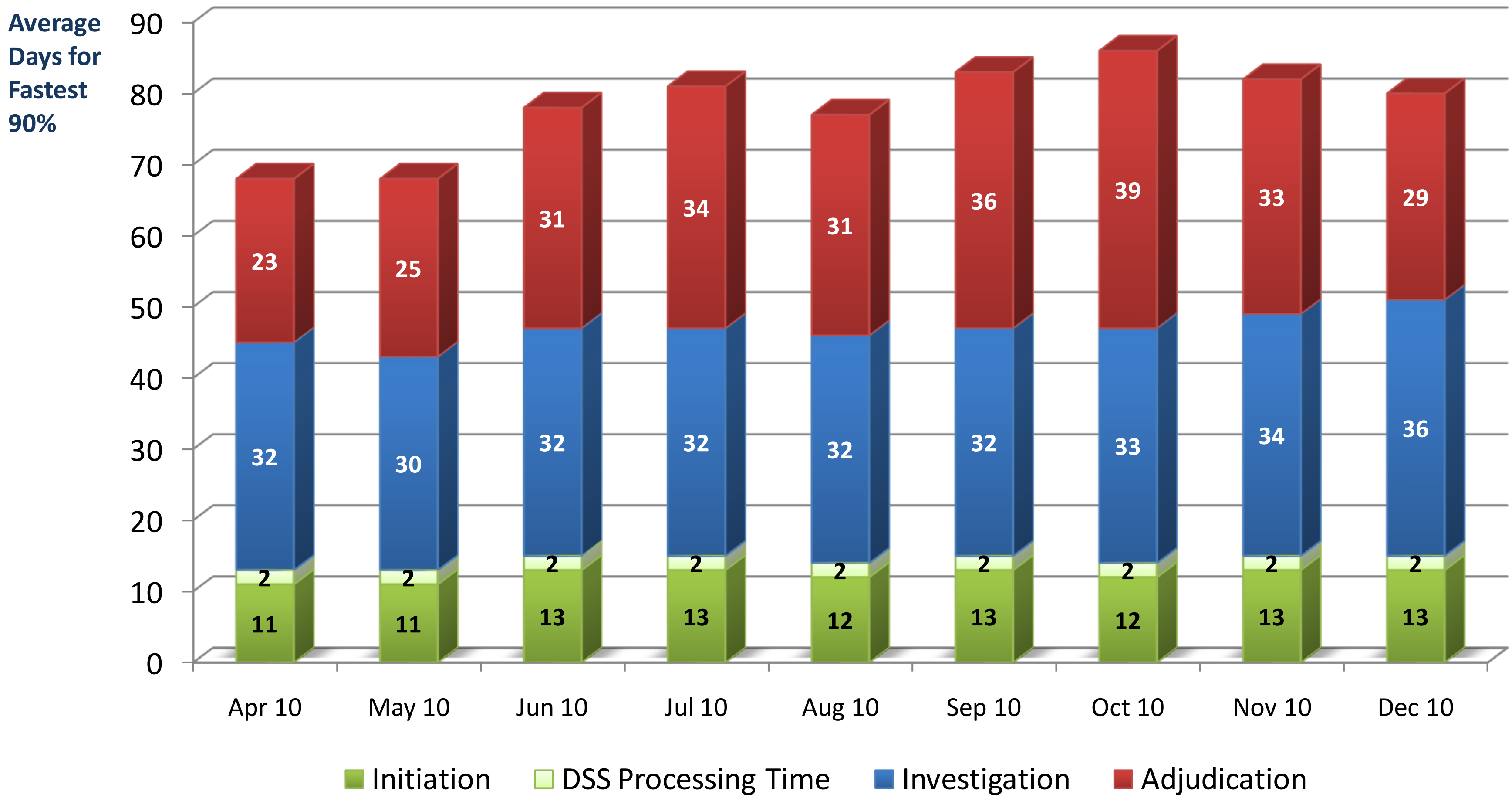
	Apr 10	May 10	Jun 10	Jul 10	Aug 10	Sep 10	Oct 10	Nov 10	Dec 10
100% of Reported Adjudications	8,245	7,903	8,531	6,037	10,235	9,233	9,994	9,729	9,662
Average Days for fastest 90%	78 days	79 days	89 days	92 days	87 days	91 days	95 days	97 days	87 days

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



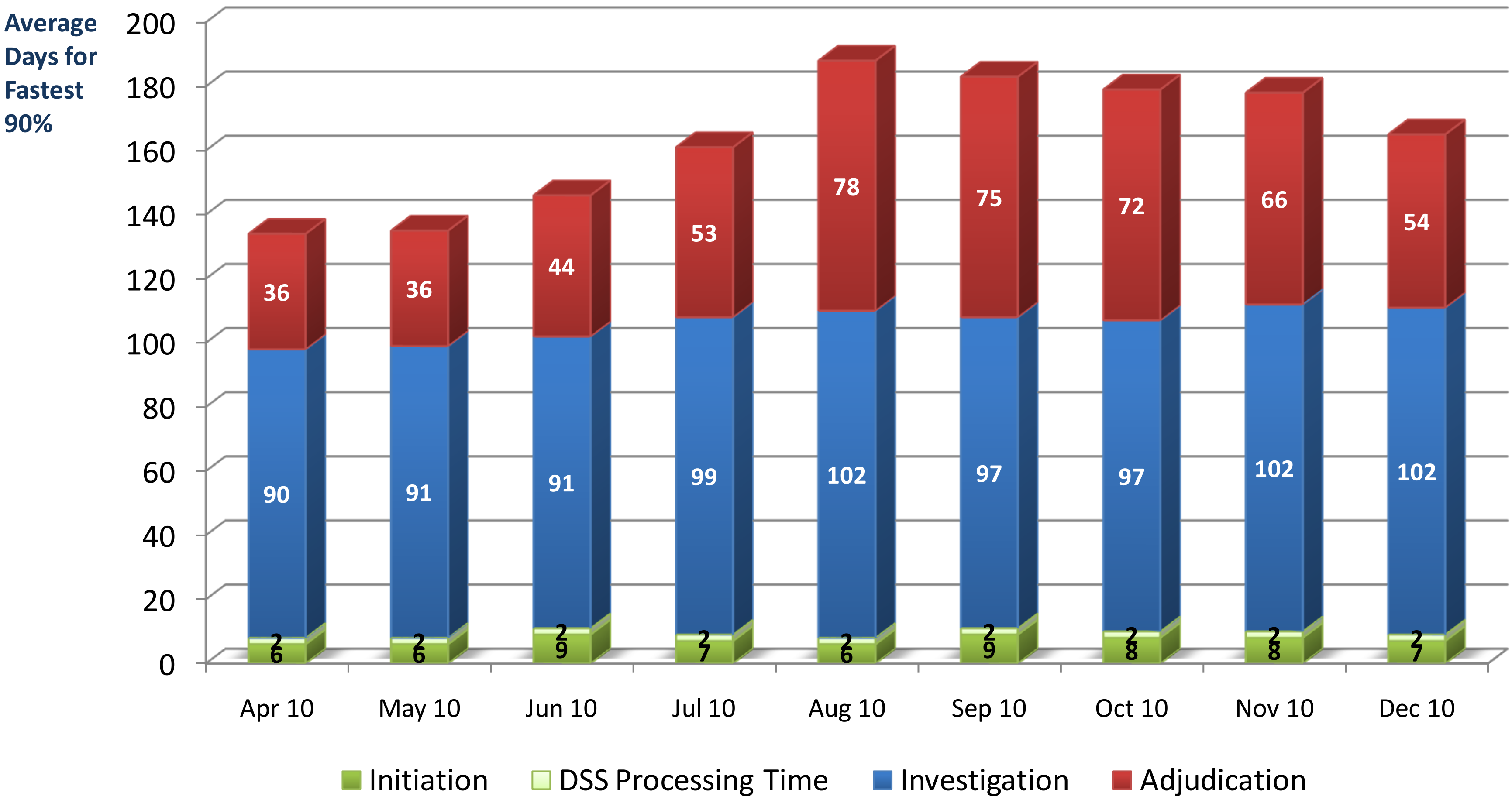
	Apr 10	May 10	Jun 10	Jul 10	Aug 10	Sep 10	Oct 10	Nov 10	Dec 10
100% of Reported Adjudications	1,575	1,825	1,935	1,330	1,975	1,964	2,282	2,669	1,781
Average Days for fastest 90%	122 days	119 days	128 days	133 days	137 days	128 days	127 days	138 days	125 days

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



	Apr 10	May 10	Jun 10	Jul 10	Aug 10	Sep 10	Oct 10	Nov 10	Dec 10
100% of Reported Adjudications	6,670	6,078	6,596	4,707	8,260	7,269	7,712	7,060	7,881
Average Days for fastest 90%	68 days	68 days	78 days	81 days	77 days	83 days	86 days	82 days	80 days

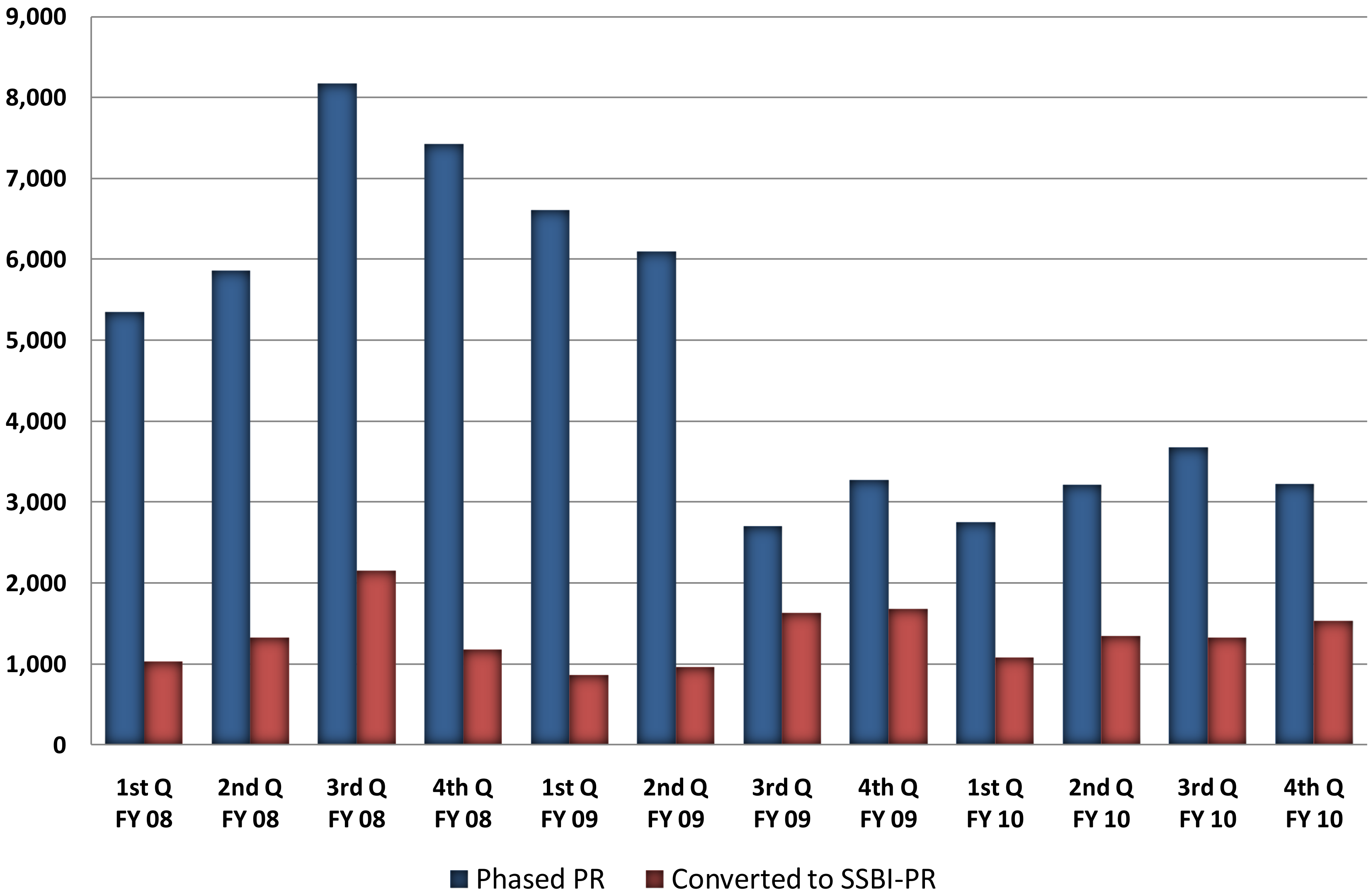
Industry's Average Timeliness Trends for 90%
Top Secret Reinvestigation Security Clearance Decisions



	Apr 10	May 10	Jun 10	Jul 10	Aug 10	Sep 10	Oct 10	Nov 10	Dec 10
Reported Adjudications	1,643	1,513	1,917	1,423	1,170	1,497	2,197	2,008	2,522
Average Days for fastest 90%	134 days	135 days	146 days	161 days	188 days	183 days	179 days	178 days	165 days

Phased PR Investigations - Industry

Based on Cases Closed by Quarter

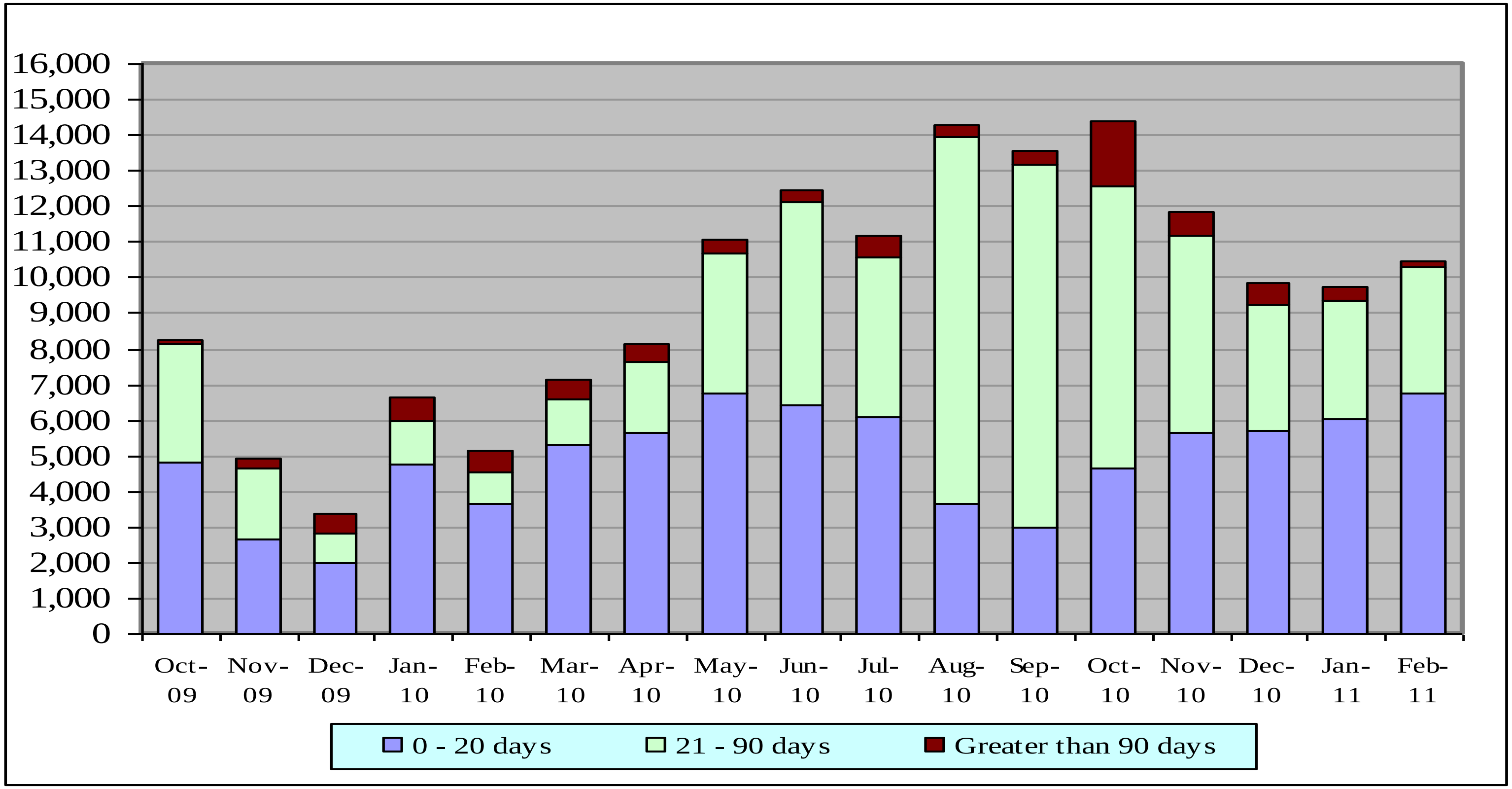


Appendix 2- DISCO PCL Presentation

DISCO

FY11 Adjudication Inventory

SSBI/NACLC Clearance Adjudications



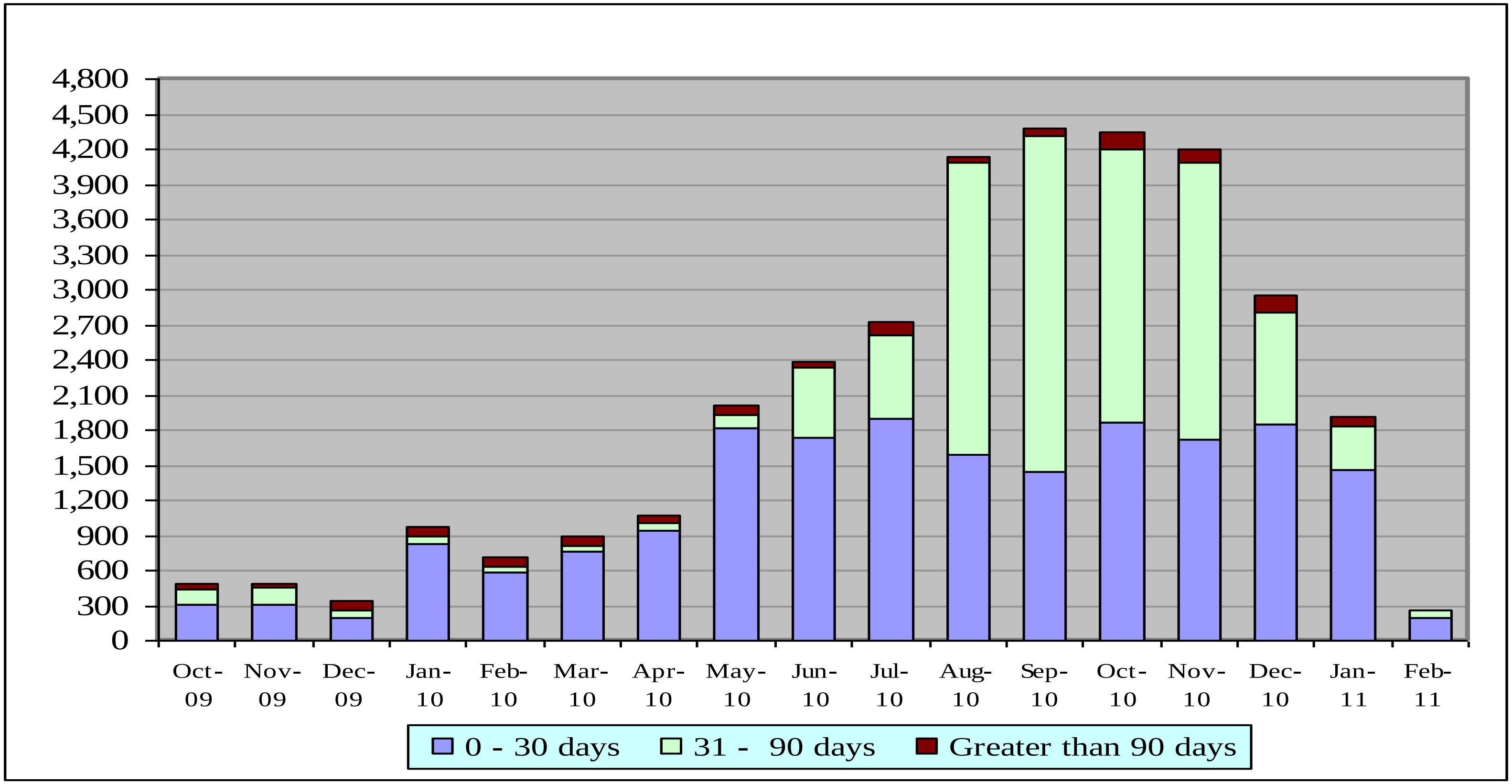
Category	Oct-09	Nov-09	Dec-09	Jan-10	Feb-10	Mar-10	Apr-10	May-10	Jun-10	Jul-10	Aug-10	Sep-10	Oct-10	Nov-10	Dec-10	Jan-11	Feb-11
0 - 20 days	4,797	2,650	2,002	4,752	3,656	5,331	5,642	6,759	6,414	6,087	3,666	2,975	4,661	5,643	5,709	6,020	6,782
21 - 90 days	3,349	1,987	840	1,238	890	1,247	2,012	3,935	5,728	4,470	10,288	10,210	7,925	5,556	3,536	3,315	3,517
Greater than 90 days	91	269	557	653	591	550	505	374	315	599	315	379	1,799	670	593	414	192
Grand Total	8,237	4,906	3,399	6,643	5,137	7,128	8,159	11,068	12,457	11,156	14,269	13,564	14,385	11,869	9,838	9,749	10,491

Source: JPAS and CATS

DISCO

FY11 Adjudication Inventory

Periodic Reinvestigation Adjudications



Category	Oct-09	Nov-09	Dec-09	Jan-10	Feb-10	Mar-10	Apr-10	May-10	Jun-10	Jul-10	Aug-10	Sep-10	Oct-10	Nov-10	Dec-10	Jan-11	Feb-11
0 - 30 days	308	312	201	831	586	761	946	1,812	1,733	1,890	1,583	1,437	1,868	1,718	1,843	1,454	201
31 - 90 days	133	135	54	53	47	56	55	113	599	722	2,496	2,877	2,331	2,373	967	380	52
Greater than 90 days	47	37	87	82	73	71	73	82	51	111	50	58	142	108	145	79	13
Grand Total	488	484	342	966	706	888	1,074	2,007	2,383	2,723	4,129	4,372	4,341	4,199	2,955	1,913	266

Source: JPAS and CATS

FY11 INDUSTRY CASES AT OPM

Investigation Inventory

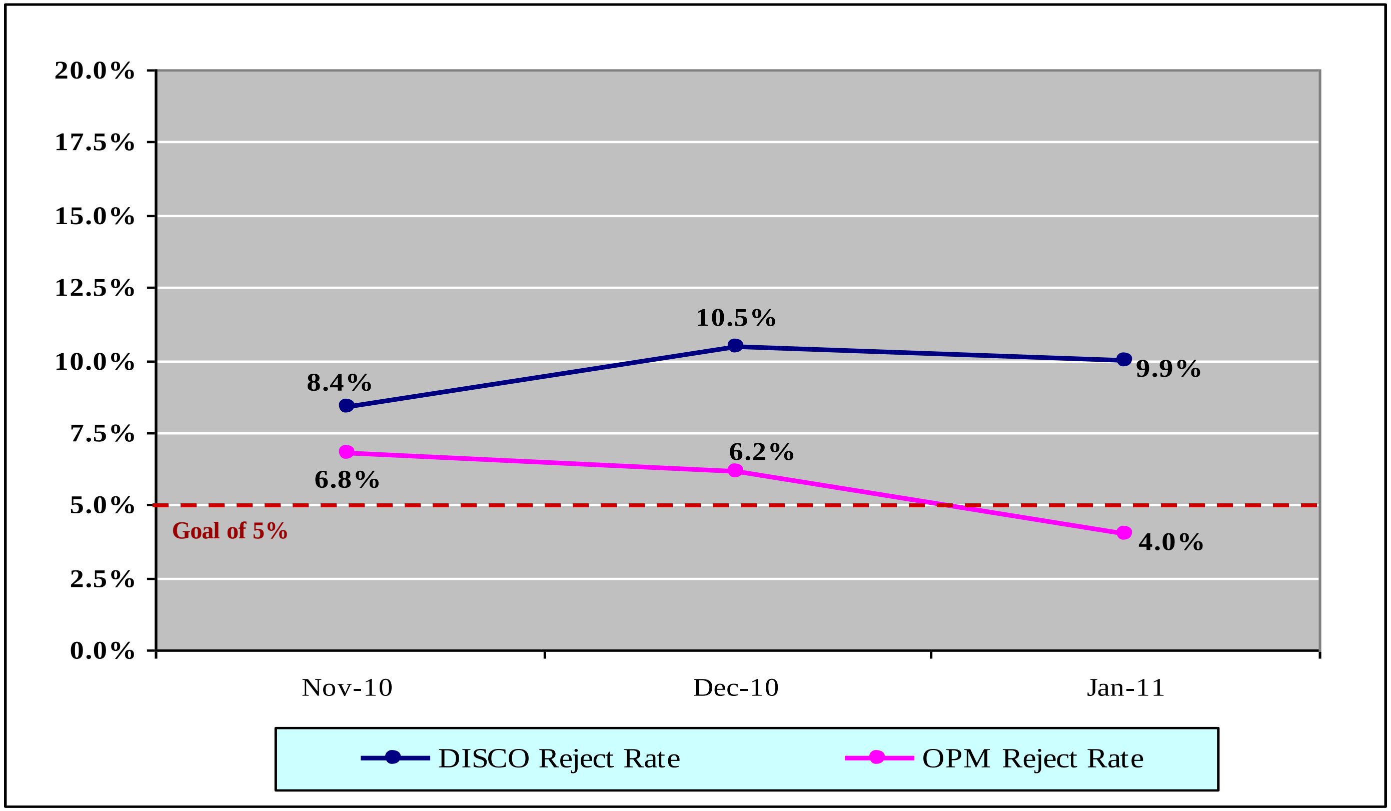
Case Type	FY09				FY10				FY11		Delta Q1FY10 vs Feb FY11
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Feb-11	
NACLC	13,209	13,982	13,900	12,307	11,730	11,685	13,016	13,556	13,118	13,473	15%
SSBI	6,626	6,687	6,944	6,561	6,782	7,012	6,561	6,178	6,308	5,714	-16%
SSBI-PR	3,772	4,160	4,692	3,703	4,096	4,521	4,859	5,115	5,436	7,103	73%
Phased PR	5,430	2,771	2,476	2,640	3,158	3,629	3,665	4,248	4,781	5,306	68%
Total Pending	29,037	27,600	28,012	25,211	25,766	26,847	28,101	29,097	29,643	31,596	23%

Overall increase of 23% for NACLC, SSBI, SBPR and Phased PR case types from 1QFY10 to Feb FY11.

Source: OPM Customer Support Group

FY11 REJECT RATES

Initial and Periodic Reinvestigation Requests



- **FY11**
  - **<u>DISCO</u> Received 35,539 investigation requests**
    - **Rejects** – DISCO rejected **3,425 (9.6% on average)** investigation requests to FSOs for re-submittal
  - **<u>OPM</u> Received 43,936 investigation requests**
    - **Rejects** - OPM rejected **2,474 (5.6% on average)** 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 / DISCO Monthly Counts

Appendix 3- Joint Reform Team Presentation

Joint Suitability and Security Clearance Process Reform Team

Briefing for NISPAC

March 3, 2011

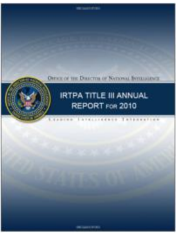
Joint Reform Team

AGENDA

- Joint Reform Team Overview and Background
- Transformed Process
- Current Status
- Performance Measures
- Federal Investigative Standards

Joint Reform Team

JOINT REFORM TEAM OVERVIEW


Office of the Director of National Intelligence
IRTPA TITLE III ANNUAL REPORT FOR 2010

SECURITY AND SUITABILITY PROCESS REFORM
STRATEGIC FRAMEWORK
February 2010

Team Members

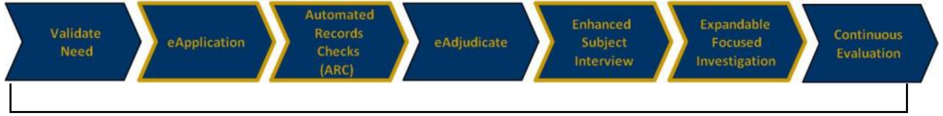
ODNI
DoD
OPM
OMB

Authorities

IRTPA
EO 13467
EO 12968

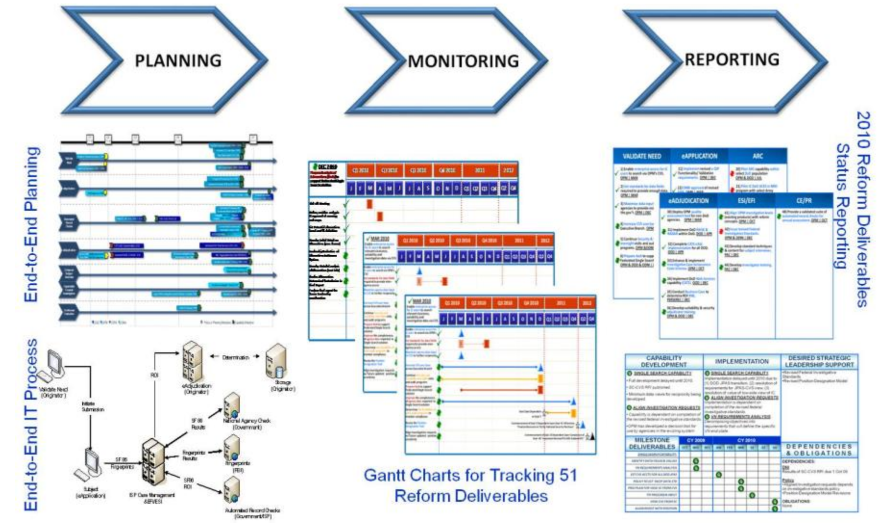
Mission

- The JRT organizes and drives Executive Branch efforts to improve the timeliness, efficiency and quality of the USG's personnel security and suitability determination processes


Validate Need
eApplication
Automated Records Checks (ARC)
eAdjudicate
Enhanced Subject Interview
Expandable Focused Investigation
Continuous Evaluation

Major Functional Areas

- Security Executive Agent Support
- Program Management (planning, monitoring and reporting) for 51 Executive Branch-wide and IC-specific reform effort projects
- Reports to / interfaces with PAC, Congress, GAO


PLANNING
MONITORING
REPORTING
End-to-End Planning
End-to-End IT Process
Gantt Charts for Tracking 51 Reform Deliverables
2010 Reform Deliverables Status Reporting

Joint Reform Team

REFORM BACKGROUND

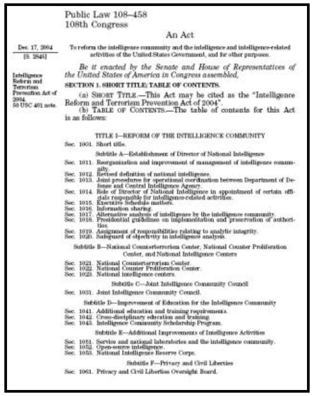
GAO
U.S. Government Accountability Office

DoD Placed on GAO "High Risk" List

2004

2005

IRPTA



Public Law 108–458
108th Congress

An Act

Dec. 17, 2004
[S. 2845]

To reform the intelligence community and the intelligence and intelligence-related activities of the United States Government, and for other purposes.

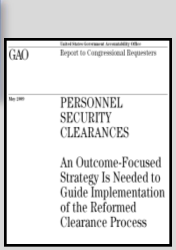
Intelligence Reform and Terrorism Prevention Act of 2004.
50 USC 401 note.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Intelligence Reform and Terrorism Prevention Act of 2004".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

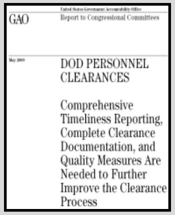


United States Government Accountability Office
GAO
Report to Congressional Requesters

May 2009

PERSONNEL SECURITY CLEARANCES

An Outcome-Focused Strategy Is Needed to Guide Implementation of the Reformed Clearance Process

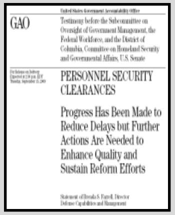


United States Government Accountability Office
GAO
Report to Congressional Committees

May 2009

DOD PERSONNEL CLEARANCES

Comprehensive Timeliness Reporting, Complete Clearance Documentation, and Quality Measures Are Needed to Further Improve the Clearance Process



United States Government Accountability Office
GAO
Testimony before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery Expected at 2:30 p.m. EDT Tuesday, September 15, 2009

PERSONNEL SECURITY CLEARANCES

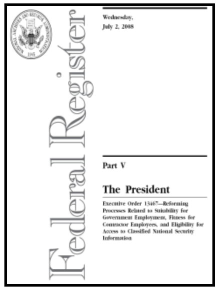
Progress Has Been Made to Reduce Delays but Further Actions Are Needed to Enhance Quality and Sustain Reform Efforts

Statement of Brenda S. Farrell, Director Defense Capabilities and Management

2006

2007

Joint Reform Team



Federal Register

Wednesday,
July 2, 2008

Part V

The President

Executive Order 13467—Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information

E.O. 13467

2008

United States Government Accountability Office
GAO
Testimony
Before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, House of Representatives

For Release on Delivery Expected at 10:00 a.m. EDT Thursday, October 1, 2008

PERSONNEL SECURITY CLEARANCES

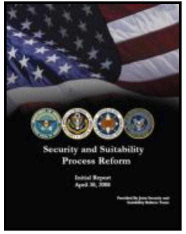
An Outcome-Focused Strategy and Comprehensive Reporting of Timeliness and Quality Would Provide Greater Visibility over the Clearance Process

Hearings

2009

2010

2011



Security and Suitability Process Reform

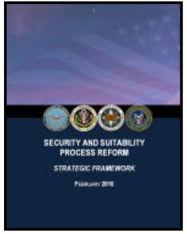
Initial Report
April 30, 2008

Provided by the Joint Security and Suitability Reform Team

Security and Suitability Process Reform

December 2008

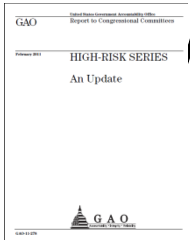
Provided by the Joint Security and Suitability Reform Team



SECURITY AND SUITABILITY PROCESS REFORM

STRATEGIC FRAMEWORK

FEBRUARY 2010



United States Government Accountability Office
GAO
Report to Congressional Committees

February 2011

HIGH-RISK SERIES

An Update

GAO

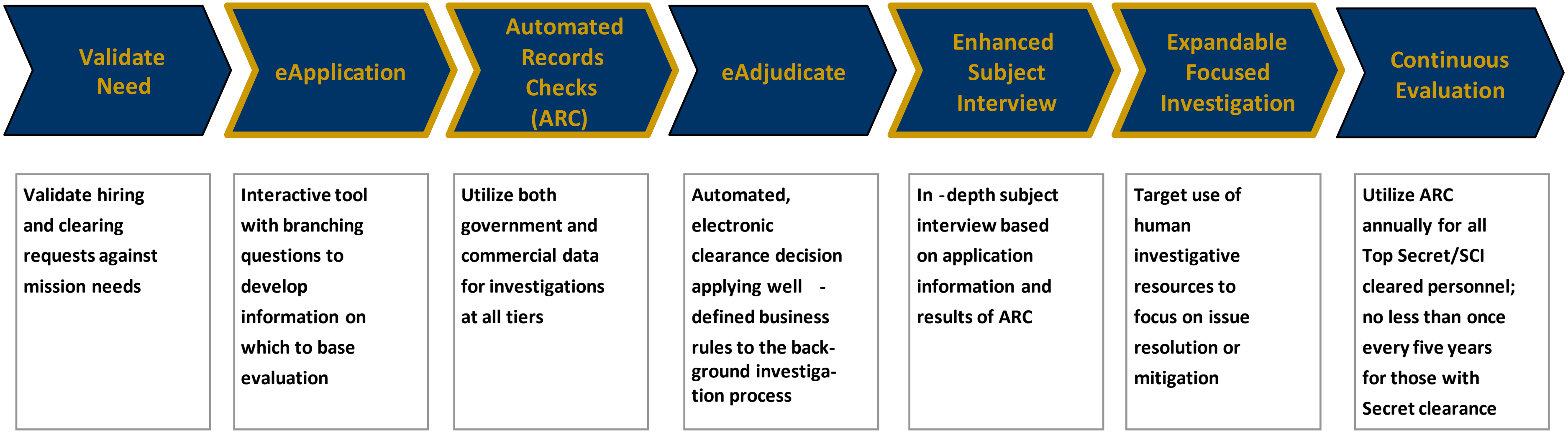
GAO-11-278

GAO
U.S. Government Accountability Office

DoD Removal from GAO "High Risk" List

Joint Reform Team

TRANSFORMED PROCESS



Validate Need: Validate hiring and clearing requests against mission needs

eApplication: Interactive tool with branching questions to develop information on which to base evaluation

Automated Records Checks (ARC): Utilize both government and commercial data for investigations at all tiers

eAdjudicate: Automated, electronic clearance decision applying well-defined business rules to the background investigation process

Enhanced Subject Interview: In -depth subject interview based on application information and results of ARC

Expandable Focused Investigation: Target use of human investigative resources to focus on issue resolution or mitigation

Continuous Evaluation: Utilize ARC annually for all Top Secret/SCI cleared personnel; no less than once every five years for those with Secret clearance

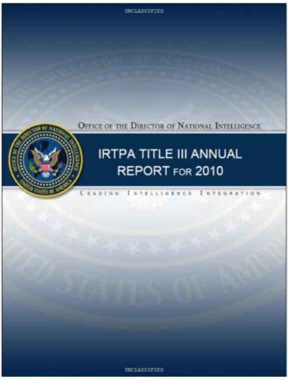
Key Features:

- Data is better used to reduce duplication of requests and ensure consistent quality and standards
- More relevant information is collected and validated at the beginning of the process
- Automation makes the process faster, reduces manual activity and leverages additional data sources
- Field investigative activity is focused to collect and validate targeted information
- Risk decisions rely on modem analytic methods rather than practices that avoid risk
- Continuous evaluation techniques utilize more frequent automated database checks to identify security relevant issues

= modules critical to investigative case flagging strategy

Joint Reform Team

CURRENT STATUS



Office of the Director of National Intelligence

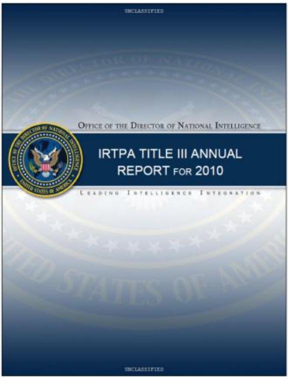
IRTPA TITLE III ANNUAL REPORT FOR 2010

Leading Intelligence Integration

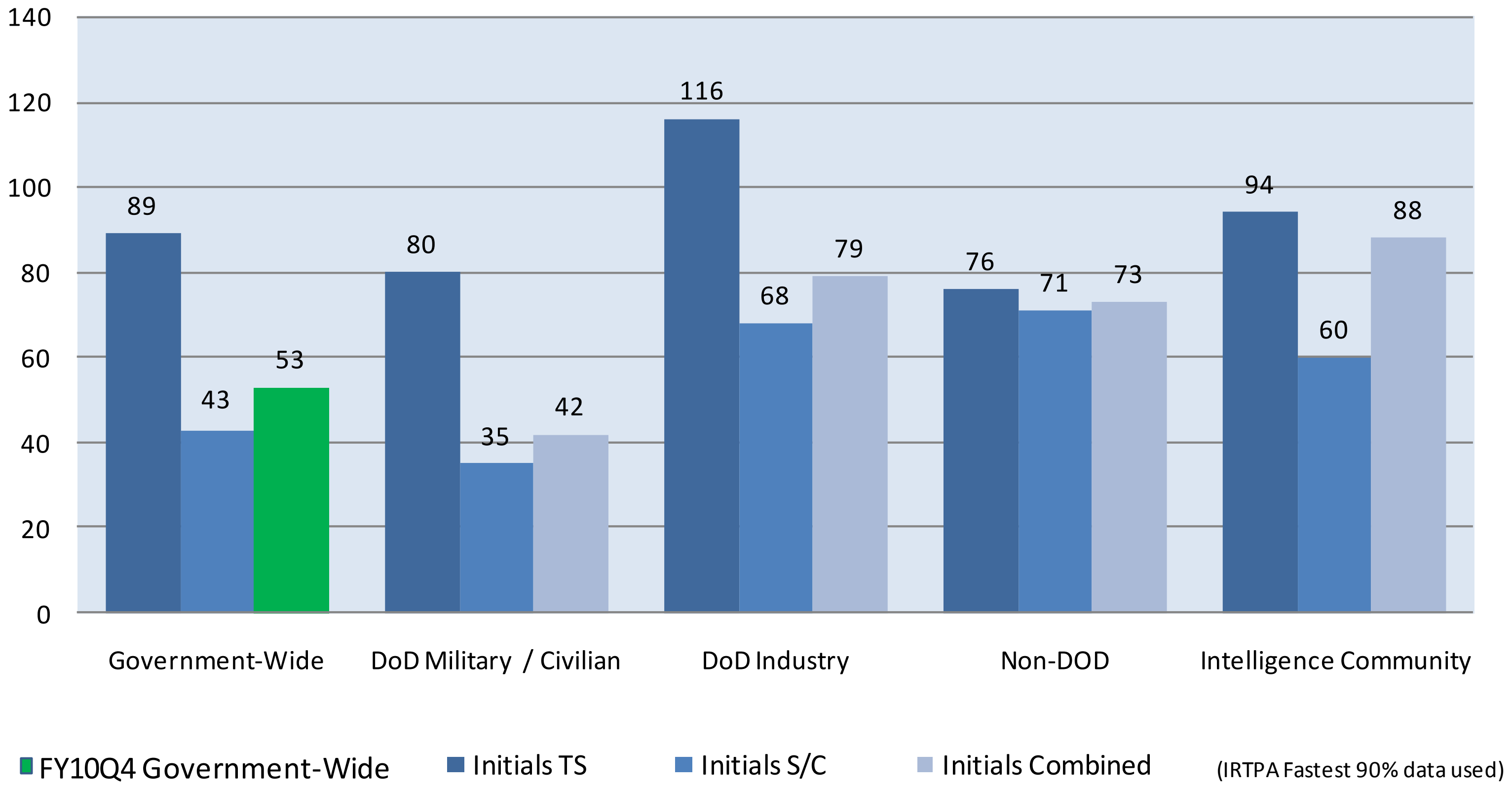
- <u>Timeliness significantly improved over last 5 years:</u>
  - GAO removed DoD clearance program from the High Risk List in February 2011
  - As of December 2010, the Executive Branch averaged **<u>58 days</u>** processing time for fastest 90% of initial clearances (compared to 57 days in 2009 and 165 days in 2006); 2009 IRTPA requirement was met again.
- <u>Maintain focus on Quality:</u>
  - <u>Policy</u>: Investigative criteria clarified, streamlined into five "tiers," and aligned security and suitability to provide consistency needed for reciprocity
  - <u>Technology</u>: Automated data gathering and Quality Control checks gather more accurate data and evaluate completeness of reports
  - <u>Training and Communication</u>: Investigators trained on new standards and Executive Branch-wide exchanges held to implement reform consistently
  - <u>Oversight</u>: Security and Suitability Executive Agent on-site Assessment Programs monitor consistent policy implementation and share best practices to sustain quality
- <u>Enabling Reciprocity:</u>
  - Improved capabilities result in more accurate electronically-collected data, aligned policy and standards, consistent processes, complete and thorough investigative reports, and transparent adjudicative documentation

Joint Reform Team

PERFORMANCE MEASURES


UNCLASSIFIED
Office of the Director of National Intelligence
IRTPA TITLE III ANNUAL REPORT FOR 2010
Leading Intelligence Integration
UNCLASSIFIED

Component Times for Initials, FY10Q4

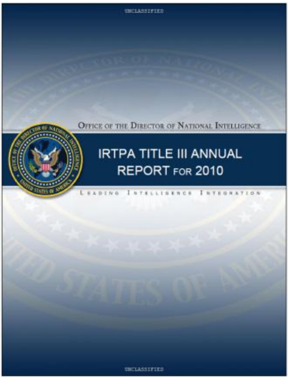


	Initials TS	Initials S/C	Initials Combined
Government-Wide	89	43	53
DoD Military / Civilian	80	35	42
DoD Industry	116	68	79
Non-DOD	76	71	73
Intelligence Community	94	60	88

(IRTPA Fastest 90% data used)

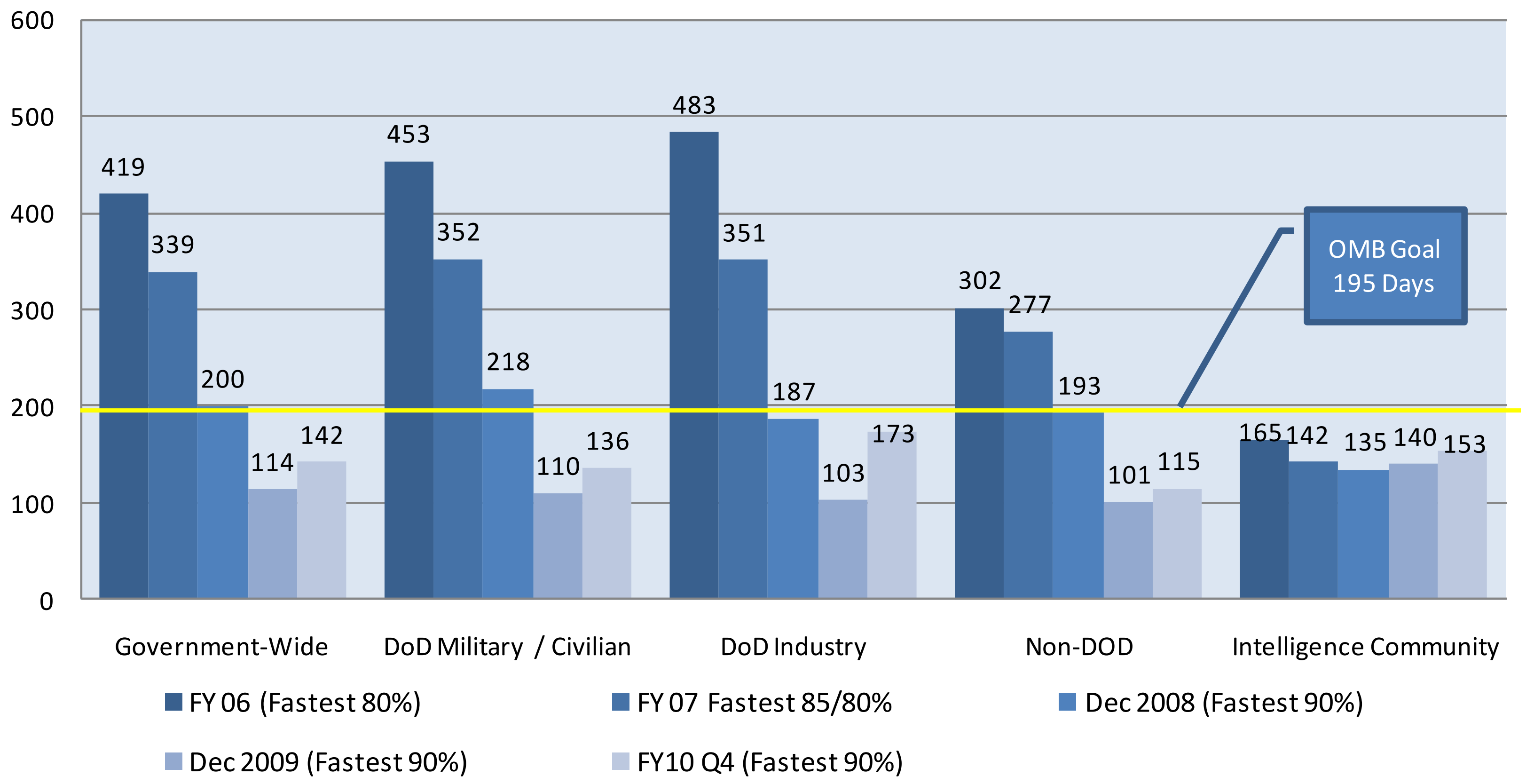
Joint Reform Team

PERFORMANCE MEASURES


Office of the Director of National Intelligence
IRTPA TITLE III ANNUAL REPORT FOR 2010
Leading Intelligence Integration
UNCLASSIFIED

Reinvestigations (IRTPA Fastest 90%)

Average Investigative and Adjudicative Processing Time in Days



Joint Reform Team

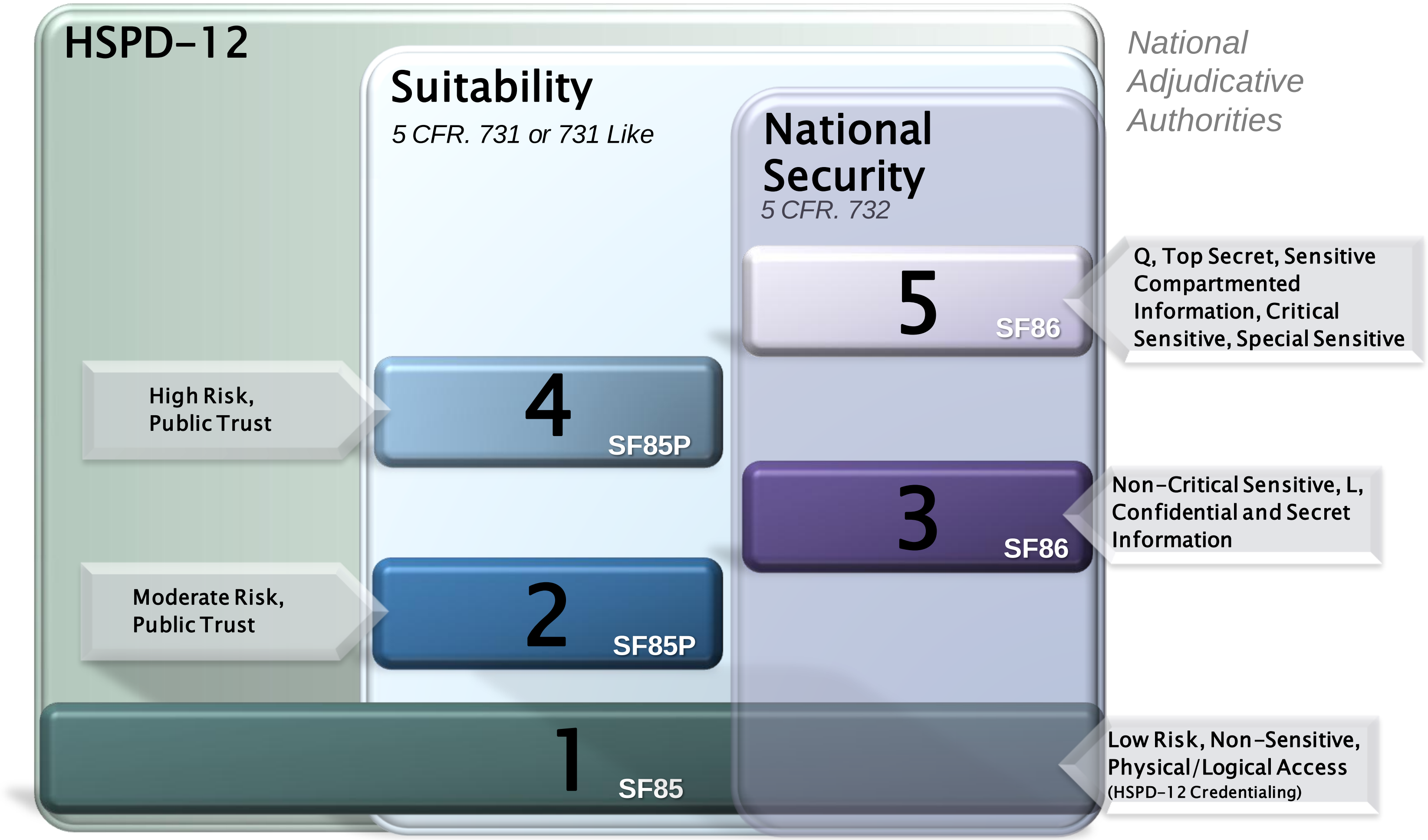
FEDERAL INVESTIGATIVE STANDARDS UPDATE

- Description: JRT formed inter-agency working group to revise the December 2008 Federal Investigative Standards to improve cost, quality, and timeliness of investigations by: aligning suitability and security investigations; facilitating reciprocity; using automation to the greatest extent practicable; and employing the most productive investigative elements, as determined by research
- Status:
  - Original 3 and 4-tiered FIS models redesigned as a 5-tiered system to reflect differences in forms and investigative scope for public trust positions
  - Tiers 1-3
    - FISWG reviewing 198 formal agency comments received in February 2011
    - Comment areas include Tier 2 subject interview, costs, overseas investigations/foreign nationals in addition to more general comments
  - Tiers 4 & 5
    - Expanding model to 5-tiers impacted further development of the revised FIS and extended delivery of remaining tier(s) into CY2011
    - Draft Tier 5 standards expected by March 2011
- Updated FIS will resolve some policy conflicts (e.g. ICD 704 and 1997 FIS)

Joint Reform Team

FEDERAL INVESTIGATIVE STANDARDS

Five-Tiered Investigative Model


HSPD-12
Suitability
5 CFR. 731 or 731 Like
National Security
5 CFR. 732
National Adjudicative Authorities
5
SF86
Q, Top Secret, Sensitive Compartmented Information, Critical Sensitive, Special Sensitive
High Risk, Public Trust
4
SF85P
3
SF86
Non-Critical Sensitive, L, Confidential and Secret Information
Moderate Risk, Public Trust
2
SF85P
1
SF85
Low Risk, Non-Sensitive, Physical/Logical Access
(HSPD-12 Credentialing)

Appendix 4- DAA C&A Presentation

Industrial Security Field Operations (ISFO)

Office of the Designated Approving Authority (ODAA)

Feb 2011

Defense Security Service

Overview:

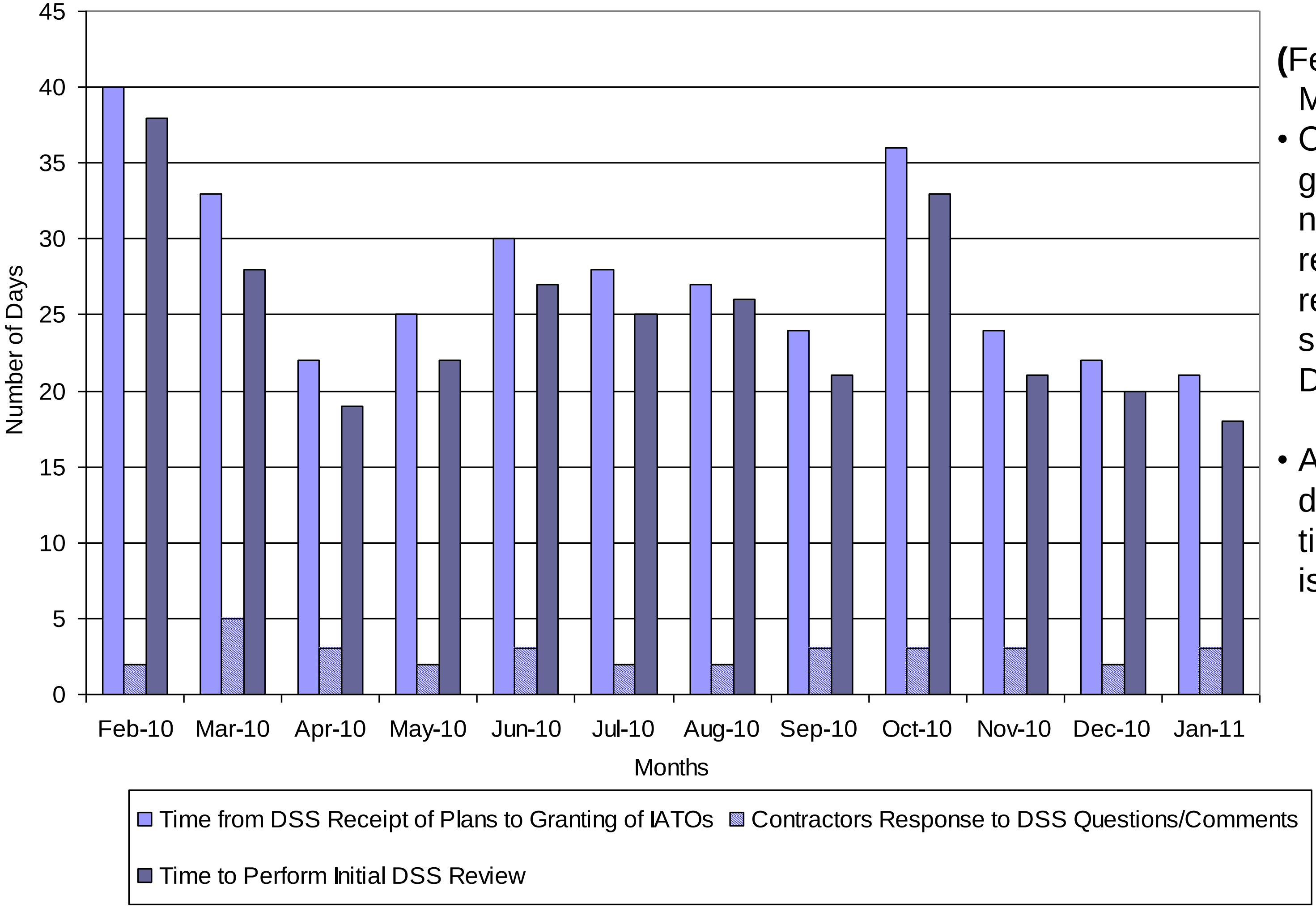
- Certification & Accreditation (C&A)
- C&A Metrics

Certification & Accreditation

- DSS is the primary 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

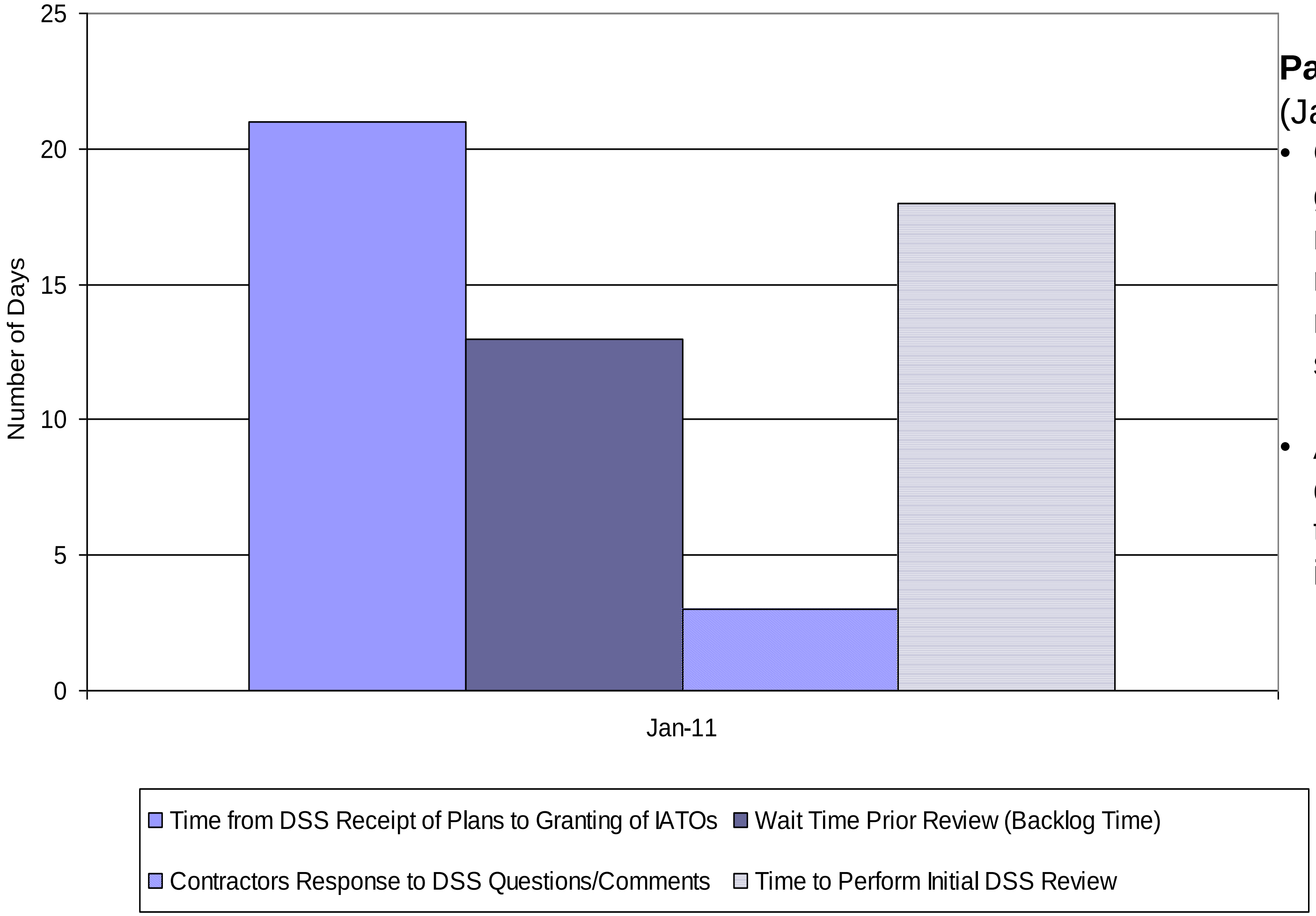


(Feb 2010 – Jan 2011) Metrics

- Out of 3859 IATO's granted the average number of days to receive an IATO after receipt of a submission is 28 Days
- Average number of days for IATO to ATO time to be completed is 84 Days

ODAA Improving Accreditation Timeliness and Consistency

ODAA Metrics for # Days to Process Plan Submissions

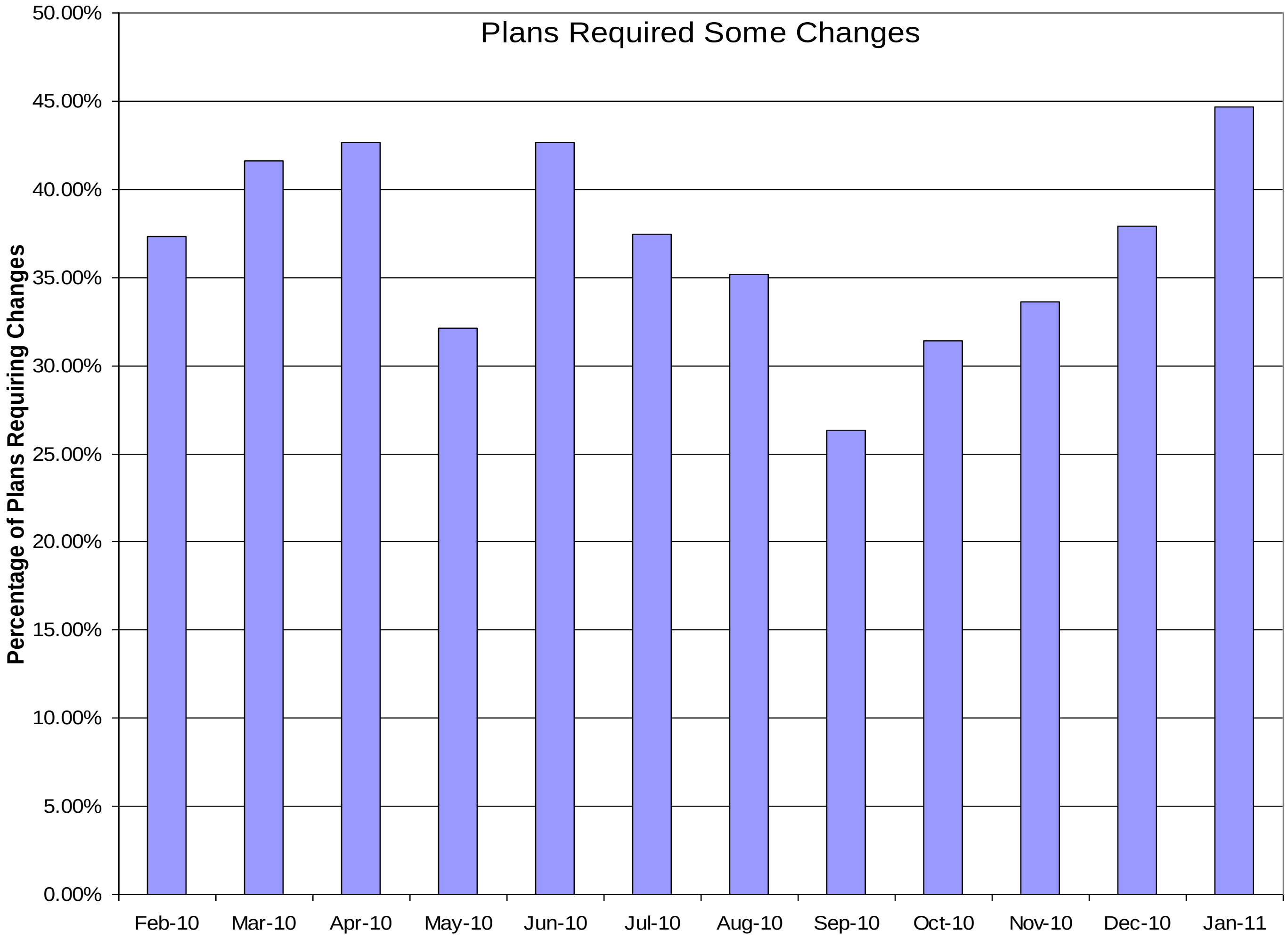


Past One Month
(Jan 2011)

- Out of 317 IATO's granted the average number of days to receive an IATO after receipt of a submission is 21 Days
- Average number of days for IATO to ATO time to be completed is 82 Days

ODAA Metrics
Security Plan Reviews

Review Questions and/or Comments, Errors and Corrections Noted

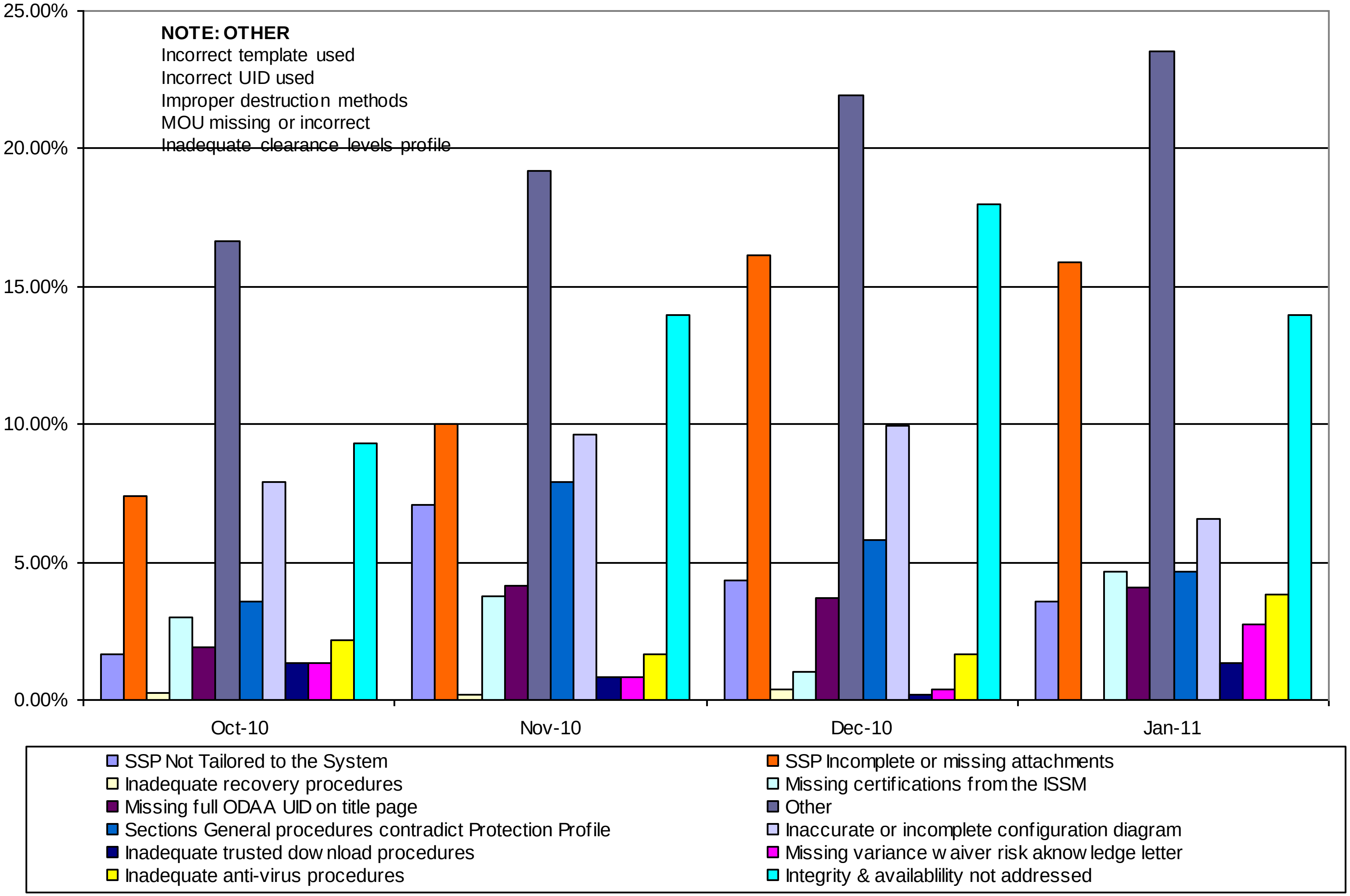


Feb 2010 – Jan 2011

Reviewed 4906 plans:

- On average 36.9% of all plans submitted required changes prior to the On-site Verification for ATO

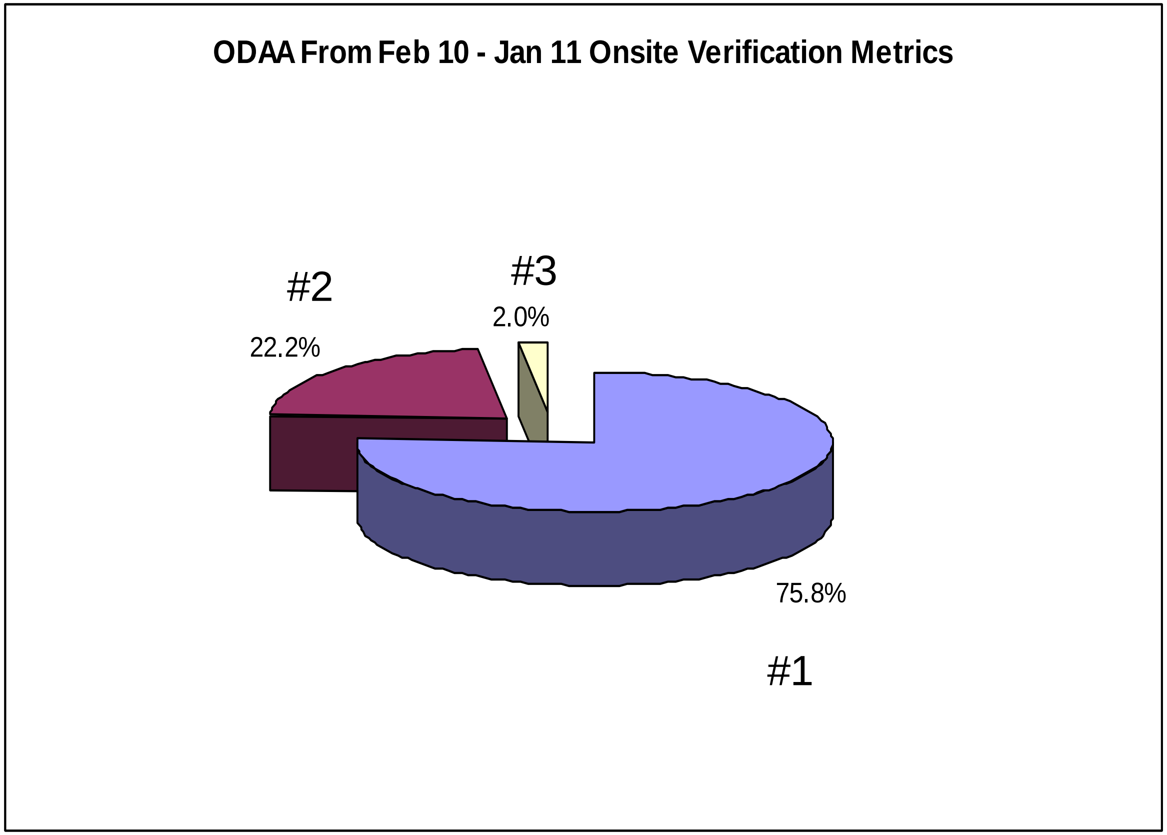
ODAA Metrics
Security Plan Reviews Common Errors



NOTE: OTHER
Incorrect template used
Incorrect UID used
Improper destruction methods
MOU missing or incorrect
Inadequate clearance levels profile

ODAA Metrics and Organization

3662 On-site Verifications (24.2% Required Some Level of Modification)

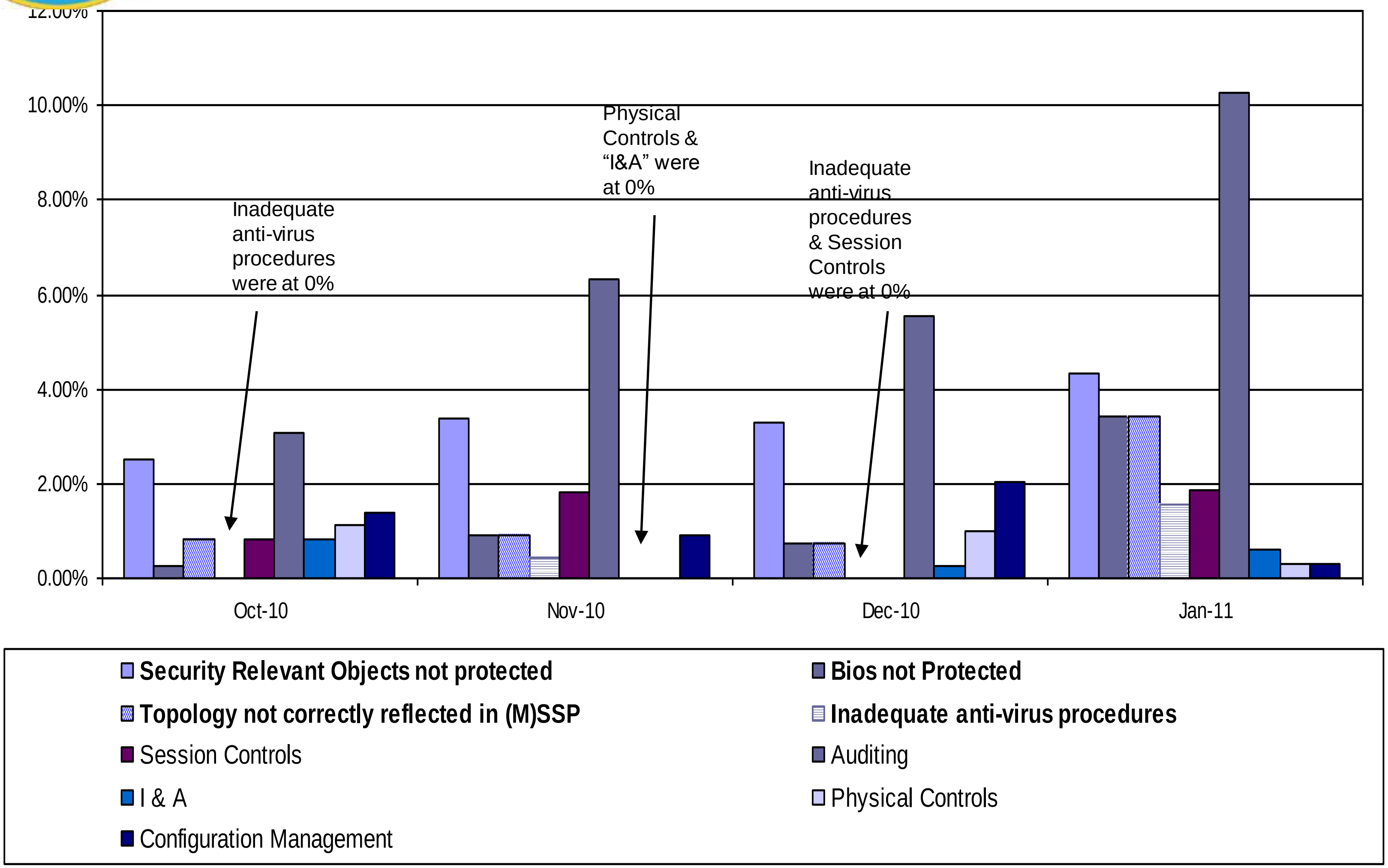


#1. (2775) no discrepancy discovered during on-site validation.

#2. (814) minor discrepancy noted and resolved during on-site validation.

#3. (73) significant discrepancy noted and could not be resolved during on-site validation.

ODAA Metrics
Onsite Plan Reviews Discrepancies



Inadequate anti-virus procedures were at 0%

Physical Controls & "I&A" were at 0%

Inadequate anti-virus procedures & Session Controls were at 0%

Back-Up Slides

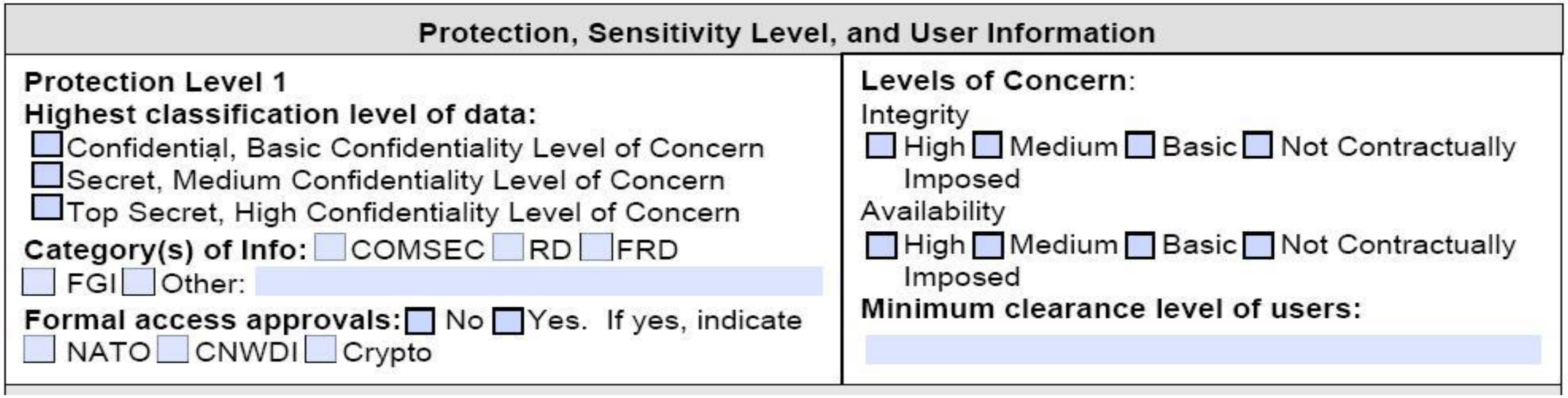
General Reasons for IATO Extensions

There are generally three reasons:

- Conducted on-site that did not result in ATO - may require an extension. (ex. Requires additional documents, Risk Acceptance, POAM.)
- DSS had to postpone an on-site requiring an extension. (Scheduling/resources)
- Contractor had to postpone the on-site that may require an extension.

We are looking at our current processes to determine how/if we can provide the metric in the future.

Integrity and Availability Requirement



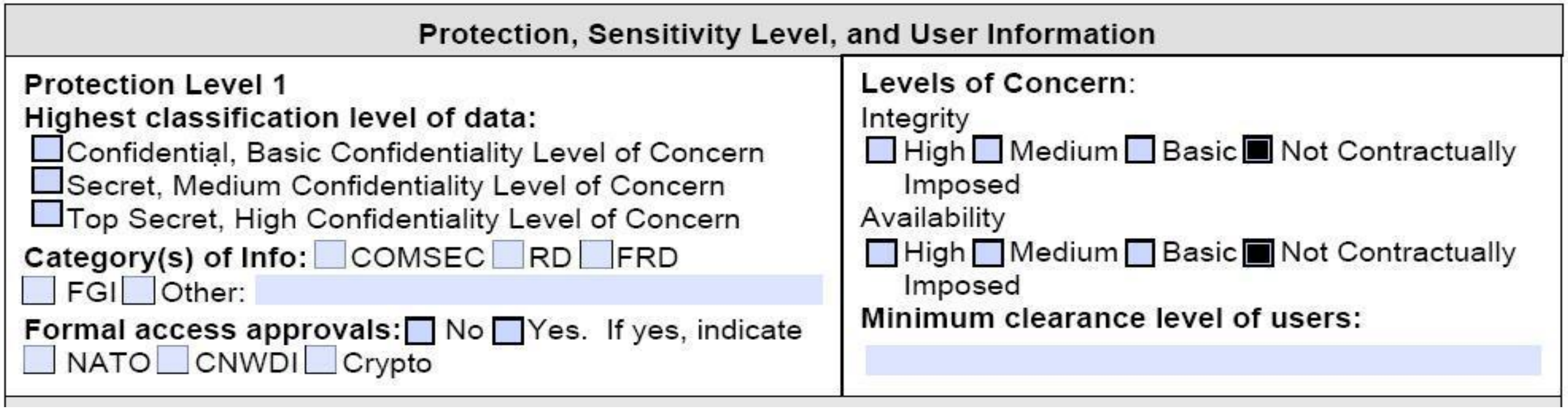
Protection, Sensitivity Level, and User Information

Protection Level 1
Highest classification level of data:
□ Confidential, Basic Confidentiality Level of Concern
□ Secret, Medium Confidentiality Level of Concern
□ Top Secret, High Confidentiality Level of Concern

Category(s) of Info: □ COMSEC □ RD □ FRD
□ FGI □ Other:

Formal access approvals: □ No □ Yes. If yes, indicate
□ NATO □ CNWDI □ Crypto

Levels of Concern:
Integrity
□ High □ Medium □ Basic □ Not Contractually Imposed
Availability
□ High □ Medium □ Basic □ Not Contractually Imposed
Minimum clearance level of users:



Protection, Sensitivity Level, and User Information

Protection Level 1
Highest classification level of data:
□ Confidential, Basic Confidentiality Level of Concern
□ Secret, Medium Confidentiality Level of Concern
□ Top Secret, High Confidentiality Level of Concern

Category(s) of Info: □ COMSEC □ RD □ FRD
□ FGI □ Other:

Formal access approvals: □ No □ Yes. If yes, indicate
□ NATO □ CNWDI □ Crypto

Levels of Concern:
Integrity
□ High □ Medium □ Basic ■ Not Contractually Imposed
Availability
□ High □ Medium □ Basic ■ Not Contractually Imposed
Minimum clearance level of users:

Appendix 5- DMDC JPAS Presentation

DMDC

Information and Technology for Better Decision Making

JPAS Status Update for NISPPAC

Mr. George Angelovic

JPAS PM Support

Personnel Security/Assurance Division

March 3, 2011

Overview

- PK-Enable JPAS
- JPAS Fax Server Ending
- Timeout Policy

Public Key (PK)-Enabling Status Update

- **Phase I (Completed):**
  - JPAS was CAC-Enabled as of January 19, 2010
  - Involved coordination between DSS, DMDC, USDI, and F5
  - Solicited stakeholder guidance and comments
  - Users can now login via Username/Password or CAC for JPAS login
- **Phase II (In Development):**
  - Deployment scheduled for July 23, 2011
  - PIV-Card testing begins mid-June with a select group of Industry users
  - Coordination between DSS, DMDC, USDI, F5 and the Federal Bridge
  - Users will be able to use Username/Password, CAC, and/or PIV for JPAS login
- **Phase III:**
  - Tentatively scheduled for end-CY2011/start-CY2012
  - Will be testing Industry-issued and DoD-approved PKIs
  - Able to use CAC and/or PIV for JPAS login

Fax Server

- JPAS Fax Server Option ending on **May 1, 2011**

- Scan and Upload method is currently available for submission of Signature Pages
  - SF86 Certification
  - Authorization for Release of Information
  - Authorization for Release of Medical Information (when applicable)

- Benefits of using the Scan and Upload feature now:
  - Decrease delays and improve protection of Personally Identifiable Information (PII)
  - Eliminates 25% delay rate for fax submissions
  - Removes unsecure submission method
  - Saves DoD nearly $1M annually by eliminating an inefficient, manual process
  - Resolves data quality issues by 100%. Currently half the faxes need manual attention due to data quality issues
  - Removal of 150 CAT II & 3 CAT III system security vulnerabilities

Timeout Policy Status Update

- **JAMS**
  - Modified timeout policy from current 4 hours to **30 mins**
- **JCAVS**
  - Modified timeout policy from current 45 minutes to **15 mins**
- **Benefits:**
  - Mitigates significant security vulnerabilities to the network, web servers and PII data
  - Complies with DoD Guidance on Protecting PII which states sessions are not to exceed 30 minutes (15 minutes or less rec.)
  - Complies with DISA Unified Capabilities Guidance which requires defaults set at 15 minutes

Communication Plan

- Notification of Changes to Users and Stakeholders
  - DSS JPAS Web Page
  - DMDC JPAS Support Web Page
  - JPAS Welcome Page within the JPAS Application
  - The National Center for Manufacturing Science (NCMS) Web Site
  - Industry Sector Advisory Committee (ISAC) Web Site

- Brief Stakeholders
  - Local Change Control Board (LCCB) Meeting with JPAS Program Management Offices
  - National Industrial Security Program Policy Advisory Committee (NISPPAC) Meeting
  - DSS Industry Stakeholders Meeting
  - DSSS Security Conference

Questions?

Appendix 6- Combined Industry Presentation

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

UPDATE

MARCH 3, 2011

Outline

- Current Membership
  - NISPPAC
  - Industry MOU’s
- Charter
- Working Groups
- Issues/Concerns
- Current and Future Actions

National Industrial Security Program Policy Advisory Committee Industry Members

Members	Company	Term Expires
Sheri Escobar	Escobar Security Consulting	2011
Chris Beals	Fluor Corporation	2011
Scott Conway	Northrop Grumman	2012
Marshall Sanders	SRA	2012
Frederick Riccardi	ManTech	2013
Shawn Daley	MIT Lincoln Laboratory	2013
Rosalind Baybutt	Pamir Consulting LLC	2014
Mike Witt	Ball Aerospace	2014

Industry MOU Members

AIA	Vince Jarvie
ASIS	Marshall Sanders
CSSWG	Randy Foster
ISWG	Mitch Lawrence
Tech America	TBD
NCMS	Tony Ingenito
NDIA	Jim Hallo

National Industrial Security Program Policy Advisory Committee

- Charter
  - Membership provides advice to the Director of the Information Security Oversight Office who serves as the NISPPAC chairman on all matters concerning policies of the National Industrial Security Program
  - Recommend policy changes
  - Serve as forum to discuss National Security Policy
  - Industry Members are nominated by their Industry peers & must receive written approval to serve from the company’s Chief Executive Officer
- Authority
  - Executive Order No. 12829, National Industrial Security Program
  - Subject to Federal Advisory Committee Act (FACA), the Freedom of Information Act (FOIA) and Government Sunshine Act

National Industrial Security Program Policy Advisory Committee Working Groups

- Personnel Security Clearance Processing
- Automated Information System Certification and Accreditation
- NISPOM Review Teams
- DoD SAP Manual Review Team

Industry Areas of Interest

- **Information Sharing – Threat**
- **Certification & Accreditation (C&A) Process Timelines**
- **Personnel Security Clearance Reform**
  - **Consolidating adjudication facilities; Base realignment**
  - **Automated Continuous Evaluation System (ACES) to be implemented in 2-3 years**
  - **JPAS transition to PKI**
- **Industrial Security Policy Modernization**
  - **National Industrial Security Program Operations Manual revision and update**
  - **Department of Defense Special Access Program Manual development**
  - **Industrial Security Regulation, Volume II update**

Industry Areas of Interest

- IT Security Strategy
  - Implement – DFAR regarding IT security DIB-wide
- Insider Threat Programs
  - WikiLeaks problem
  - Increased focus on counterintelligence
  - Governance and governance gaps
- Data Spills
  - Costs & Impact

Industry Areas of Interest

- Defense Industrial Security Clearance Office (DISCO)
  - BRAC Relocation impacting staffing levels
  - Impact: Potential temporary delays in clearance processing
- Future of “NISPOM Supp”
  - Consistent National Policy for Special Security Requirements
  - IC has ICDs and DoD has future “SAP Manual”
  - What of DHS? DoE? Etc?

Thank You