NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

SUMMARY MINUTES OF THE MEETING

The NISPPAC held its 37th meeting on Wednesday, November, 17, 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 7 February 2011.

The following members/observers were present:

- William J. Bosanko (Chairman)
- Daniel McGarvey (Department of the Air Force)
- Pamela Spillman (Department of the Army)
- George Ladner (Central Intelligence Agency)
- Eric Dorsey (Department of Commerce)
- Stanley Sims (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)
- Peter Ambrose (National Aeronautics & Space Administration)
- Dennis Hanratty (National Security Agency)
- Sean Carney (Department of the Navy)
- Kimberly Baugher (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)
- 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 am. After introductions, he recognized the two new Industry representatives, Rosalind Baybutt and Michael Witt, and expressed his appreciation for the service of the two outgoing Industry representatives, Lee Engel and Vince Jarvie, who was also recognized for his service as the Industry Spokesperson.

II. Old Business

Greg Pannoni, Designated Federal Officer and ISOO Associate Director, reviewed the action items from the previous meeting. He stated that the first action item was to form an Ad-hoc NISPPAC Working Group to review the causes of case rejections, and specifically fingerprint card rejections. He advised that this group had met once and received a comprehensive briefing on the Secure Web Fingerprint Transmission (SWFT) system. The group determined that missing fingerprint cards was the primary reason for OPM case rejections noting that only 8% of industry fingerprints were being submitted electronically. The group determined that the objective is to achieve a cost effective and universal capability for submitting fingerprints electronically, by using standardized fingerprint scanning equipment and the SWFT system.

Mr. Pannoni noted the second action item concerned the NISPPAC meeting in June 2011 that is being held in conjunction with the annual training seminar of the National Classification Management Society (NCMS). The meeting will be held from 1:00 to 3:00 p.m. on June 20, 2011 in New Orleans, Louisiana. As the NISPPAC By-laws require a quorum of both Government and Industry members for an official meeting, members were asked to confirm their planned attendance at a June 2011 meeting if it were held in New Orleans, Louisiana by December 31, 2010.

Regarding the third action item, Mr. Pannoni noted that the Certification and Accreditation (C&A) Working Group reviewed the causes and scope of rejections of interim approvals to operate (IATO), the processes followed in the granting of the approval to operate (ATO), and the self certification of information systems. He noted that the working group will incorporate new data regarding IATO and ATO approval timelines into their report. Mr. Pannoni noted self certification was discussed at length, indicated that there is an appreciation for its importance to Industry, and that a performance standard and additional training would enable a more consistent application of self certification authority.

Finally, Mr. Pannoni noted that action item four, which concerned the appointment of two new NISPPAC Industry members, has been completed.

III. Working Group Updates

A) Personnel Security Clearance (PCL) Working Group Report

William Marosy, OPM, reported (appendix 1) on the timeliness performance metrics for Industry PCL submissions, investigations, and adjudications and noted that there were slight increases in every category. He then presented the Industry scheduling trends for Fiscal Years (FY) 2008 through 2010 and noted that more investigations were opened in the third quarter of each FY, which has had an impact on the number of adjudications required in the fourth quarter of the FY. He noted that if this could be balanced across an FY, it would have a positive impact on overall clearance timeliness. In his review of the metrics concerning Industry's overall timeliness trends for the fastest 90% of initial Top Secret and all Secret and Confidential PCL decisions, Mr. Marosy noted that the numbers

were within the 14 days allowed for the initiation of the clearance and the 40 days allowed for the investigation under the Intelligence Reform and Terrorism Prevention Act (IRTPA) standard. Mr. Marosy advised that the trends indicate that Top Secret PCL initiations are exceeding the 14 day goal, while the investigation and adjudication timelines are within the IRTPA standard. He noted the trend for Secret and Confidential PCL decisions were similar, although the adjudication timeline is increasing and the initiation timeline is within 14 days. Regarding Top Secret periodic reinvestigations, (PRs), the initiation time remains steady, but both investigation and adjudication timelines have increased. Scott Conway, Industry, inquired regarding the status of the Government clearance reform efforts. Gina Otto, Office of the Director of National Intelligence, (ODNI), offered to provide an update on clearance reform at the next NISPPAC meeting.

Helmut Hawkins, DSS, then presented the Defense Industrial Security Clearance Office (DISCO) portion of the presentation (appendix 2), noting that in FY 2010 the adjudication inventory decreased, with those less than 21 days old reduced by 27%, those 21-90 days old reduced by 65%, and those 91 days old or greater reduced by 3%. However the inventory of PRs shows a slight increase. He noted that 66% of the PRs are between 21 and 90 days old, 1.5 % are over 90 days old and less than a third are under 21 days old. Regarding Industry cases pending at OPM there was only a marginal increase of .2% between FY 2009 and FY 2010, and an incremental increase in PRs. The overall rejection rate for FY 2010 was 9.8 % with 4.7% of the rejections at DISCO and 5.1% at OPM. He noted that the primary cause of case rejections continues to be missing fingerprint cards.

The Chairman, while noting the overall FY 2010 adjudication inventory reduction, commented that the inventory increase during the fourth quarter of the FY was primarily due to DISCO's ongoing relocation and postulated that we should expect it to further increase. Drew Winneberger, DSS, interjected that DISCO has reinstated mandatory overtime for its adjudicators to help eliminate the backlog, and that the relocation has caused an 80% attrition rate among the adjudicators. He indicated this has created a challenge because DSS must hire new adjudicators in the Washington DC area and have them trained and pre-positioned to support DISCO's workload requirements. He also noted that DISCO is using experienced adjudicators to train the new adjudicators which also impacts resources. The Chairman opined that there is only so much that can be done and as long as the effort is closely monitored to ensure sufficient capability is deployed the issue will eventually be resolved. Stan Sims, DoD, commented on the on-going effort to consolidate the department's clearance adjudication facilities (CAFs). He noted it is expected to produce synergy and identify best practices that will result in improved collaboration between the CAFs. In response to a question from Ms. Baybutt regarding how Industry could help, Mr. Winneberger replied that Industry has been doing a good

job in forecasting investigative requirements, which has helped DSS in accurately planning the level of manpower needed to support the effort. Mr. Hawkins noted that since investigations can be submitted six months in advance, earlier submissions could help even out the fourth quarter spike. He added that while holding back the investigations could have short term benefits, delaying them too long could create cost issues with FY expenditures not occurring as forecasted, resulting in current year funding not being spent.

B) Certification and Accreditation Working Group Report

Mike Farley, DSS, noted that DSS recently funded a contract to create the Office of the Designated Approval Authority business management system which will automate the data DSS currently collects manually and indicated it could be a year before this system becomes operational. He then presented (appendix 3) statistics pertinent to IATOs for FY 2010. He noted that the average time to receive an IATO was 31 days, and 77 days from receiving the IATO to receiving an ATO. He noted that the DSS goal is 30 days to issue an IATO. In response to Mr. Sim's inquiry regarding how these numbers compared with past years, Mr. Farley responded that they were definitely lower, due primarily to Industry becoming familiar with the process and increased resources that allow faster review and turnaround of the plans. Mr. Conway commented that there are locations where these numbers are much higher and suggested an Industry survey or data call to see how the timelines compare. Mr. Pannoni noted that while the IATO to ATO average is 77 days, the IATO extensions beyond the initial 180 day timeframe impacts the contractor's ability to operate effectively and needs to be reviewed. Mr. Farley noted that while there are things that cannot be done under an IATO, such as self certification, contractors can still operate effectively under its authority. Mr. Sims suggested that it might be useful to relay to Industry any trends showing the causes of IATO extensions. The Chairman suggested that a report be provided at the next NISPPAC meeting showing metrics of this issue which over time could be of benefit to Industry.

Mr. Farley continued with the presentation noting that in September 2010 IATO's were issued in an average of 24 days, and the ATOs in an additional 92 days. He explained that system security plan (SSP) reviews identify discrepancies that must be corrected prior to the on-site verification and issuance of the ATO and noted that about one-third of the 4,197 SSPs received in FY 2010 contained such discrepancies. He identified the common errors such as missing forms and lack of proper signatures, as the most prevalent causes of rejections. Mr. Sims commented that more details about the errors could be useful to avoiding repetition of those errors. Ms. Baybutt inquired about the high percentage of SSPs not addressing integrity and availability. Mr. Farley explained that most often information systems are not contractually required to have integrity and availability controls, but the contractor checks the blocks anyway and that raises an issue that has to be resolved prior to the on-site review. While the Chairman suggested that the

form be modified to address this problem, Mr. Farley noted that the form already addresses the issue and suggested more education and attention to detail by the submitters would help fix the problem. Mr. Pannoni inferred that the automation of the process may assist in resolving the issue. Marshall Sanders, Industry, suggested this information be reported to those developing security education and awareness classes, so they can address the issue in their training products. Ms. Baybutt suggested this could be corrected via a phone call instead of rejecting the entire SSP. Mr. Sims stated that DSS would take this for action. The Chairman reiterated that both parties need to collectively seek to solve the problem.

Mr. Farley advised that 21.2 % of SSPs had discrepancies that were identified during the on-site validation. While 18.7% were minor discrepancies and corrected during the validation, the remaining 2.5 % had significant discrepancies that could not be resolved during the on-site review. He concluded his presentation with a review of the on-site discrepancies and noted that auditing and security relevant objects continue to be the main discrepancies documented during the on-site validations.

Before moving to new business, the Chairman discussed the issue of eliminating the use of non-GSA approved security containers for classified storage by October 2012. He reiterated his responsibility to keep checking to ensure progress is being made, and requested updates on Industry compliance in both the spring of 2011 and again in 2012. Mr. Sims agreed and directed DSS to continue its survey of Industry regarding their progress on replacement of non-GSA approved security containers.

IV. New Business

A) Security Degree Update

The Chairman noted that, at the July 2009 NISPPAC meeting, the members received a briefing from the Industry Security Working Group (ISWG) and the DNI Security Education Council on their joint initiative to establish a security degree program to attract more people into the security profession. He then introduced Jay Chambers, DNI, who presented an update on this initiative (appendix 4). Mr. Chambers informed that a goal of the National Intelligence Strategy was to "Develop the Workforce" and that it is being done through education, training, and career development through the Security Education Council, which is made up of members from the 16 intelligence agencies. Stating that the DNI's focus is on security education, Mr. Chambers spoke about the need for the Intelligence Community (IC) to ensure that there is a properly trained workforce for the future. He noted that, with the retirement of a significant number of IC professionals over the next few years, there will be a shortfall in the number of trained security professionals available to the IC. Mr. Chambers reiterated that the vision is to collaborate with academia to develop a security operations degree program that will allow the

Government and Industry to produce future security professionals. He emphasized that there is no comprehensive degree program available that covers all aspects of security as practiced by the Government and its' contractors. He stressed the importance of attracting college students to the security profession and enabling graduates to become effective entry-level security professionals. Mr. Chambers added that the state of the security environment will increase the need for educated and trained security professionals, while the traditional competition for talent between the Government and Industry and between the security profession and other disciplines will remain.

Addressing educational program development, Mr. Chambers noted that the Security Operations Curriculum Working Group, which is composed of more than 60 Government and Industry security professionals who support five functionally oriented Curriculum Requirement Development Teams, have had numerous meetings to identify what capabilities are needed to meet the need for entry-level security professionals in the future. He spoke about the colloquium held among Government, Industry, and academia to identify the academic and occupational skills needed in the security profession, and the outlook for jobs in security operations in both Government and Industry. He noted that academia highlighted the need for internships, subject matter experts and seed money if institutions of higher learning are to be effective in supporting the effort.

Mr. Chambers then outlined a list of skills and requirements garnered from interviews with Government and Industry security directors and panel members. The skills and requirements will be organized into nine categories of academic capabilities, consisting of general, advanced, and discipline-specific courses. Mr. Chambers reviewed the details of the FY 2010 activities that resulted in the marking strategy and award of contracts to universities. He reviewed the planned activities for the next three FYs, which include the commencement of classroom instruction and the construction and maintenance of the infrastructure of the programs. A copy of "*Security Operations 2010: Curriculum and Academic Certification Guidelines for Undergraduate Degree Programs in Security Operations*" was provided after the meeting and is included as an attachment to the minutes.

Mr. Chambers then detailed the two initial programs being developed under grants by Eastern Kentucky University and Embry-Riddle Aeronautical University, as well as an overview of a program proposed by the University of Miami. He provided the following contact information for each program: Eastern Kentucky University, Mike Collier at mike.collier@eku.edu; Embry-Riddle Aeronautical University (Prescott), Bob Baker at bakere9d@erau.edu, and University of Miami, Bruce Bagley at bbagley@miami.edu. He then offered a concept of a nationwide academic network of colleges and universities providing degrees in various aspects of security operations. Mr. Chambers summarized that Government and Industry leaders could no longer rely on talent to be delivered and that they must be actively involved in its development.

Melton Miller, OPM, inquired about how the curriculum was being developed. Mr. Chambers explained that the security operations requirements were being developed using existing curriculum development tools and practices. Mr. Sanders asked what Industry could do to support this initiative. Ms. Otto suggested working through the ISWG which is co-sponsoring this effort. Mr. Sims suggested that we identify those jobs that can be marketed and the job opportunities that will be available. Ms. Otto added that there will be a need for support to academia from Government and Industry in the form of instructors and subject matter experts, and that it is important to look for opportunities to support this program.

B) Recent Changes in Security Policy

The Chairman reviewed recent policy changes, noting that there have been three executive orders in the last year reforming some aspect of the classification management system. Executive Order (E.O.) 13526, *Classified National Security Information*, was issued on December 29, 2009. On August 18, 2010 E.O.13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*, was issued. E.O. 13549 designates the Department of Homeland Security (DHS) as the executive agent for the State, Local, Tribal and Private Sector (SLTPS) program. ISOO has a policy and oversight role similar to that of the National Industrial Security Program (NISP), and the Director of ISOO chairs a Policy Advisory Committee (PAC), which is similar to the NISPPAC. It is expected that some issues and some members will be common to both PACs. He noted that the interagency group advising the National Security Staff went to great lengths to ensure the private sector element of the SLTPS Program does not conflict with the NISP. DHS is required to issue an implementing directive for E.O. 13549 in early 2011.

The Chairman then spoke regarding E.O.13556, *Controlled Unclassified Information*, (CUI), which was issued on November 4, 2010. He noted that this was a collaborative effort that produced an order that would reform the CUI environment. Emphasizing that E.O. 13556 will require no major change for at least a year, the Chairman, outlined actions required in the initial 180 days and in the subsequent six-month period. In noting the effects of the CUI order on Industry, the Chairman discussed the need to include Defense Federal Acquisition Regulation (DFAR) clauses in Government contracts, and advised that patience will be required as the agencies issue new guidance to implement the CUI requirements. Fred Riccardi, Industry, advised that it is premature to place CUI requirements in Requests for Proposals since CUI is at least a year from implementation. The Chairman echoed the advice, stating that agencies prematurely issued CUI implementation guidance in contracts after President Bush's memo in 2008. He advised that it is still premature for agencies to issue such guidance and agencies should continue to issue guidance for their current Sensitive But Unclassified information.

C) DoD Update (Appendix 5)

The Chairman recognized the efforts of Steve Lewis, DoD, and Mr. Pannoni for their work on the first comprehensive revision of the NISP Operating Manual (NISPOM) in several years. Mr. Sims echoed the Chairman's praise to those involved in the revision process. He noted that from the beginning of the revision effort he had insisted on openness and transparency, and this has remained true throughout the process. Commenting that seven working group meetings, comprised of representatives from both Government and Industry, were held between September 9, and November 5, 2010, Mr. Sims noted that the meetings considered 261 comments. He added that 57 comments were fully or partially accepted, and 70 were rejected. In all cases, the submitters were told why their comments were rejected. The review process resulted in 137 action items, and responses for 40 of these items are pending. Mr. Sims noted that once the final action items are resolved, a new draft will be provided to the Government participants for a review of the consolidated comments. The draft will then be published in the Federal Register for public comment. Mr. Sims envisions the revised NISPOM being released in early calendar year 2011. Summarizing on-going activities relating to the DFAR supplement, Mr. Sims noted that guidance for CUI processes would be included in the final wording and that the new clause would be provided by the end of calendar year 2011.

D) Combined Industry Presentation (Appendix 6)

Mr. Conway, Industry Spokesperson, noted the current Industry representation on the NISPPAC, and updated Industry representatives to the Memorandum of Understanding organizations. Mr. Conway commented that the NISPPAC charter remains consistent with Industry's needs, and that the working groups are providing the interaction needed to address the issues of importance to Industry. Mr. Conway noted that the information-sharing and threat-data issue is improving with more Industry interaction through the Federal Bureau of Investigation's Strategic Business Council and through the on-going Secure Internet Protocol Routing Network pilot project. He noted that with the release of the CUI order, the process to implement the CUI program can move forward. The PCL Working Group is addressing clearance reform and the Joint Personnel Adjudication System transition to Public Key Infrastructure requirements. The C&A Working Group continues to look at the process-timeliness issues relating to IATOs and ATOs. Mr. Conway acknowledged the good working relations between Government and Industry and recognized Mr. Riccardi for his monitoring of the CUI activities and Ms. Baybutt for her efforts on the NISPOM revision. Mr. Conway cited the work done on the NISPOM revision and noted that Industry's concern remains with the proposed six month implementation timeframe and potential cost impacts once it is implemented. Regarding Industry watch items, he noted that a proposed DFAR supplement establishes new cyber security requirements for safeguarding unclassified information across the defense

industrial base and that its creation of a two-tier protection scheme will impact all defense contractors. He concluded that CUI is no longer a watch item and noted that Mr. Riccardi will continue to represent Industry on CUI issues.

V. General Open Forum/Discussions

A) Christal Fulton, DHS, reported that her agency has had inquiries regarding the processing of contractors into DHS facilities and advised that industrial security issues should be addressed to Mr. John Young at (202) 447-5337 or (202) 447-5348.

B) Tim McQuiggan, Industry commented on recent requirements on some contracts for random drug testing of employees and asked if the DFAR allows such testing. Mr. Sims commented that DoD would address the issue and report back as appropriate.

VI. Closing Remarks and Adjournment

The Chairman noted that the next two NISPPAC meetings are scheduled for Thursday, March 3, 2011, from 10:00 a.m. to 12:00 noon, at the National Archives, and Monday June 20, 2011, from 1:00 to 3:00 p.m., in New Orleans, Louisiana, in conjunction with the NCMS Annual Training Seminar. He noted that the final meeting for the next calendar year is scheduled for November 16, 2011. The Chairman expressed his sincere thanks to everyone, and the meeting was adjourned at 12:01 p.m.

Summary of Action Items

A) The ODNI agreed to provide an update on the status of the government clearance reform at the March 2011 NISPPAC meeting.

B) The Chairman requested that metric and trend data regarding causes of IATO extensions be included in the C&A Working Group report at the March 2011 NISPPAC meeting.

C) DSS will report on efforts to resolve issues pertaining to the designation of integrity and availability requirements for information systems security plans.

D) DSS will provide a report on Industry's progress in replacing non-GSA security containers at both the March 2011 and the first 2012 NISPPAC meetings.

E) DoD will report to the NISPPAC on whether the DFAR permits random drug testing of contractor personnel.

Appendix 1-OPM-PCL Presentation

Appendix 2-DSS-PCL Presentation

Appendix 3- ISFO –C&A Presentation

Appendix 4- Security Degree Presentation

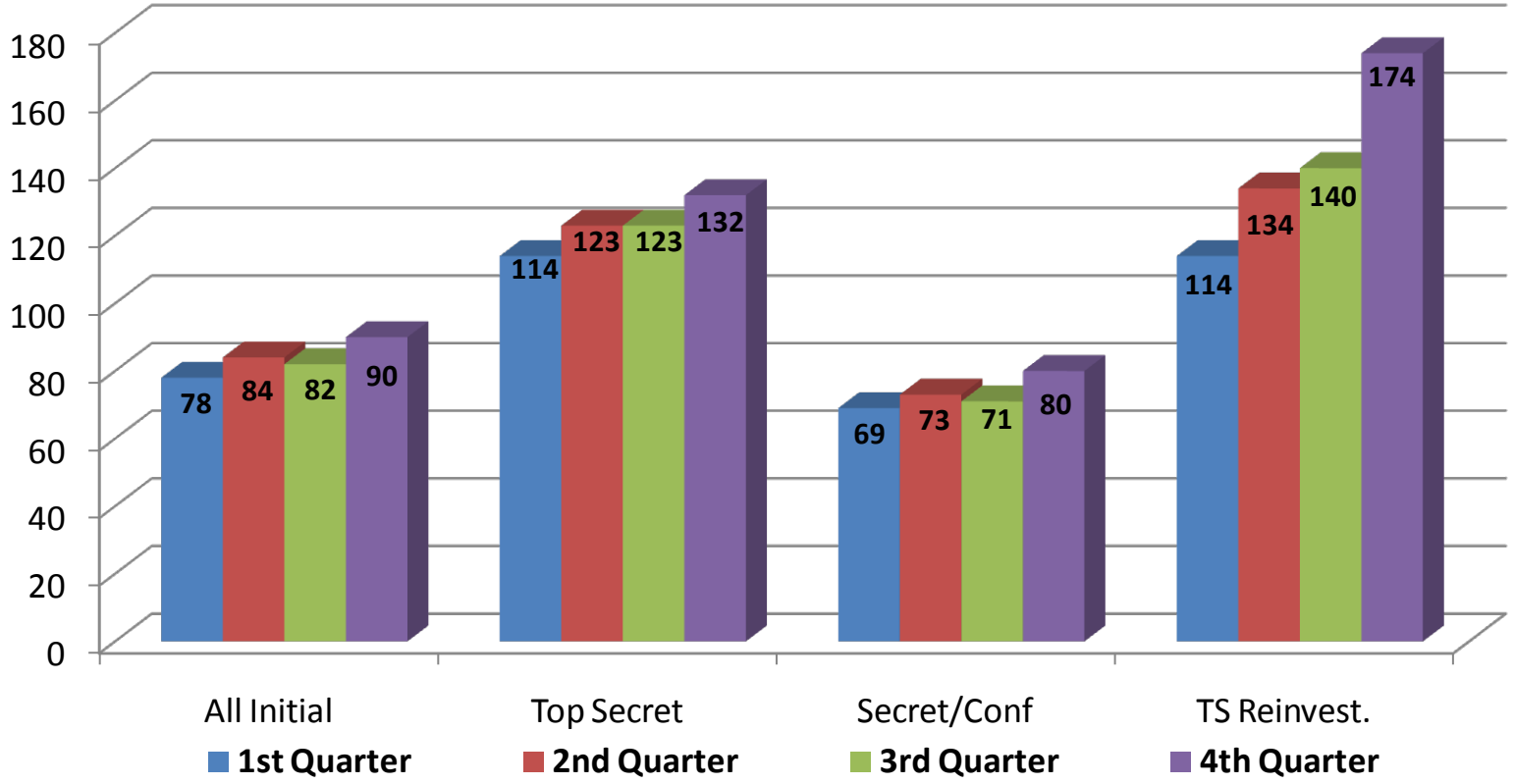
Appendix 5-DoD Update Presentation

Appendix 6- Combined Industry Presentation

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

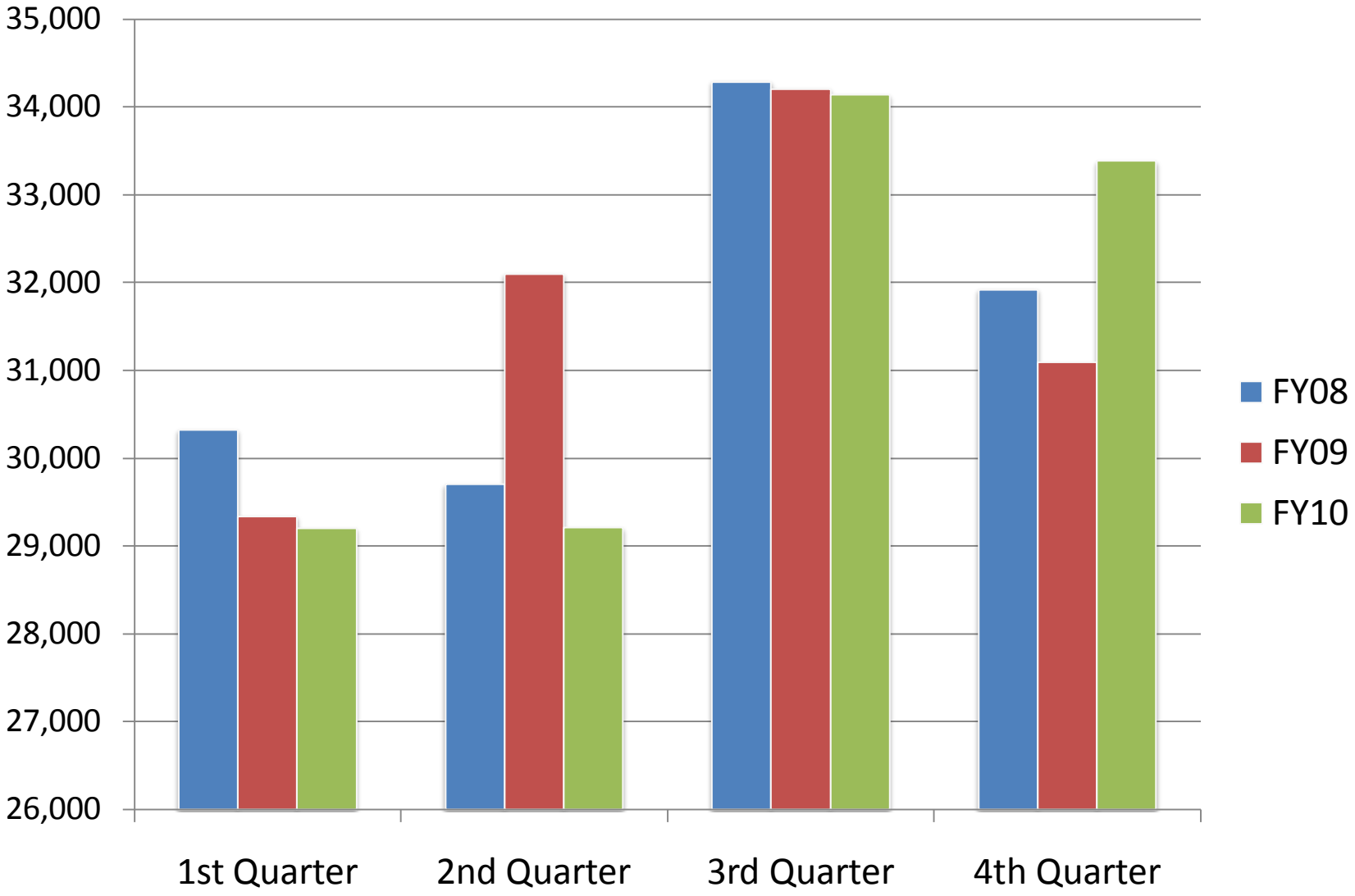


	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 1st Q FY10	31,439	6,709	24,730	5,360
Adjudication actions taken – 2nd Q FY10	23,143	5,210	17,933	4,611
Adjudication actions taken – 3rd Q FY10	25,027	5,422	19,605	5,320
Adjudication actions taken – 4th Q FY10	25,446	5,247	20,199	4,051

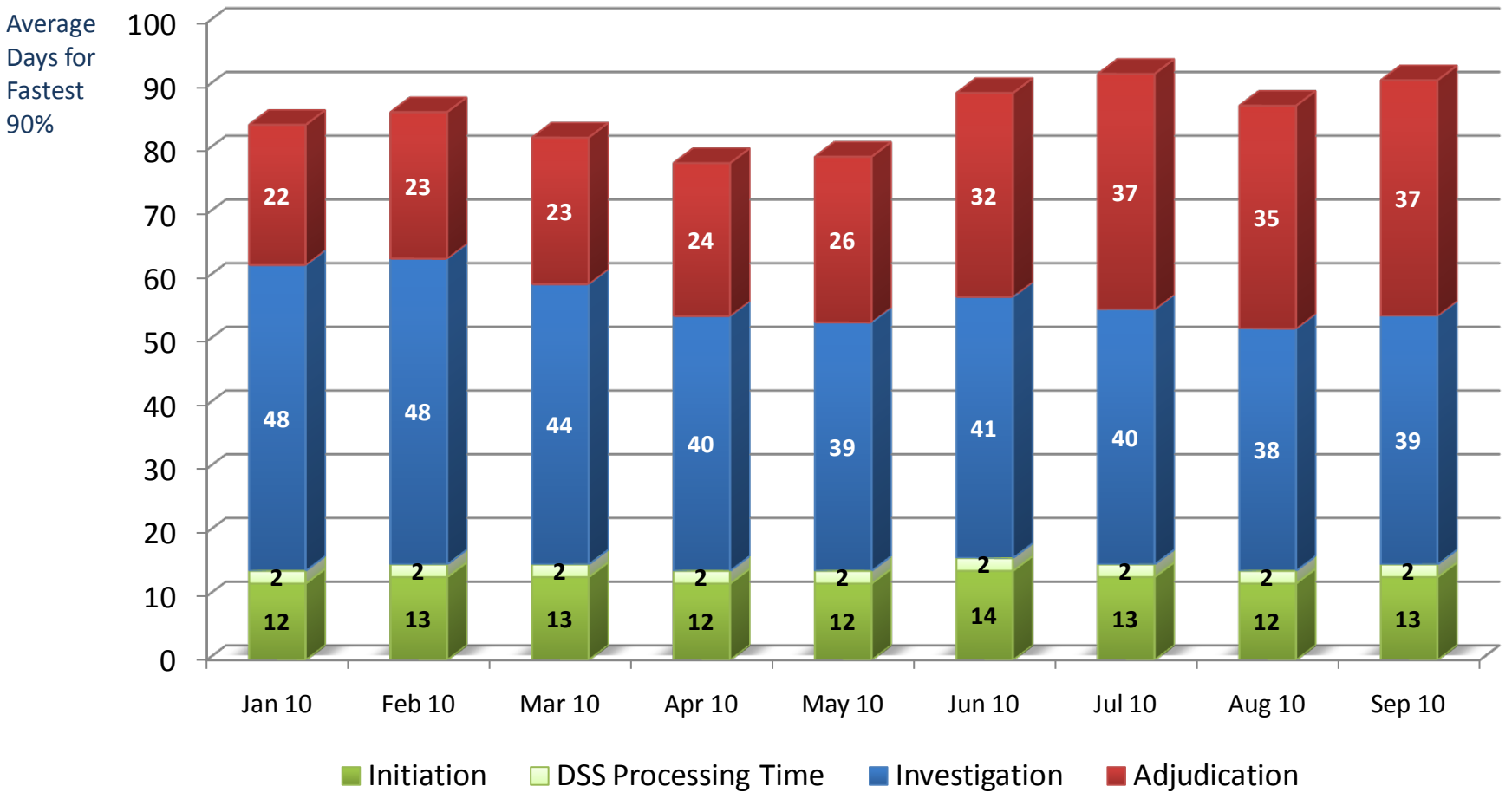
*The adjudication timelines include collateral adjudication by DISCO and SCI adjudication by other DoD adjudication facilities

DISCO Scheduled Trends

All Initial Top Secret & Secret/Confidential

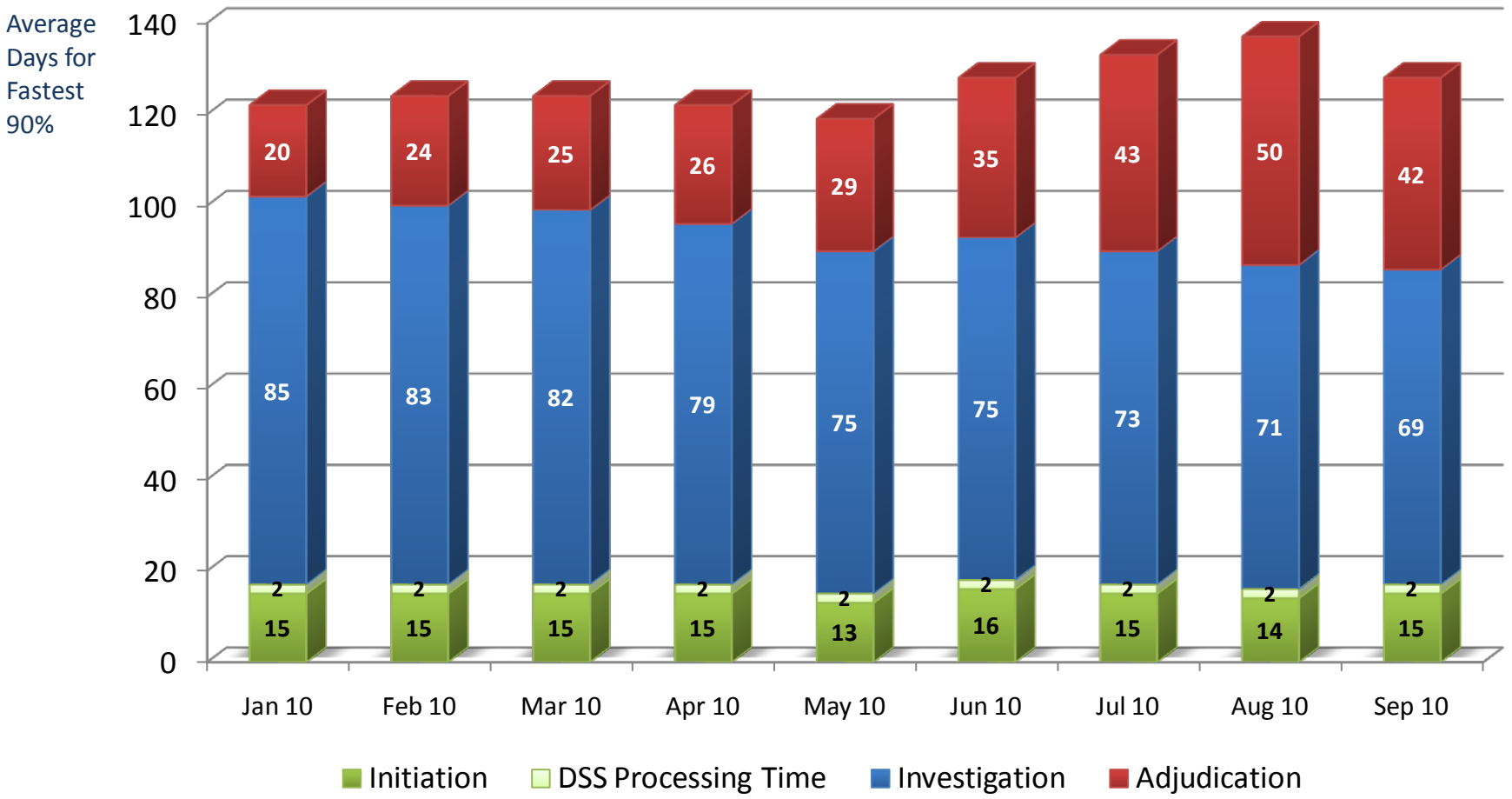


Industry's Average Timeliness Trends for 90% Initial Top Secret and All Secret/Confidential Security Clearance Decisions



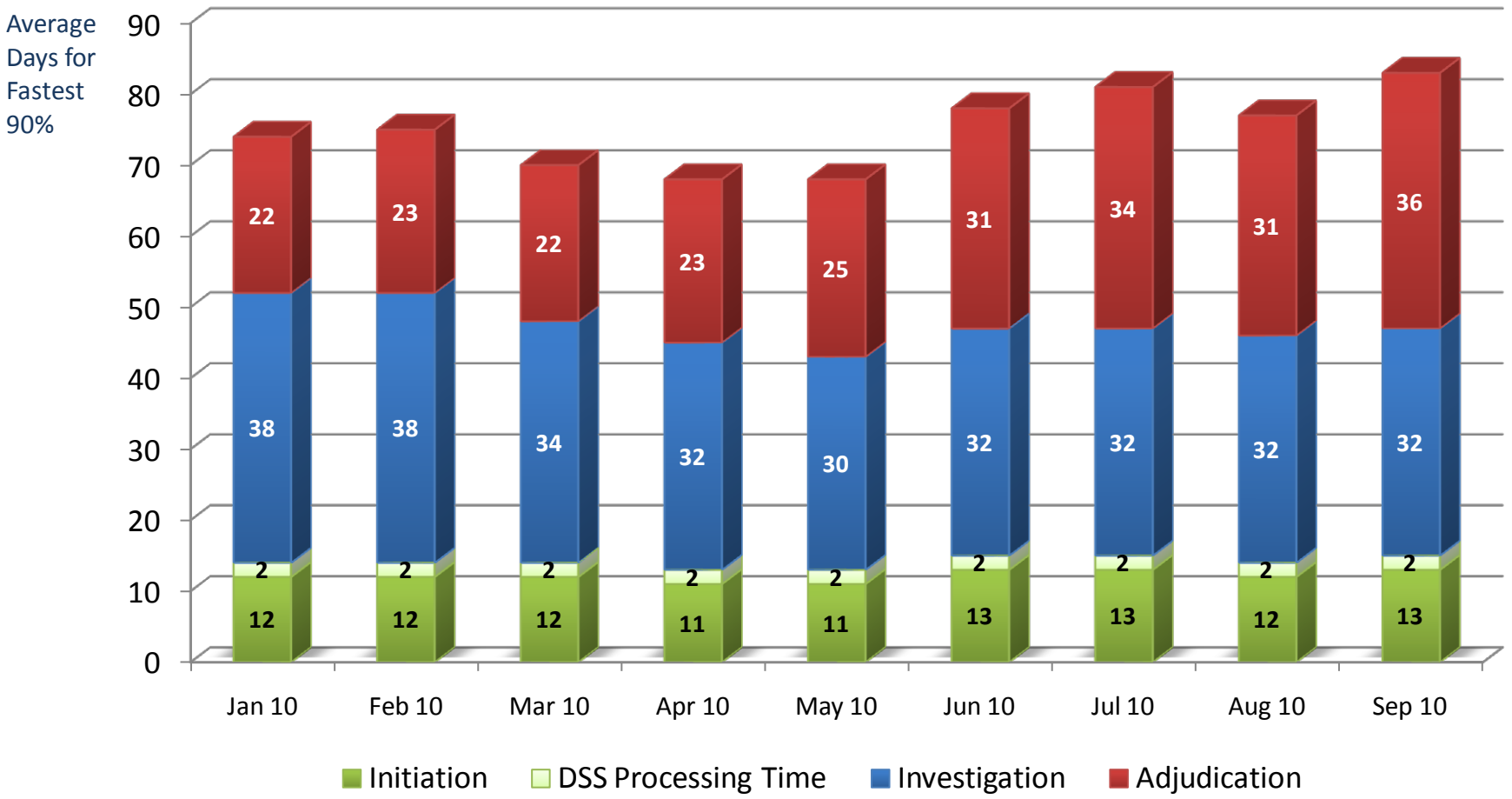
	Jan 10	Feb 10	Mar 10	Apr 10	May 10	Jun 10	Jul 10	Aug 10	Sep 10
100% of Reported Adjudications	7,604	6,560	8,953	8,245	7,903	8,531	6,037	10,235	9,233
Average Days for fastest 90%	84 days	86 days	82 days	78 days	79 days	89 days	92 days	87 days	91 days

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



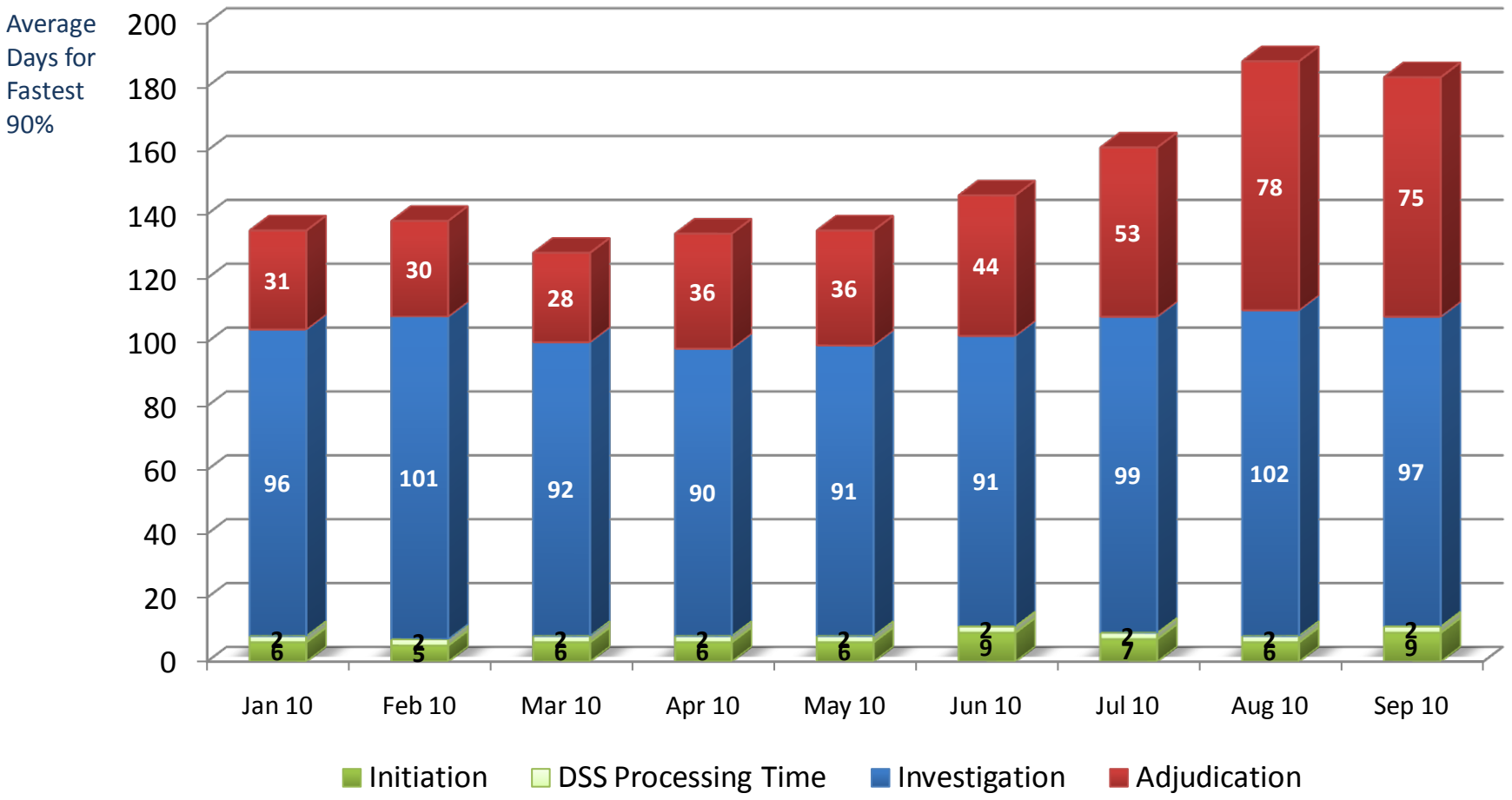
	Jan 10	Feb 10	Mar 10	Apr 10	May 10	Jun 10	Jul 10	Aug 10	Sep 10
100% of Reported Adjudications	1,641	1,537	2,030	1,575	1,825	1,935	1,330	1,975	1,964
Average Days for fastest 90%	122 days	124 days	124 days	122 days	119 days	128 days	133 days	137 days	128 days

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



	Jan 10	Feb 10	Mar 10	Apr 10	May 10	Jun 10	Jul 10	Aug 10	Sep 10
100% of Reported Adjudications	5,963	5,023	6,923	6,670	6,078	6,596	4,707	8,260	7,269
Average Days for fastest 90%	74 days	75 days	70 days	68 days	68 days	78 days	81 days	77 days	83 days

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



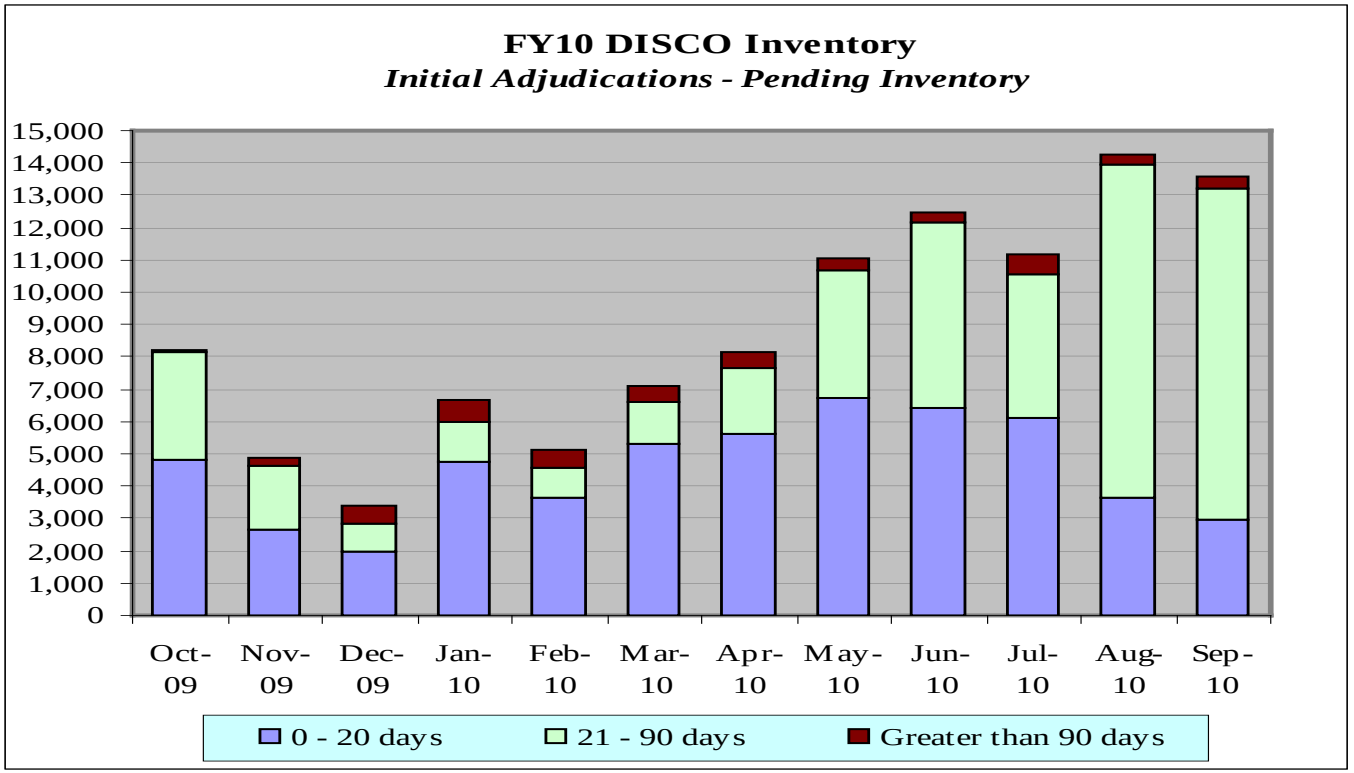
	Jan 10	Feb 10	Mar 10	Apr 10	May 10	Jun 10	Jul 10	Aug 10	Sep 10
Reported Adjudications	1,322	1,376	1,857	1,643	1,513	1,917	1,423	1,170	1,497
Average Days for fastest 90%	135 days	138 days	128 days	134 days	135 days	146 days	161 days	188 days	183 days

Appendix 2-DSS-PCL Presentation

DISCO

FY10 Adjudication Inventory

Initial Clearance Adjudications



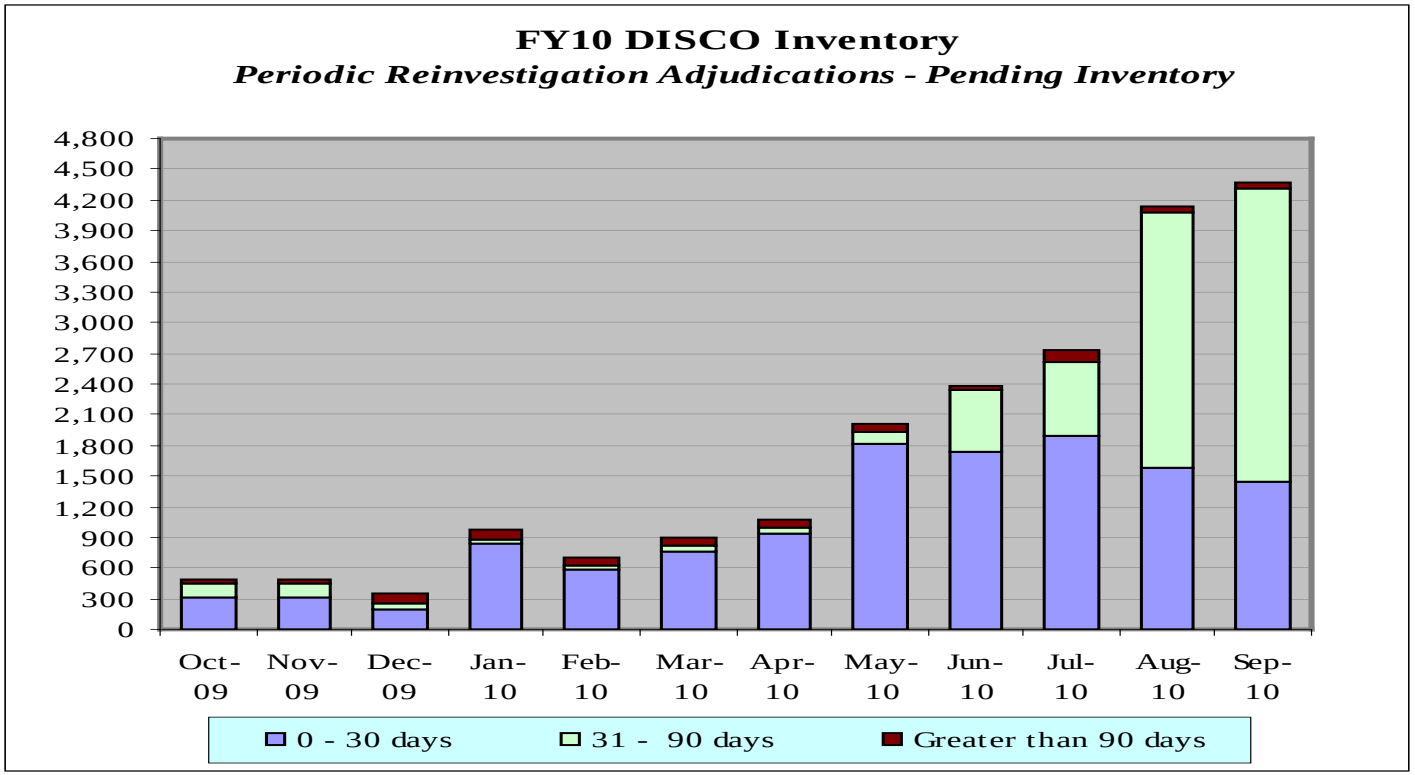
Category	Oct-09	Nov-09	Dec-09	Jan-10	Feb-10	Mar-10	Apr-10	May-10	Jun-10	Jul-10	Aug-10	Sep-10
0 - 20 days	4,797	2,650	2,002	4,752	3,656	5,331	5,642	6,759	6,414	6,087	3,666	2,975
21 - 90 days	3,349	1,987	840	1,238	890	1,247	2,012	3,935	5,728	4,470	10,288	10,210
Greater than 90 days	91	269	557	653	591	550	505	374	315	599	315	379
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

Source: JPAS and CATS

DISCO

FY10 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
0 - 30 days	308	312	201	831	586	761	946	1,812	1,733	1,890	1,583	1,437
31 - 90 days	133	135	54	53	47	56	55	113	599	722	2,496	2,877
Greater than 90 days	47	37	87	82	73	71	73	82	51	111	50	58
Grand Total	488	484	342	966	706	888	1,074	2,007	2,383	2,723	4,129	4,372

Source: JPAS and CATS

FY10 INDUSTRY CASES AT OPM

Investigation Inventory

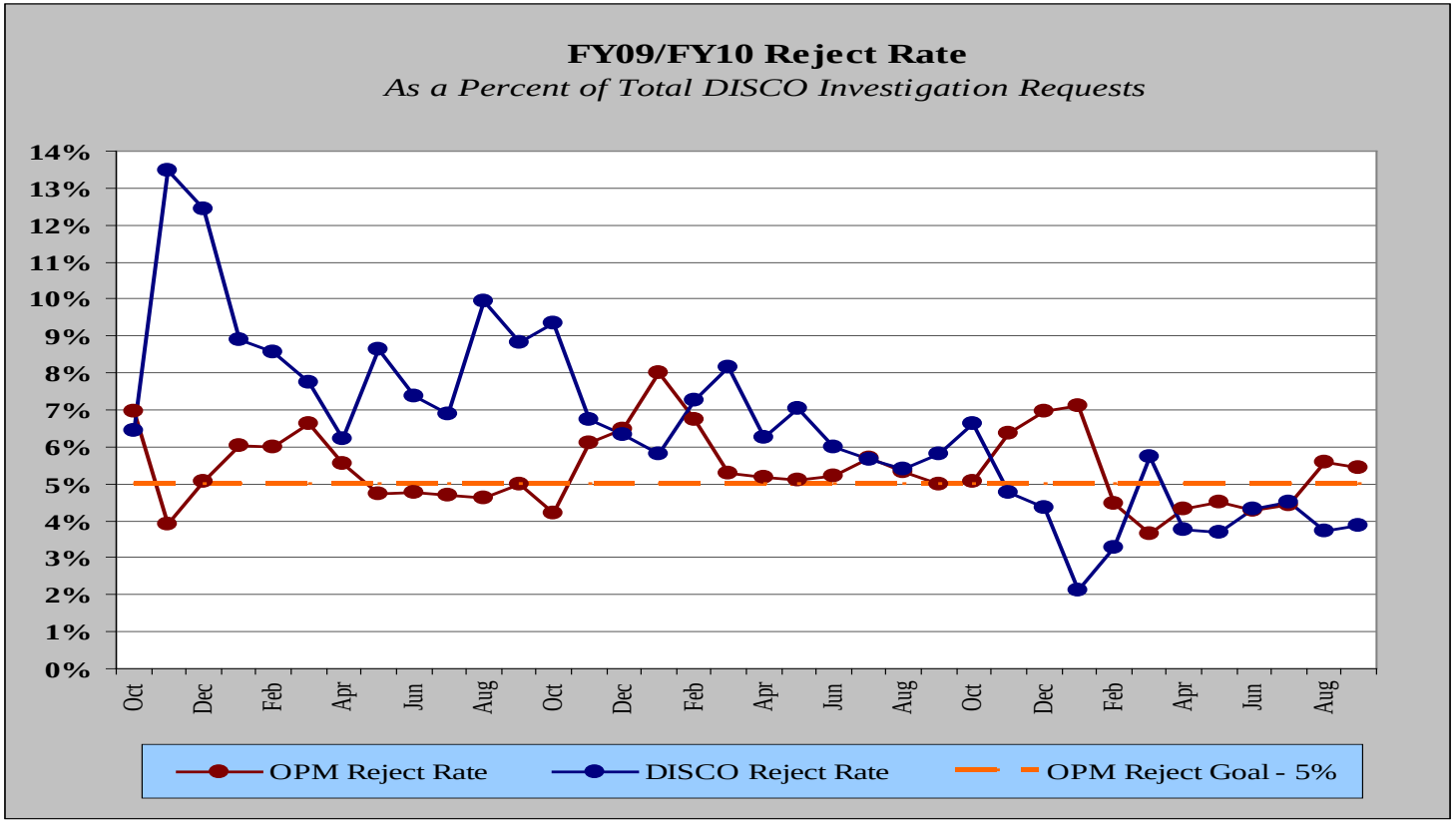
Case Type	FY 08				FY 09				FY 10				Delta Q1FY09 through Q4FY10
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
NACLC	29,575	25,085	22,077	15,561	13,209	13,982	13,900	12,307	11,730	11,685	13,016	13,556	*2.6%*
SSBI	14,110	8,796	7,404	6,720	6,626	6,687	6,944	6,561	6,782	7,012	6,561	6,178	*-6.8%*
SSBI-PR	11,761	9,943	5,639	4,167	3,772	4,160	4,692	3,703	4,096	4,521	4,859	5,115	*35.6%*
Phased PR	7,711	7,749	6,734	6,408	5,430	2,771	2,476	2,640	3,158	3,629	3,665	4,248	*-21.8%*
Total Pending	**63,157**	**51,573**	**41,854**	**32,856**	**29,037**	**27,600**	**28,012**	**25,211**	**25,766**	**26,847**	**28,101**	**29,097**	*0.2%*

Overall marginal increase of .2% for NACLC, SSBI, SBPR and Phased PR case types from 1QFY09 to 4QFY10.

Source: OPM Customer Support Group

FY10 REJECT RATE

Initial and Periodic Reinvestigation Requests



- **FY10: DISCO approved 160K investigation requests**
  - **Rejects –** A total of **15,724 (9.8%)** of incoming investigation requests rejected back to FSOs
    - DISCO rejected **7,508 (4.7%)** investigation requests to FSOs for re-submittal
    - OPM rejected **8,216 (5.1%)** 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

FY10 REJECTS

DISCO Front-End Statistics

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

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

Category	NACLC	PPR	SSBI	Overall % by Category
A/AA	*3%*	*3%*	*3%*	*3%*
B	*2%*	*3%*	*2%*	*2%*
C	*6%*	*13%*	*10%*	*8%*
D	***29%***	***36%***	***29%***	***30%***
E	***60%***	***44%***	***56%***	***57%***
	100%	*100%*	*100%*	*100%*

Source: Monthly JPAS Reports

Appendix 3- ISFO –C&A Presentation

Defense Security Service

Industrial Security Field Operations (ISFO)

Office of the Designated Approving Authority (ODAA)

Oct 2010

Defense Security Service

Overview:

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

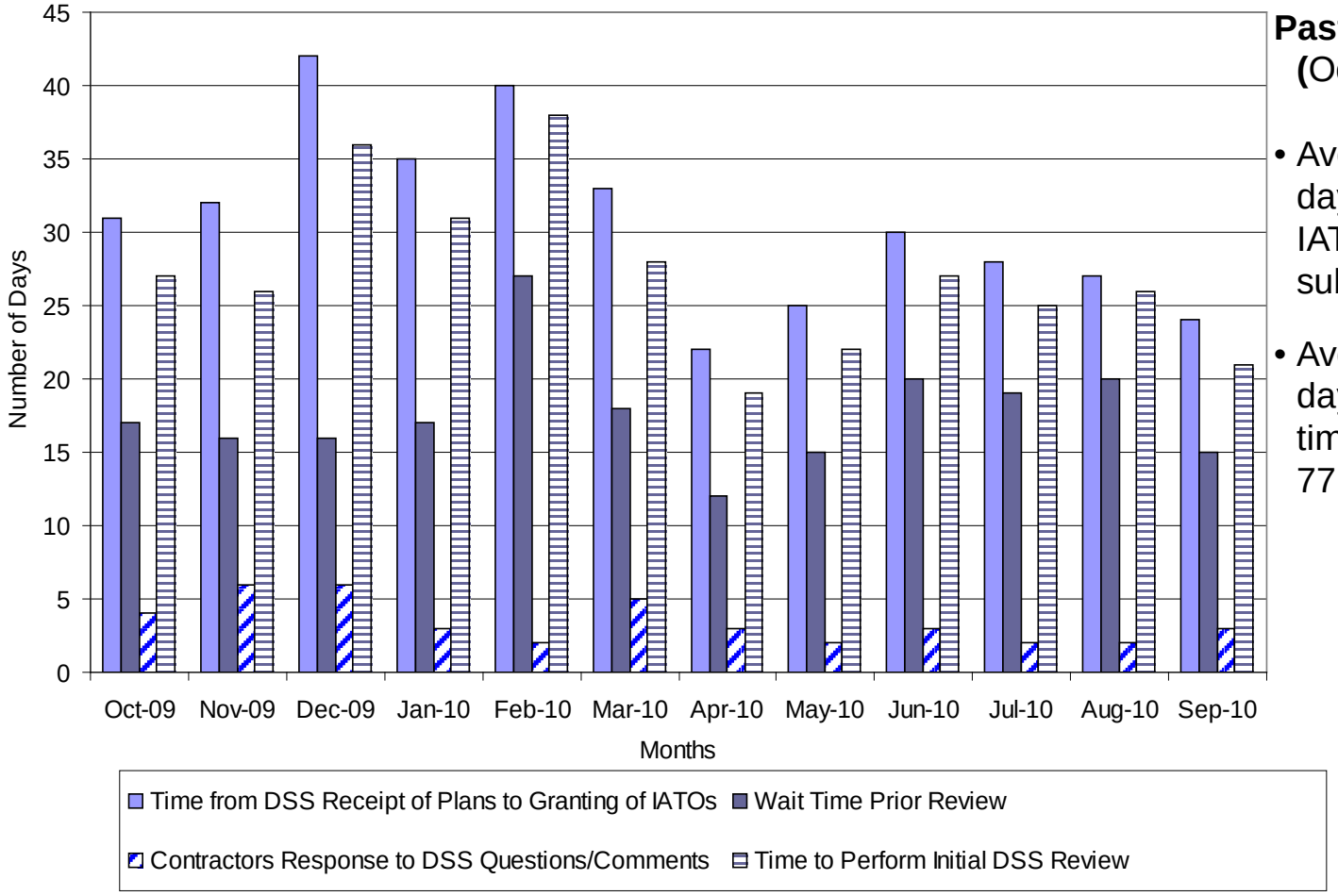
Defense Security Service

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

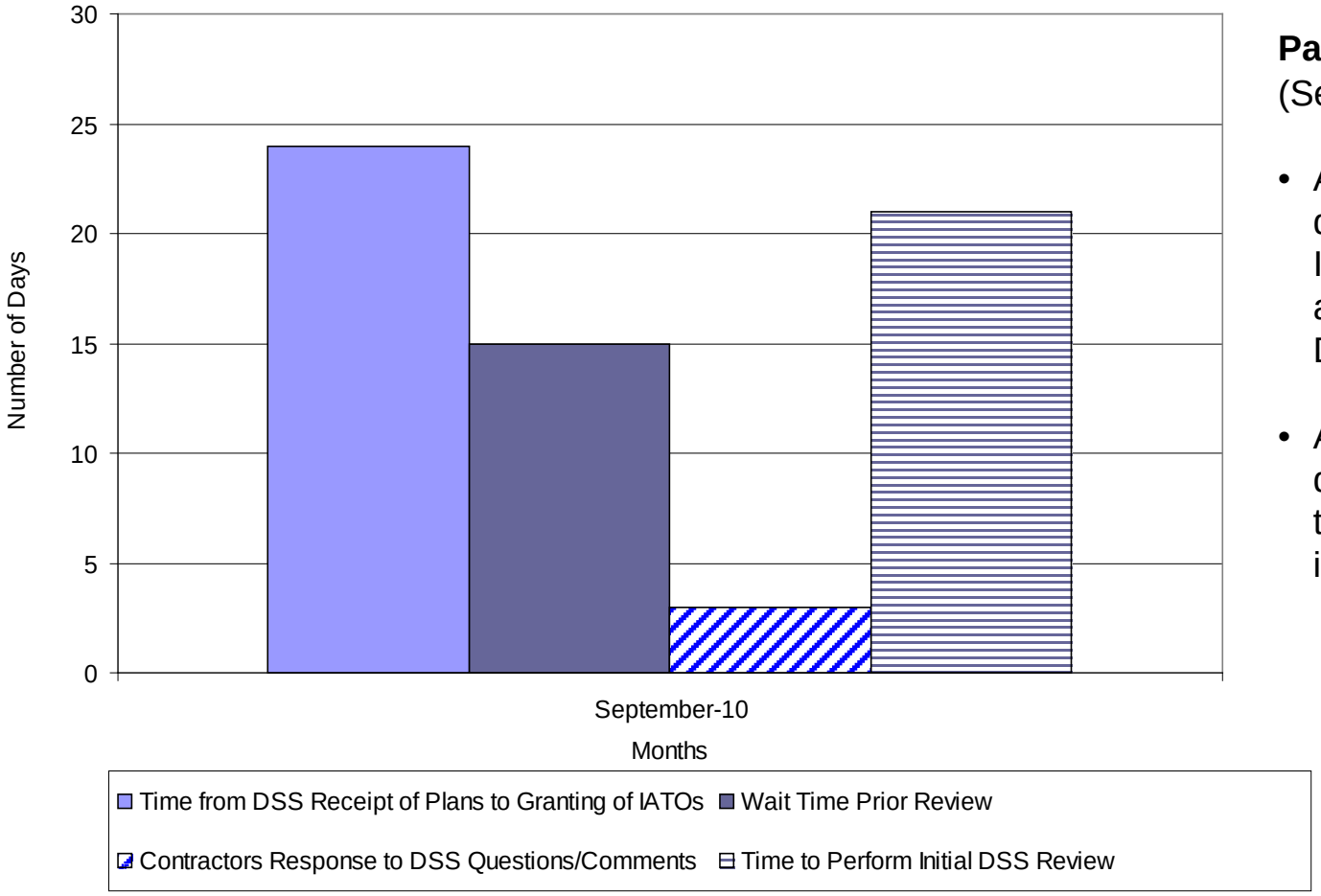


Past Twelve Months:
(Oct 2009 – Sep 2010)

- Average number of days to receive an IATO after receipt of a submission is 31 Days
- Average number of days for IATO to ATO time to be completed is 77 Days

ODAA Improving Accreditation Timeliness and Consistency

ODAA Metrics for # Days to Process Plan Submissions

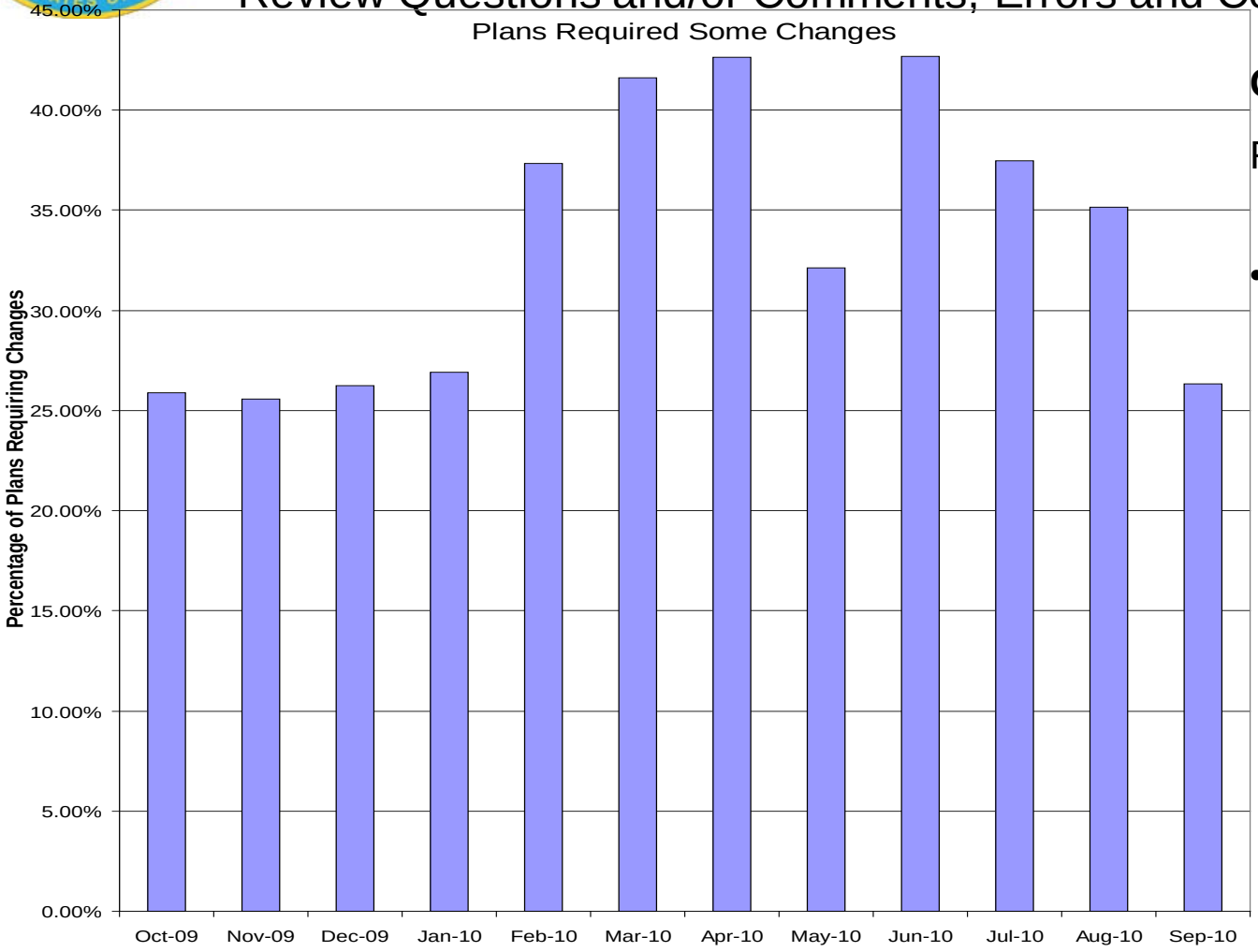


Past One Month
(Sep 2010)

- Average number of days to receive an IATO after receipt of a submission is 24 Days
- Average number of days for IATO to ATO time to be completed is 92 Days

ODAA Metrics
Security Plan Reviews

Review Questions and/or Comments, Errors and Corrections Noted

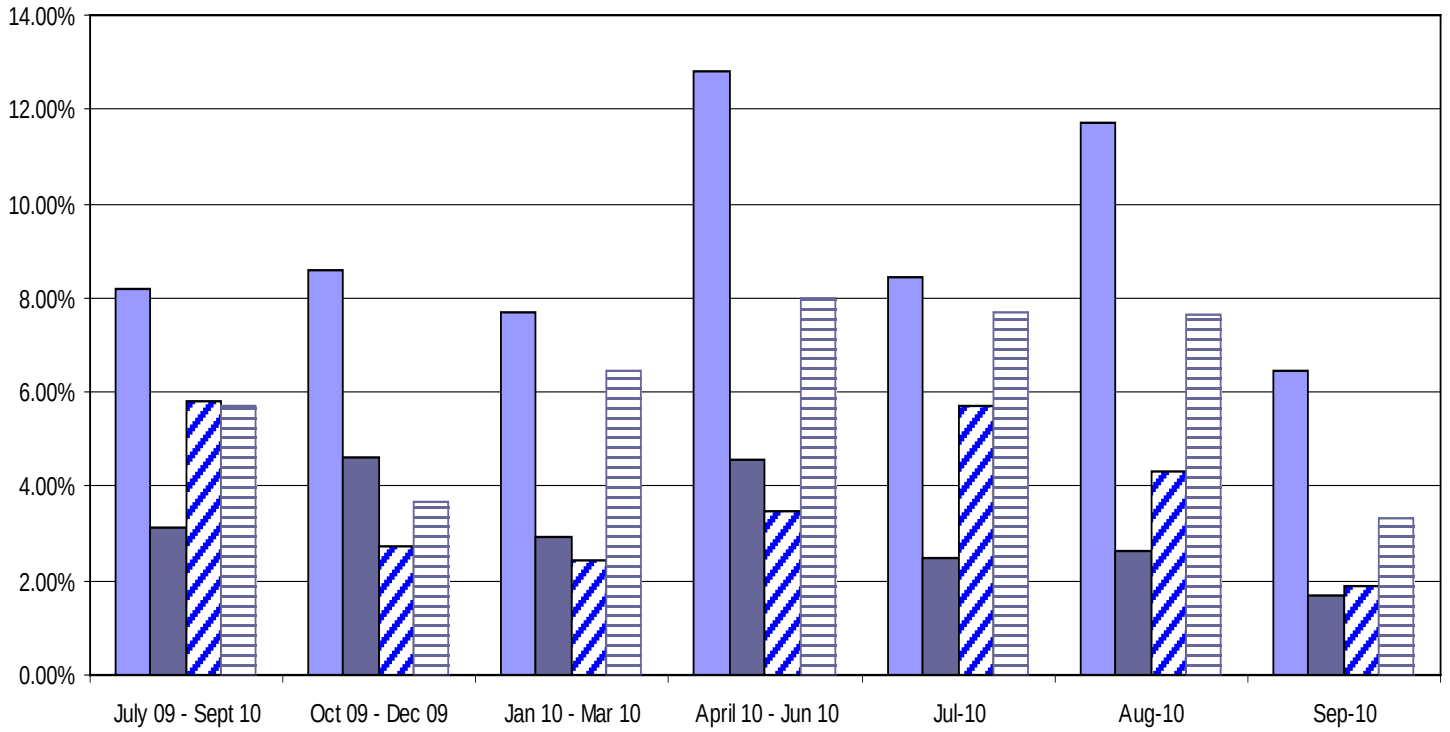


Oct 09 – Sep 2010

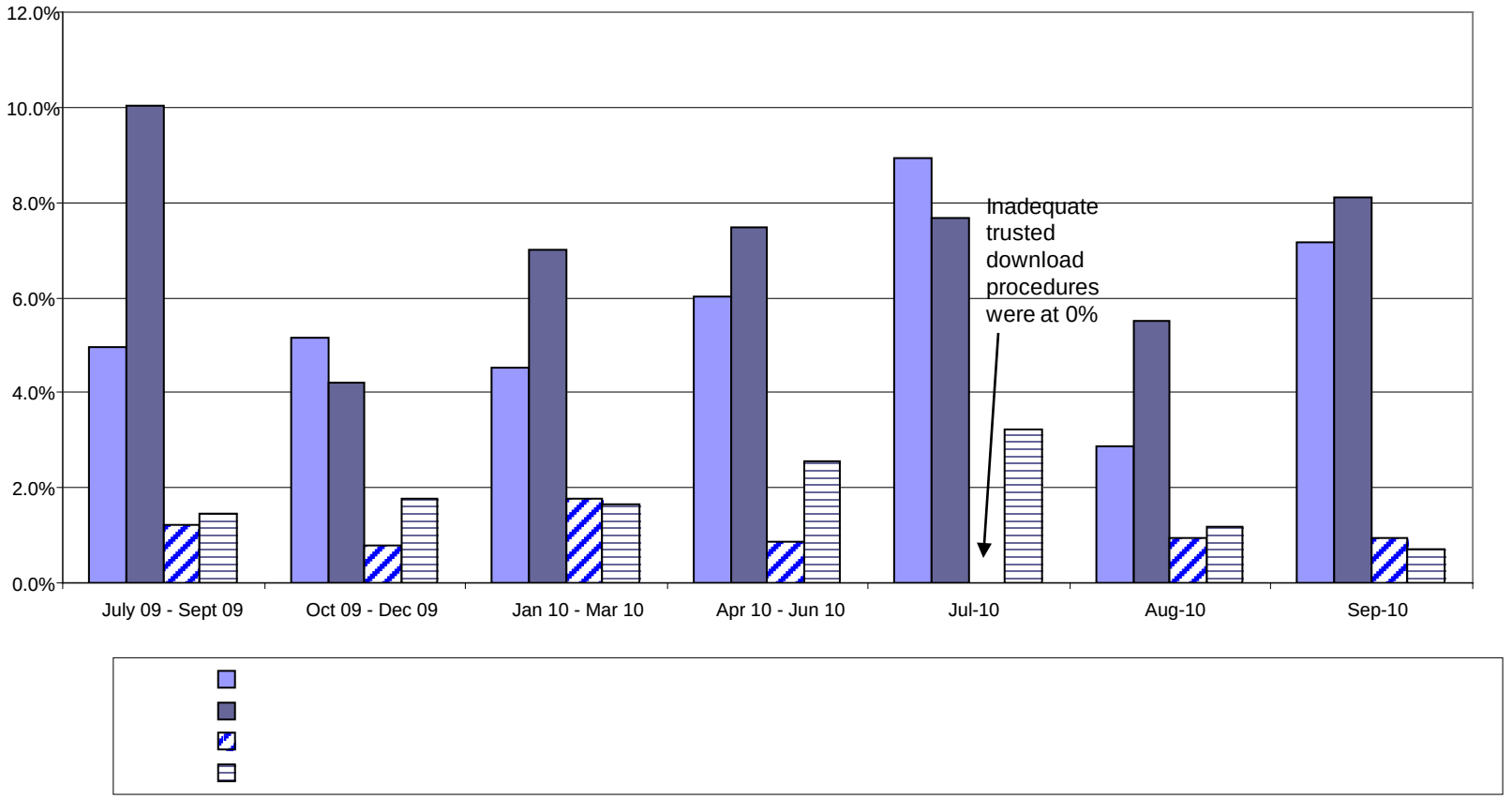
Received 4197 plans:

- On average 33.34% of all plans submitted required changes prior to the On-site Verification for ATO

ODAA Metrics
Security Plan Reviews Common Errors
Part One

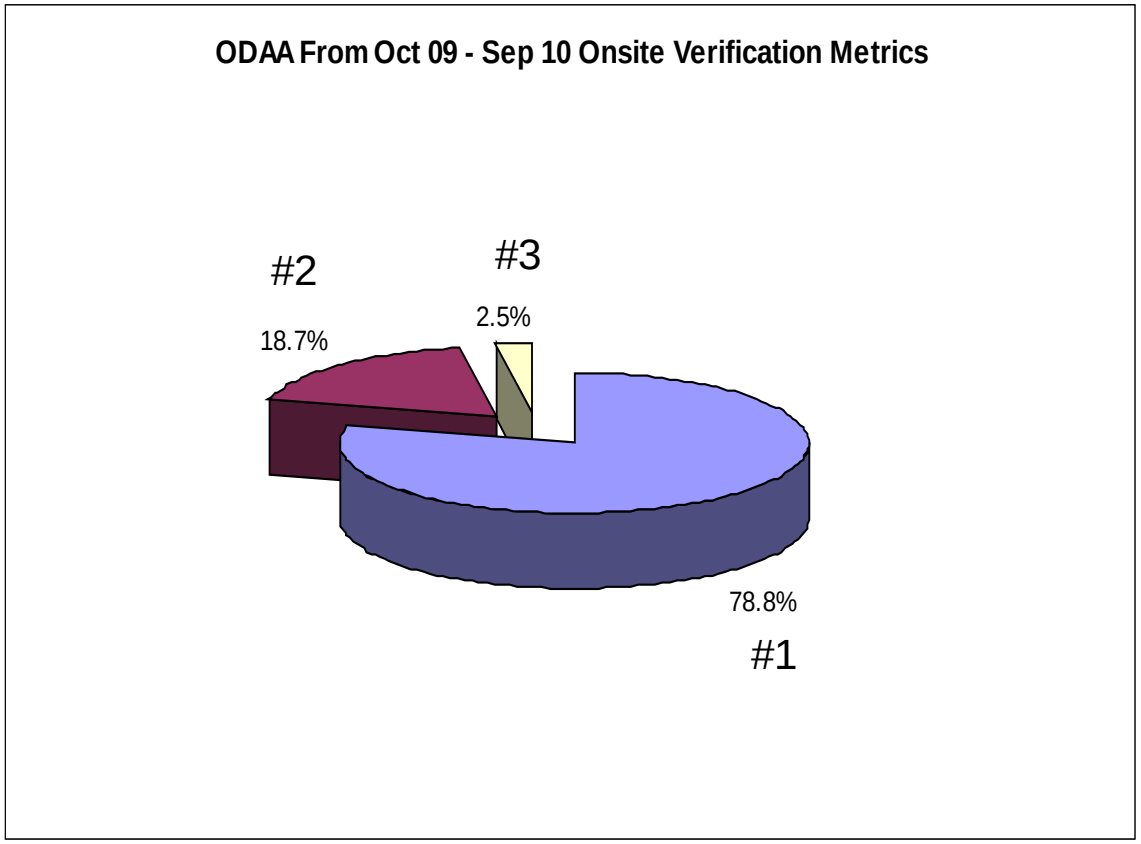


ODAA Metrics
Security Plan Reviews Common Errors
Part Two



ODAA Metrics and Organization

On-site Verification Stats (21.2% Required Some Level Modifications)

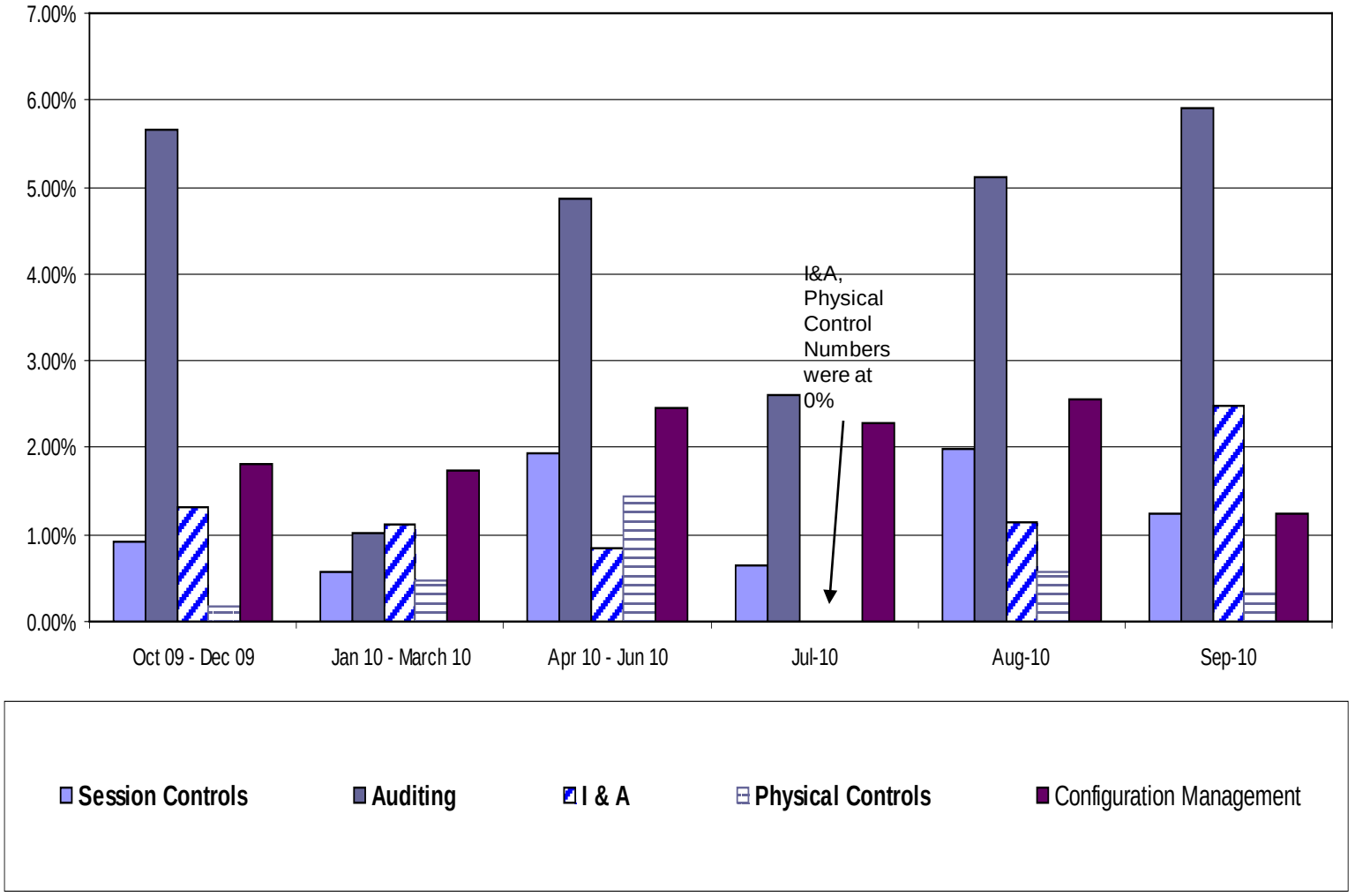


#1. No discrepancies discovered during on-site validation.

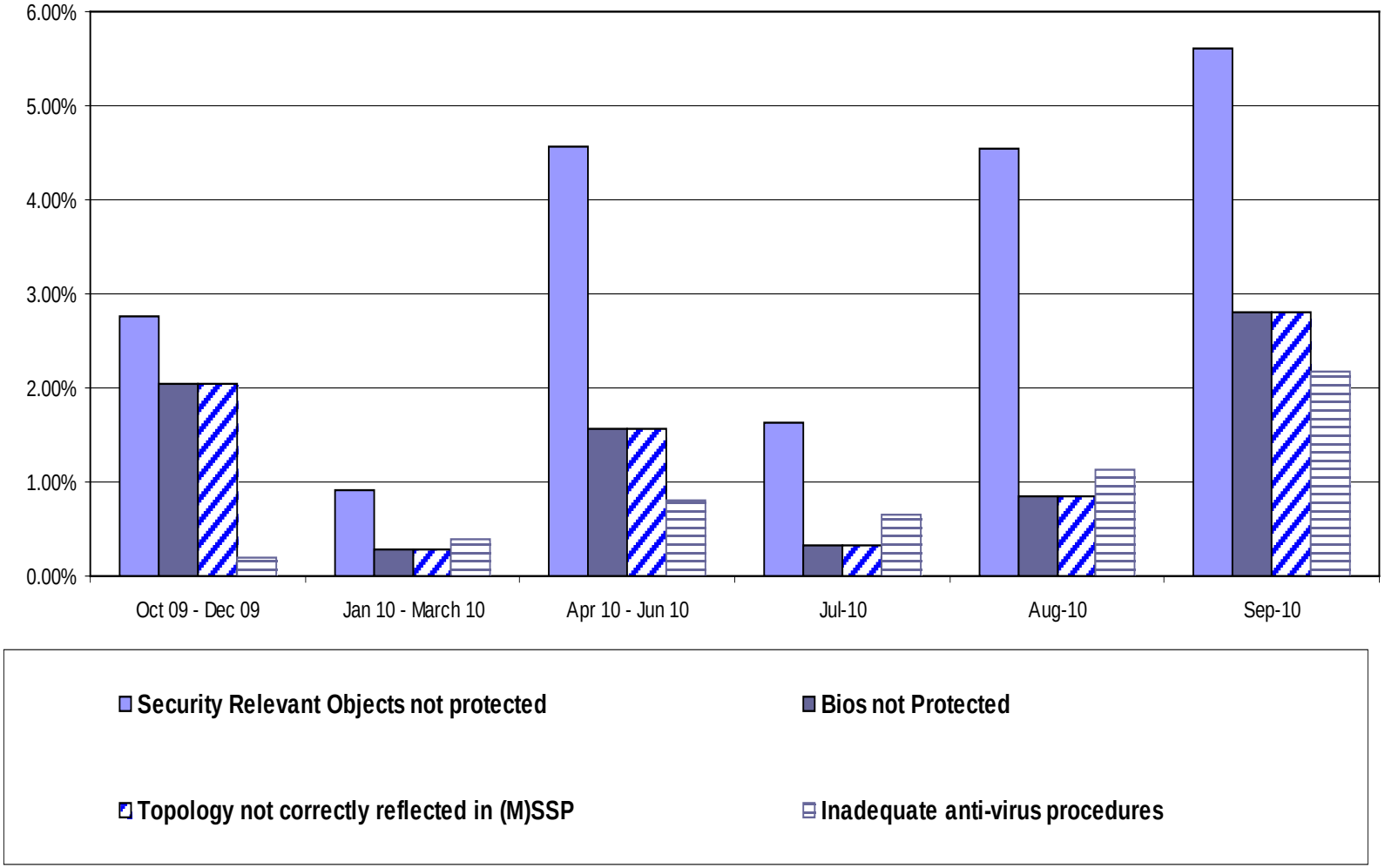
#2. Minor discrepancies noted and resolved during on-site validation.

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

ODAA Metrics
Onsite Plan Reviews Discrepancies
Part One



ODAA Metrics
Onsite Plan Reviews Discrepancies
Part Two



Appendix 4- Security Degree Presentation

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

ODNI SECURITY EDUCATION AND TRAINING PROGRAM

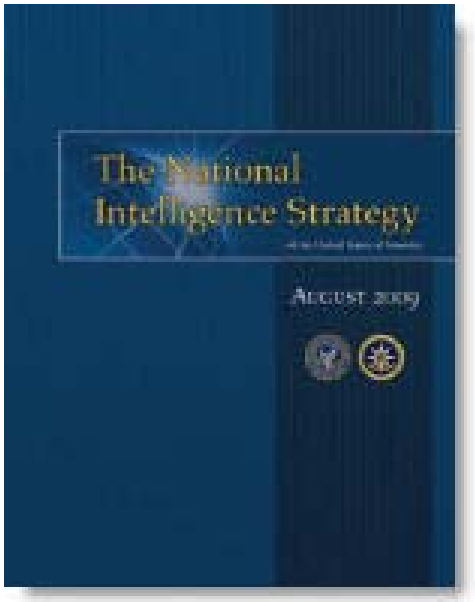
Community Services Division, Special Security Center/ONCIX

LEADING INTELLIGENCE INTEGRATION

NISPPAC
17 November 2010

National Intelligence Strategy
"Develop the Workforce"

- Build a diverse and balanced workforce
- Enhance professional development
- Cultivate relevant expertise
- Support an entrepreneurial ethos
- Deploy integrated, agile teams
- Build a culture of leadership excellence



Education:

Collaborate with academia to develop a Security Operations Baccalaureate Degree

Career Development:

Build professional standards/ certifications; provide framework for career progression

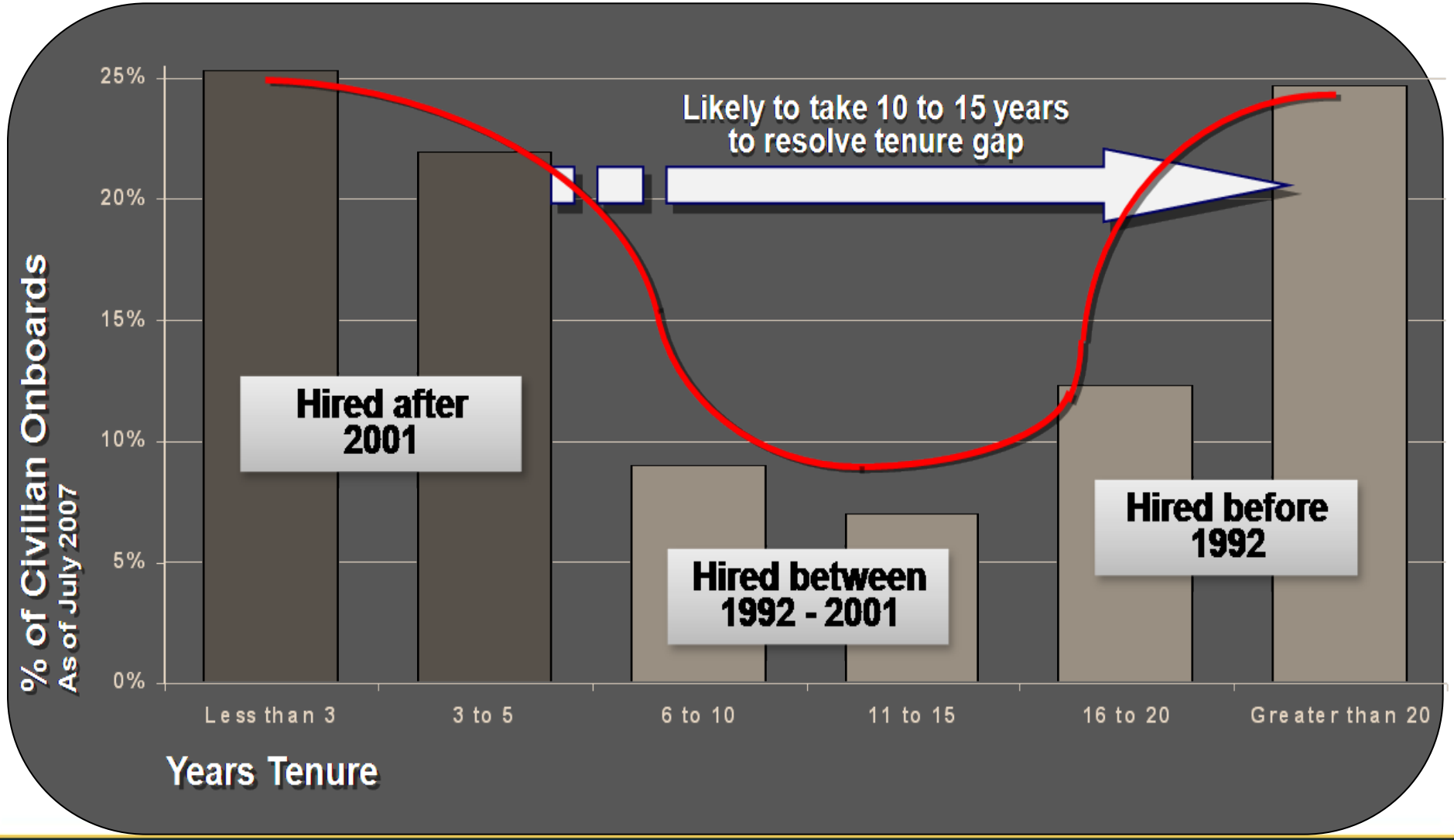
Training:

Provide training that supports the IC mission and promotes career development

Council:

An alliance that integrates the three components; easily adapts to changing requirements

IC Workforce…The Last 30 Years



Security Education

Collaborate with academia to develop a Security Operations Baccalaureate Degree Program allowing the USG and Industry to grow future security professionals

Why this Curriculum?

- No comprehensive bachelor's degree that covers all aspects of security as practiced by the U.S. Government and supporting contractor industry
- Attract college students to the security profession; and enable graduates to become more effective entry-level security professionals
- Security environment and retirements will increase the need for educated and trained security professionals
  - Competition for talent will increase proportionally
  - Between government and industry
  - Between Security Profession and other disciplines

Education Program Development

- Security Operations Curriculum Working Group
  - Government and Industry security professionals
    - What capabilities do I want to see in a future entry-level security professional?
  - Curriculum Requirement Development Teams
    - Personnel Security
    - Physical/Technical Security
    - IA/Cyber Security
    - Program Security
    - Security Organizational Mgmt

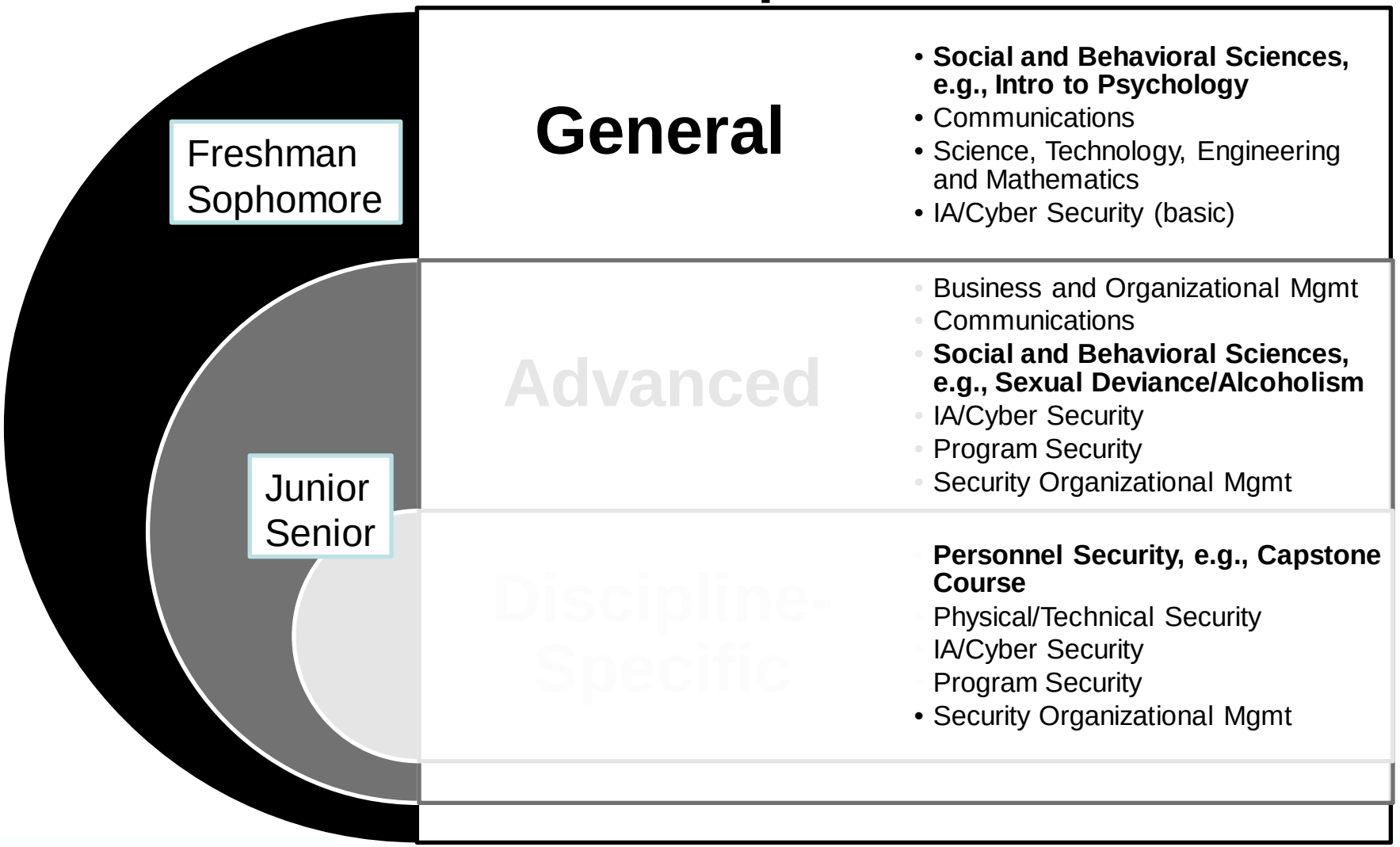
Education Program Development

- Colloquium (Government, Industry, Academia)
  - Presented government and industry job outlook to academia
  - Addressed academic & occupational skills needed in the profession
    - Security Operations Curriculum Working Group
    - Leadership from government and industry
  - Academia explained course/degree development process and highlighted need for **internships, subject matter expertise** and **seed money**
  - Not prescriptive, but maintain Government and Industry requirements

Senior Leadership Requirements

- Critical thinking
- Financial literacy
- Acquisition process
- Technology
- Policy awareness
- Analysis
- Processes
- Leadership
- Economics
- Business management
- Negotiating
- Communications
- Interagency relationships
- Creative solution development
- Innovative thinking
- Change Management
- Ethics
- Decision-making
- Mass media

Academic Capabilities



Education Program Development

FY 2010

- Funded Pilot
- SPAWAR BAA: 26 May – 28 Jul
- Contract Award: 28 Sep, 1-yr duration
- Develop Supporting Infrastructure
- Develop Marketing Package

FY 2011

- Project Mgmt
- Cultivate Supporting Infrastructure
  - Academic liaison
  - SecOps Centers of Academic Excellence
  - Admin Board
  - Selection Process
- Fund Accredited Program

FY 2012

FY 2013

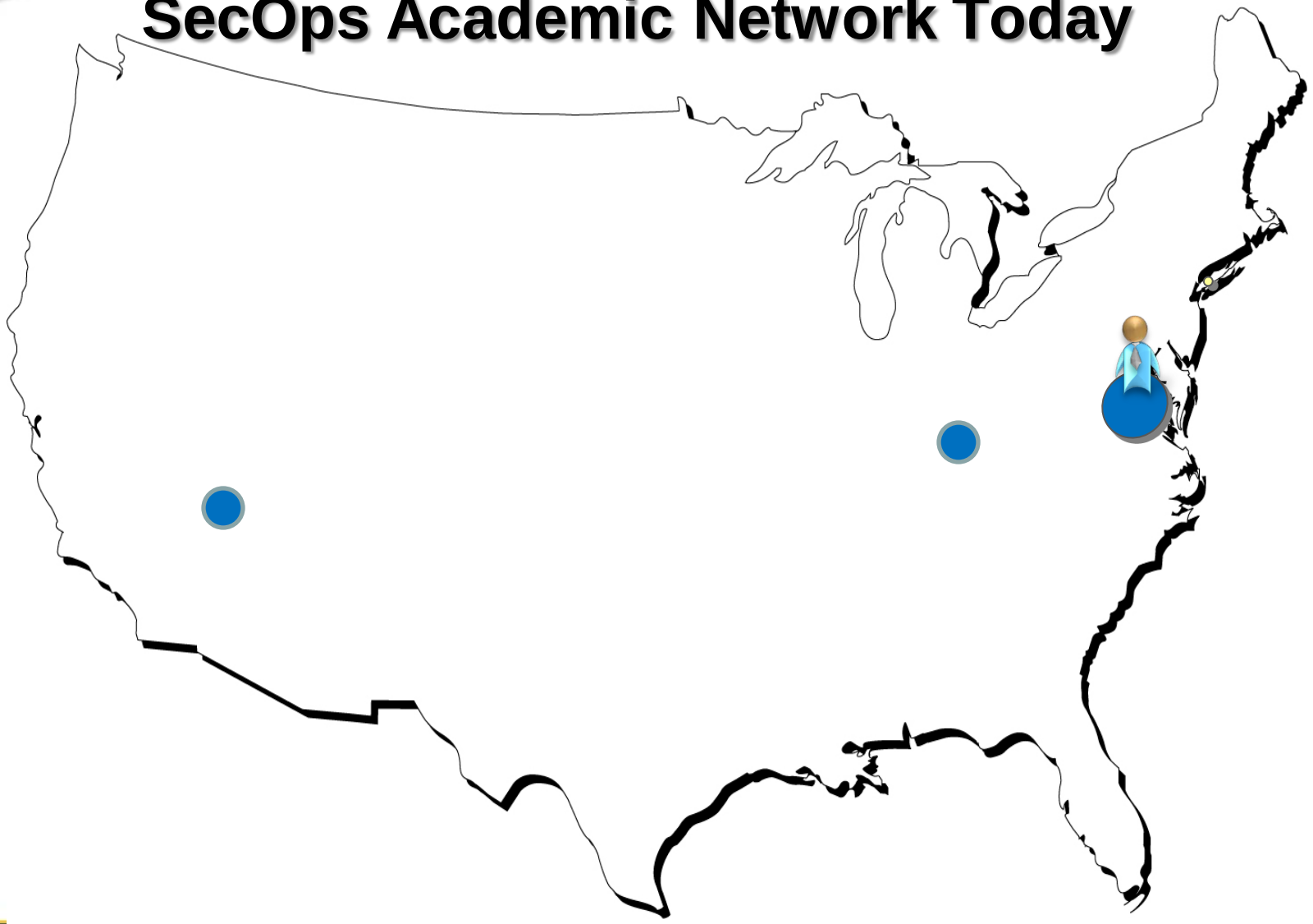
Pilot Universities

- College of Justice and Safety
  - Safety, Security and Emergency Management Department
  - ***SecOps Degree***

In-residence, online and 170 teaching centers worldwide

- Global Security and Intelligence Studies Degree
  - Standard track
  - Chinese track
  - ***SecOps track***

SecOps Academic Network Today

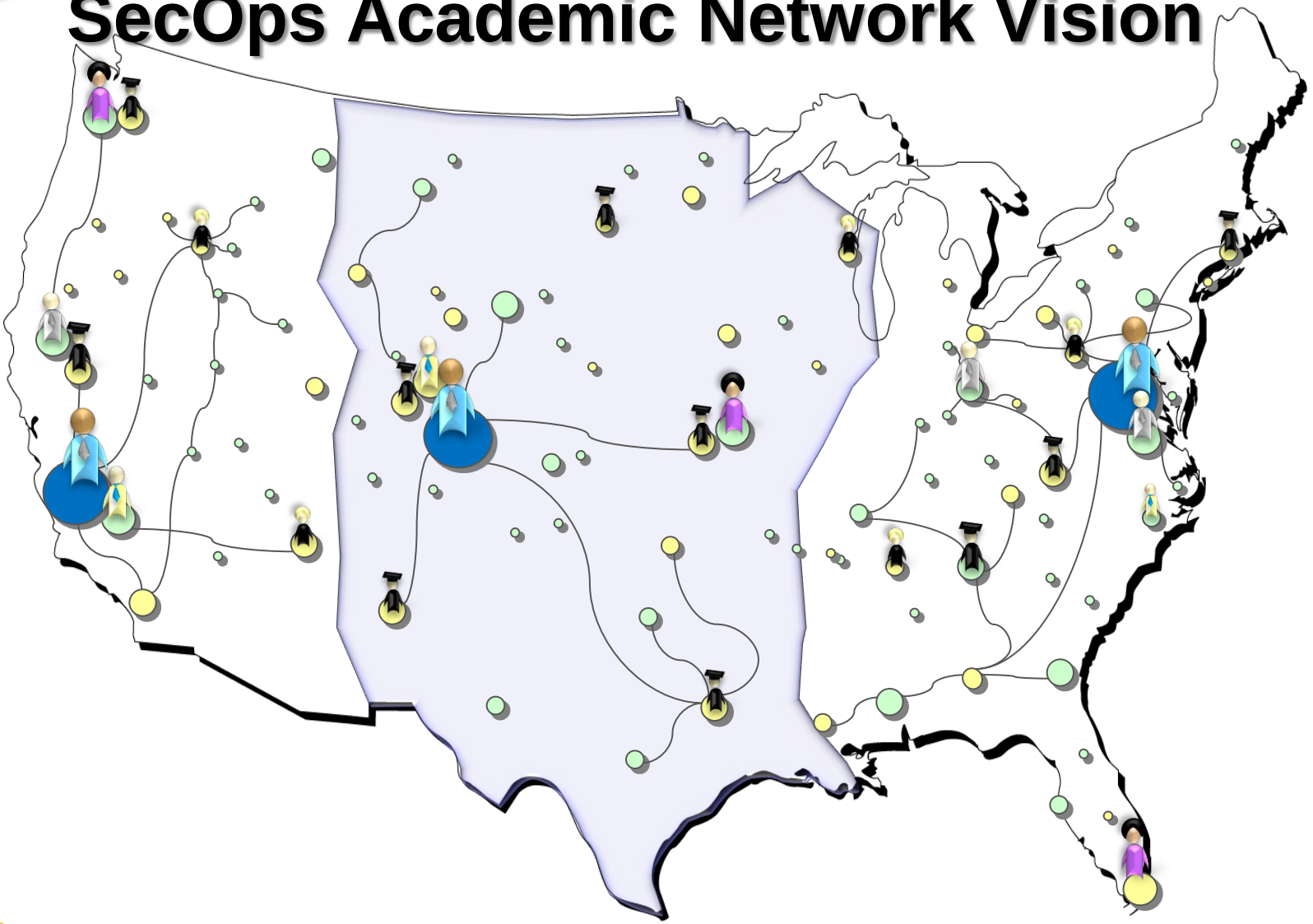


University of Miami

- *U.S. News & World Report*'s 2011 "America's Best Colleges" rankings placed UM No. 47 in the National Universities category
- UM is now ranked as the No. 1 school in the state of Florida

- $1.4 billion from more than 131,000 donors
- Merge Political Science and International Studies
  - Security Operations bachelors and masters degrees in this department
- Exceptional working relationship with US SOUTHCOM, DEA
- Multiple opportunities for federal, state, local, tribal and industry in peninsula

SecOps Academic Network Vision



Summary

Government and industry leaders of the Security Profession will no longer rely on talent to be delivered

– they will be actively involved in growing talent

Appendix 5-DoD Update Presentation

DOD UPDATE

Stan Sims
Director of Security

November 17th, 2010

NISPPAC NISPOM WG Meetings

- September 9, 2010—Kickoff Meeting/Core
- September 14—Chapter 8 (Information Systems Security)
- September 15—Chapter 10 (International)
- September 23—Core Continuation
- September 30—Core Continuation
- October 7--Chapter 8 Continuation
- November 5- Completion of Core/Review of Action Items

Statistics

- **261 comments received and reviewed**
- **57 comments fully or partially accepted**
- **70 comments rejected**
- **137 action items (awaiting input on approximately 40 items)**

Way Ahead

- **Provide resolution of action items to Working Group members for final comment by December 10th**
- **Incorporate accepted comments & resolution of action items into NISPOM draft**
- **Provide NISPOM to NISP CSAs for final comments**
- **Initiate formal coordination/ Federal Register process**

DFARS Clause

- Sets standards for the protection of DoD unclassified information in industry
- Advance Notice of Public Rulemaking completed
- Public Meeting held April 22nd, comments adjudicated
- Public comment period via Federal Register likely by end of CY

Appendix 6- Combined Industry Presentation

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

UPDATE

NOVEMBER 17, 2010

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	Ed Halibozek
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 Team**

Industry Issues

- Information Sharing - Threat
- Controlled Unclassified Information Implementation
- Personnel Security Clearance Processing
  - Clearance Reform & JPAS Transition to PKI requirements
- Certification & Accreditation (C&A) Process Timelines

DoD and Intelligence Community Policy/Regulatory Changes

- **Protecting National Security Information**
  - **National Industrial Security Program Operating Manual (NISPOM) Revision**
  - **New Executive Order: Controlled Unclassified Information (CUI) Program Establishment**
  - **Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Information (DFARs Case 2008-D028)**
  - **Executive Order No. 13526, Classified National Security Information Implementation**

NISPOM

- National Industrial Security Program Operating Manual – revision status
  - Industry Review Teams Working in Partnership with OUSD (I) and Signatory's

- Industry's concern remains with implementation timeframe will be & potential cost impacts

DoD and Intelligence Community Policy/Regulatory Changes: Watch Item

- **Draft Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Information (DFARs Case 2008-D028)**
  - **Establishes cyber security requirements across the Defense Industrial Base**
  - **Impact**
    - **Applies to all defense contractors**
    - **Creates two (2) tier protection scheme**

DoD and Intelligence Community Policy/Regulatory Changes: Watch Item

- **Controlled Unclassified Information (CUI) Protection**
  - **Executive Order Signed**
  - **Single cohesive protection program targeted**
  - **107 unique markings currently**
  - **Potential Impact:**
    - **Rules clarified and strengthened**

Thank You