NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

SUMMARY MINUTES OF THE MEETING

The NISPPAC held its 39th meeting on Monday, June 20, 2011, at 1:00 pm at the Hilton Riverside Hotel, Two Poydras Street, New Orleans, Louisiana. Greg Pannoni, Associate Director, Information Security Oversight Office (ISOO), chaired the meeting, which was open to the public. The following minutes were finalized and certified on September 19, 2011.

The following members/observers were present:

- Greg Pannoni (Chair)
- Daniel McGarvey (Department of the Air Force)
- Timothy Davis (Department of Defense)
- Richard Hohman (Office of the Director of National Intelligence)
- Stan Sims (Defense Security Service)
- Richard Donovan (Department of Energy)
- Charlie Rogers (Department of Homeland Security)
- Scott Conway (Industry)
- Shawn Daley (Industry)
- Sheri Escobar (Industry)
- Marshall Sanders (Industry)
- Michael Witt (Industry)
- William Marosy (Office of Personnel Management) – Observer

After introducing the NISPPAC members present and reviewing the meeting agenda, Greg Pannoni thanked Tony Ingenito, President of the National Classification Management Society, (NCMS) for hosting the meeting. Mr. Pannoni briefly discussed the structure, functions, and goals of the NISPPAC, and stressed that it is a combined government and industry committee that meets at least twice a year, to discuss policy issues. He noted that the committee is subject to the Federal Advisory Committee Act, which means its meetings are open and its minutes are available to the public. The Chair then recognized the two outgoing NISPPAC members, Sheri Escobar and Chris Beals (not present), for their service on the NISPPAC over the last four years. He thanked Ms. Escobar and presented her with an ISOO coin as a token of appreciation. He also mentioned that Rick Graham and Steve Kipp have been nominated as the new NISPPAC industry representatives.

The Chair then reviewed the action items from the March 3, 2011 meeting. The first item was to request the Defense Office of Hearings and Appeals (DOHA) brief the committee on the clearance appeal process and timeliness issues pertinent to the DOHA case workload. He noted that Perry Russell-Hunter, DOHA, would provide that update. The second item was for the Defense Security Service (DSS) to clarify the rejection and denial processes concerning the review and approval of system security plans, and noted that it would be presented as part of the Certification and Accreditation (C&A) Working Group report. The next item was for industry and government to identify methodologies and capabilities that will assist small and medium sized companies to eliminate rejections and other recurring problems in their submission of personnel security clearance (PCL) requests and information system accreditation packages. The Chair noted that one of the reasons for having this meeting at the NCMS Annual Training Conference was to focus on training, especially for the small to medium sized companies, and to provide an opportunity for direct, unfiltered interchange with these companies. The Chair recommended and the membership agreed to the creation of an ad hoc working group that will focus on the issues of the smaller to medium sized companies.

Next, the Department of Defense (DoD) is to provide at the next NISPPAC meeting, (November 16, 2011), an update on the number of non-GSA approved security containers in industry that will require replacement, prior to October 1st, 2012. In addition, ISOO will arrange for a presentation on the governance of the insider threat at the November meeting. The Chair commented that in the post Wiki leaks environment there has been a focused effort on structural reforms, specifically pertaining to the safeguarding and sharing of classified information, and noted that an Executive Order (EO) is being formulated to address a number of these issues to include the creation of an insider threat detection task force. The next item was the industry nomination of two new members, which was noted above. Last, he mentioned that the Office of Personnel Management (OPM) and Defense Industrial Security Clearance Office (DISCO) reports on the trends relating to a decline in the submission of phased periodic reinvestigations would be delayed until the November meeting.

The Chair then introduced, Bill Marosy, OPM, to brief on the PCL Working Group. Mr. Marosy provided an update (Attachment #1) on the performance of the background investigation process for industry. He provided the timeliness metrics for industry's PCL's, to include the submission, investigation, and adjudication timelines. He noted that there has been a reduction in timelines in all categories, with the largest change in periodic reinvestigations (PRs). He emphasized that even with a reduction in timeliness there has not been a significant reduction in the volume of investigations being requested. He provided a snapshot of the initial Top Secret, and all Secret and Confidential clearances, noting that the numbers for adjudications and investigations held steady in the last quarter while there was some fluctuation in the submission timeliness, and the initiation portion of the process. Concerning the requirement to initiate and submit an investigation to OPM within 14 days, he noted that it has fluctuated between 13 and 15 days. He noted that combined numbers for Top Secret, Secret, and Confidential submissions reflects a 92 day average to complete a background investigation, and have it adjudicated. He indicated that in the last quarter the adjudication and investigation timelines for Top Secret clearance decisions remained steady, leading to an average investigation time of 120 days. Regarding reinvestigations for Top Secret access, he noted that in the last quarter the adjudication timeliness dropped by almost half and investigation timeliness fell by approximately 15 to 16 days. He commented that the reduced timelines are a result of electronic-Questionnaires for Investigations Processing (e-QIP) usage as most applicants are now able to update data into e-QIP rather than having to input all the data from the beginning. In response to a question from an attendee regarding the impact of electronic fingerprints on investigation timeliness, Mr. Marosy stated that while DoD has emphasized electronic fingerprint usage, he did not have specific data regarding its impact. Stan Sims, DSS, advised that only about 9% of submitters are using electronic fingerprints so the impact is very insignificant.

The Chair then recognized Helmut Hawkins, DSS, who reported on the adjudication inventory for industry cases (Attachment #2). He noted that, for this fiscal year, there has been a 42% reduction in the timelines for adjudication of initial PCLs, and that the focus has been on reducing the pending inventory of initial cases. His report indicated a 35% decrease in Top Secret PCL PRs in fiscal year 2011 to date, and a steady state for the inventory of industry cases at OPM.

He noted that 10.2% of cases are rejected at DISCO and 5.5% at OPM, and that some of these will be eliminated with the introduction of the new Standard Form (SF) - 86 which contains more edits that will preclude rejections. Mr. Hawkins commented that rejections by facility category reveal that 82%

of the rejections at DISCO pertain to smaller facilities, and that the larger facilities have significant automation in place to preclude most rejections. He noted that online tutorials, available through the DSS website, can assist smaller companies with reducing their rejection rate. He also noted that a rejection by DISCO can add about 15 to 30 days to a case, while a rejection by OPM can add as much as six months. Mr. Pannoni opined that this is very important since the clock is reset when a case is rejected which directly impacts timeliness, but does not otherwise reflect in the PCL process timeline data. He also commented that it was entirely unacceptable to have a combined 15 % plus rejection rate. Mr. Sims also noted that a rejected case results in the double handling of the case which detracts from time that could be devoted to other work. Mr. Hawkins explained that over 50% of the rejections are due to missing employment information and inaccurate or missing information regarding finances. He noted that the top 10 reasons for rejections account for 91% of the rejections, and he urged submitters to closely examine what they submit to avoid rejections. Ms. Escobar commented that the information pertinent to case rejections is important to Facility Security Officers, because they can help prevent it. Mr. Hawkins added that of the 5.5% that OPM rejects, 68% are due to missing or illegible fingerprints and missing information on release forms comprise another 16%.

Mr. Sims commented, that while everyone should be excited about the decrease in adjudication timelines and case inventory, these reductions are about to end because, with the relocation of DISCO to Fort Meade, DISCO will lose about 85% of their experienced personnel. He projected that by the end of the year, new hires will have been sufficiently trained to return them to their current numbers. Mr. Pannoni asked if the planned collocation of the Clearance Adjudication Facilities (CAF) will provide any capability to leverage more support for DISCO. Mr. Sims responded that while leveraging support is possible, the other CAFs are also relocating and will have the same problems, issues, and limitations as DISCO.

Mr. Pannoni then introduced Randy Riley, DSS, who provided the report from the C&A Working Group (Attachment #3). Mr. Riley noted that most of the data is captured manually as system security plans go through the review and accreditation process. He explained that the Interim Approval to Operate (IATO) process, which is the initial approval for a system to operate, is divided into three parts. He explained that while there's one big clock representing the overall time it takes to get a system accredited, there are two smaller clocks, one indicating industry timelines, and the other DSS timelines, and this overall time is what is tracked, and reported in this metric.

Mr. Riley indicated that DSS processed 4,805 IATOs, between May 2010 and April 2011, to include plans that had to be resubmitted for corrections. He noted that the average turnaround time for that 12 month period was about 25 days, and that for April 2011, it was 21 days. He explained that industry time is how long it takes a company to respond, once DSS requests corrections and commended industry for keeping that average at about three days. Mr. Riley then provided that between May 2010 and April 2011, there were 5,229 plans submitted, and 4,080 had errors. He explained that when the reviewer identifies errors in the plan they send a list of the required corrections back to the Information Systems Security Manager (ISSM). He noted that some plans get an IATO even when minor corrections are required, and affirmed that DSS expects those corrections to be completed by the time of the onsite review. However, he advised that if certain attachments are omitted, the IATO cannot be processed, emphasizing the importance of the ISSM ensuring that all required attachments are included. He stated that from November 2010 to February 2011, about 26 % of plans submitted by the largest facilities were missing or had incomplete attachments.

Mr. Riley explained that of the 1,529 plans that were denied between May 2010 and April 2011, 424 got through an initial screening process, but were later denied because they did not include required critical information. He noted that receiving a denial doesn't mean the submitter has to re-start the process and that once the ISSM provides DSS with the corrections, an IATO is normally granted. He noted the average turnaround time for these corrections is less than five days. Continuing, Mr. Riley discussed the common errors that are seen during the plan reviews, and noted that the "other" category block will soon be eliminated, and the reviewer will now have to identify specific errors either in the comments section or select from a pre-configured list. He opined that having more details regarding the errors will be more meaningful for the Committee, especially when considering training for ISSMs. Mr. Pannoni added that it is important to collect this data so problem areas can be identified and resolved with targeted and focused educational efforts. Mr. Riley noted that system integrity and availability will now default to "not required", so ISSMs will not have to check that box unless it is contractually required. He noted that about 36% of the plans submitted required corrections at the time of the on-site validation.

Mr. Riley cited the metrics for the Approvals to Operate (ATO), noting that 3,115 or 73%, of the 4,000 plus systems reviewed had no problems and received an ATO after the on-site review. While another 1,052 systems, or about 24% had errors that were corrected on-site, and 1.7% (74 systems) were so different or misconfigured that their IATOs were revoked. Noting the 82 day average turnaround time, for getting a system from IATO to ATO, he stated the goal is to reduce that to less than 40 days. He presented the ATO statistics by facility category, noting that there were 367 errors cited during on-site reviews that had already been certified by an ISSM as being correctly configured.

Mr. Riley then discussed the differences between rejections and denials, emphasizing that a denial occurs after a plan was received and reviewed, but an IATO could not be issued until corrections were made. In response to a few questions from the Chair, he verified that these denials are normally handled in the average two to four day timeframe for industry corrections and that the majority of these plans receive an IATO. Regarding the implications of failure to correct the errors in a timely manner, Mr. Riley stated that they normally rescind the IATO if the required corrections aren't submitted within 180 days. He explained that rejections occur when a plan is received that does not have the basic required information. Concerning the issuance of a second IATO, he explained that when they are issued it is because the system either has open issues that need addressing or the onsite review is postponed because of scheduling conflicts.

The Chair introduced Charlie Rogers, Department of Homeland Security (DHS), who spoke about how EO 13549, "*Classified National Security information Program for State, Local, Tribal, and Private Sector Entities,"* (SLTPS) relates to the National Industrial Security Program (NISP) (Attachment #4). Mr. Rogers explained the SLTPS program relationship to the NISP and clarified how the private sector entities under this program are separate from the NISP. He stated that the SLTPS program was established so the executive branch could enhance consistency in sharing and safeguarding classified information with SLTPS partners. He noted that the federal government has been providing classified information to those communities on an individual basis, through DHS, DoD, and the Federal Bureau of Investigation under their own internal rules and regulations. He noted the program established a single level of access for SLTPS entities, encourages the reciprocity of clearances, and a unified standard that provides integration for classified communications, networks, and facilities supporting the SLTPS entities.

Mr. Rogers noted that EO 13549 provides for policy oversight from the national security staff, ISOO and the Office of Management and Budget, and DHS is the executive agent responsible for administering the program and issuing an implementing directive. The EO also established a SLTPS Policy Advisory Committee, with federal, state, local, tribal and private sector representation. Additionally, the EO reaffirms DoD's governance over the NISP and requires that classified information safeguarded at a private sector facility is subject to the NISP. He noted that if an SLTPS entity contracts for services that require access to classified information they have to follow NISP guidelines. Mr. Rogers concluded his remarks by noting that the intent of this program is to safeguard classified information, and to facilitate information sharing, because the federal government will be more likely to share classified information within the SLTPS community when they know that there's an oversight, training, and compliance review process in place.

The Chair introduced Mr. Russell-Hunter who provided an update on the DOHA adjudication process. Mr. Russell-Hunter stated that in calendar year 2010 DOHA received about 10,000 cases, which represented less than 10% of the overall industrial clearance workload. He reminded the members that DOHA sits at the very end of the clearance process, and noted that DISCO's success at reducing the number of cases that were more than 90 days old was accomplished by sending those cases to DOHA. He noted that there were less than 2,000 denials and revocations in calendar year 2010, with 1,800 of those from DOHA. He commented that over the last quarter century, the number of clearance denials and revocations out of the total population has stayed somewhere between 1-2%. He commented that the cases DISCO refers to DOHA usually concern financial issues and DOHA must determine if the conditions that resulted in the financial problem were largely beyond the applicant's control and that they acted responsibly under the circumstances. Mr. Sims commented that when DISCO refers a case to DOHA, it's because of that second part of not acting responsibly and noted that when the applicant refuses to reveal information, or take action, the case is referred to DOHA.

Mr. Russell-Hunter noted that at last year's NCMS Conference, a best practice concerning foreign passports was identified when it was noted that there had been some success in getting an interim clearance issued if the applicant surrendered, destroyed, or otherwise invalidated their foreign passport at the beginning of the clearance process. Mr. Russell-Hunter noted that if we collect the mitigating information upfront, not only is the case going to move forward faster, but it will also give the investigators and adjudicators what they need to resolve a case. He noted that interrogatories issued by DOHA, that were based either on questions on the SF 86 or by an investigation, helped form the branching questions in the new SF 86, thus supporting the concept of gathering more mitigating information upfront. He closed by stating that while the DISCO model was designed to get clearances out faster, the DOHA process is to get it right, which means they have to resolve issues that may require them to collect information on their own, which may take longer.

The Chair introduced Steve Lewis, Office of the Undersecretary of Defense for Intelligence, who provided an update on the status of the NISPOM. Mr. Lewis stated that DoD, as the executive agent for the NISP, is responsible for publishing the NISPOM, coordinating with the DoD components, and obtaining the concurrence from the Office of the Director of National Intelligence, (ODNI) , the Department of Energy, and the Nuclear Regulatory Commission prior to making any changes. He noted that they are required by EO 12829, "National Industrial Security Program," to work through

the NISPPAC to solicit and incorporate changes from both government and industry representatives. He explained that they have been working closely with the NISPPAC NISPOM Working Group members and have sent out an informal version for a 30 day review and comment period. He noted that they will incorporate any relevant comments, and then place the draft NISPOM into a formal coordination process. Mr. Lewis noted that a key premise in updating this document was to bring industry standards to a level equivalent with those levied on the government. He highlighted the key changes in the NISPOM, noting that Chapter One was updated to recognize the expanded role of the ODNI and the continued role of Central Intelligence Agency as the Cognizant Security Agency (CSA) for the Intelligence Community. He noted that Chapter Four has been updated to implement the EO 13526 requirement for the training of derivative classifiers and that Chapter Five applies the open storage concepts available to government as another option for classified storage by industry. He emphasized that Chapter Eight has been rewritten to require that the CSAs issue implementing instructions for compliance with national standards, such as the Committee on National Security Systems, and the National Institute of Standards and Technology Standards for the protection of Information Systems. He noted that the DSS Industrial Security Field Operations (ISFO) Process Manual will become the vehicle for addressing the specific requirements resulting from changes in technology and insider threat, and acknowledged an obligation to consult with industry on any changes to the manual. Mr. Sims agreed that DSS will coordinate changes to the ISFO Process Manual with industry, and stated that it was his goal to provide a more dynamic coordination process. Mr. Lewis continued, explaining that Chapter 10 is still in coordination because the Office of the Undersecretary of Defense for Policy has a few items to address. He added that the current NISPOM supplement will be replaced by the DoD Special Access Program (SAP) Manual. The Chair mentioned that there would be more about the upcoming NISPOM changes at the NISPPAC panel presentation during the NCMS Conference.

The Chair introduced Bryan Oklin, ISOO, who provided an update on Controlled Unclassified Information (CUI) (Attachment #5). Mr. Oklin noted that EO 13556, "*Controlled Unclassified Information,"* was signed on November 4th, 2010, and designated the National Archives and Records Administration as the executive agent to oversee agency implementation. He explained that the EO establishes a standardized system for managing information that requires safeguarding or dissemination controls pursuant to a law, a federal regulation, or a government-wide policy, but which is not classified under EO 13526 or the Atomic Energy Act. He advised that the CUI Office will consult with agencies to deconflict and standardize these categories. He noted that on June 9, 2011 the CUI Office published CUI Notice 2011-01 which provided initial guidance for agencies and emphasized that the CUI Registry, which will be issued by November 2011, will serve as the main reference tool for the approved CUI categories. He validated that agency plans for compliance with the EO are due by December 6, 2011, and that OMB will then establish target deadlines for phased implementation. He emphasized that there's no specific timeframe for implementation and that the system depends on the plans submitted by the departments and agencies. In response to a question regarding the CUI categories and their markings, Mr. Oklin explained that the goal of the system is to have the categories based on types of information such as: nuclear, medical, privacy, or infrastructure information, and within the categories there could be subcategories. The Chair noted that a key point is that the phased initial implementation is not projected until sometime in 2012, and stated that the intention is to homogenize the compliance process across the various agencies that use similar markings within the registry, especially since many NISP contractors have multiple contracts with multiple agencies.

The Chair introduced Scott Conway, Industry Spokesperson, who provided the industry update (Attachment #6). Mr. Conway reviewed industry's representation for both the NISPPAC and the Memorandum of Understanding (MOU) committees and recognized those members present. He explained how the MOU's operate and the coordination process for both vetting issues and the process for nominating new NISPPAC members. He emphasized that NISPPAC members represent all 13,000 NISP contractors and not their individual companies. He mentioned that there are currently two working groups, the PCL Working Group, was formed about six years ago to examine the clearance process, and was the beginning of a true partnership between the government and industry in working through problems and issues. He complemented DSS for providing information about the potential impact of the Base Realignment and Closure on DISCO operations. He noted that the C & A Working Group reviewed and recommended changes to the ISFO Process Manual, coordinating over 90 comments through an open discussion and dialogue. Mr. Conway expounded on other issues that are being worked through the NISPPAC processes such as: the DoD SAP Manual, the sharing of threat information, CUI, a proposed Defense Federal Acquisition Regulation clause, and insider threat issues. In response to a question regarding the Defense Manpower Data Center deadline of January 2012 for all contractors to be compliant with Common Access Card standards, Mr. Sims noted that a date had to be established in order to have a goal to work toward, but emphasized if that date comes and everything's not in place, no one will be locked out of the system.

The Chair reemphasized that the NISPPAC industry members represent all of industry and noted that their contact information will be provided during the NISP Panel discussion, and that it is also on the ISOO website. The Chair recommended that a NISPPAC working group be formed to address how appropriate threat data may be expeditiously disseminated to industry. Mr. Sims commented that DSS disseminates threat data to those who need it, and noted that when its counterparts have threat information, regarding specific companies, they find ways in which to get that information to those who need it.

The Chair thanked NCMS for hosting the meeting and all of the speakers, members, and meeting participants. The meeting was adjourned at 3:20 pm.

Summary of Action Items

(1) NISPPAC will form an ad-hoc working group to focus on the issues of smaller to medium sized companies.

(2) 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.

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

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

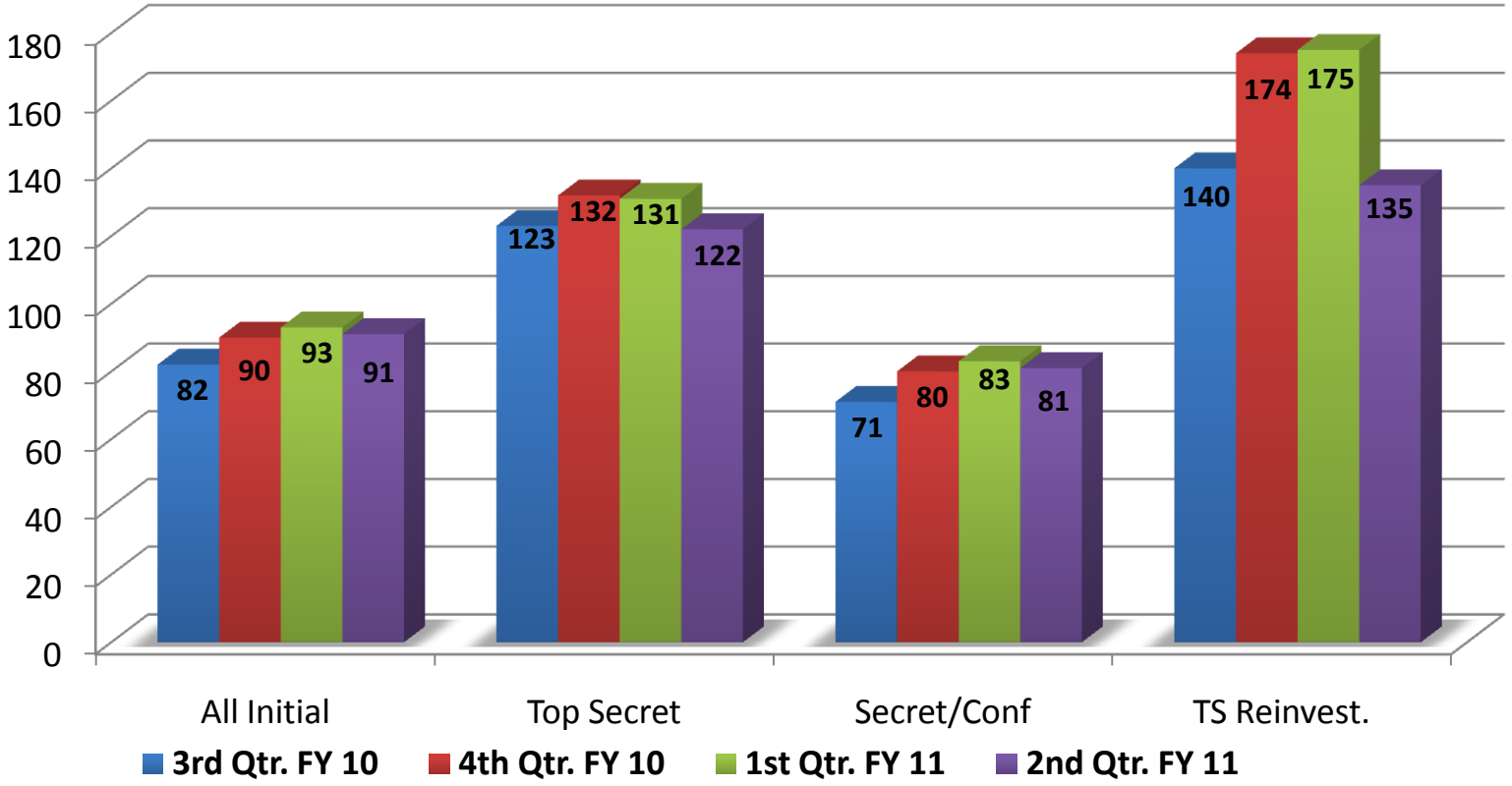
(5) NISPPAC will form an ad-hoc working group to address how appropriate threat data may be expeditiously disseminated to NISP facilities.

Attachment #1- OPM PCL Presentation
Attachment #2- DISCO PCL Presentation
Attachment #3- DAA C&A Presentation
Attachment #4- SLTPS Presentation
Attachment # 5-CUI Presentation
Attachment # 6- Combined Industry Presentation

Attachment #1- OPM PCL Presentation

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

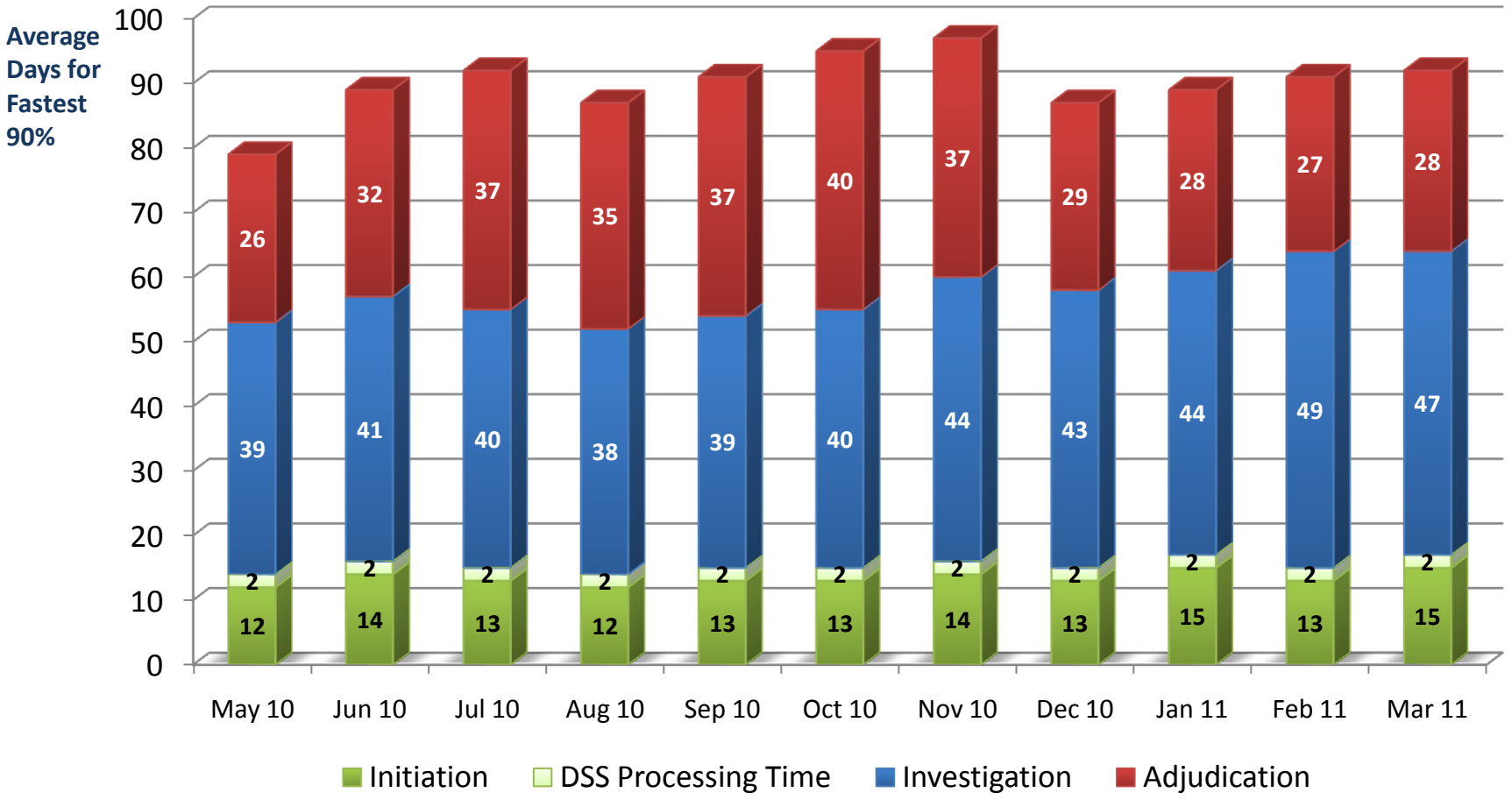
Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 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
Adjudication actions taken – 2nd Q FY11	28,912	6,763	22,149	8,143

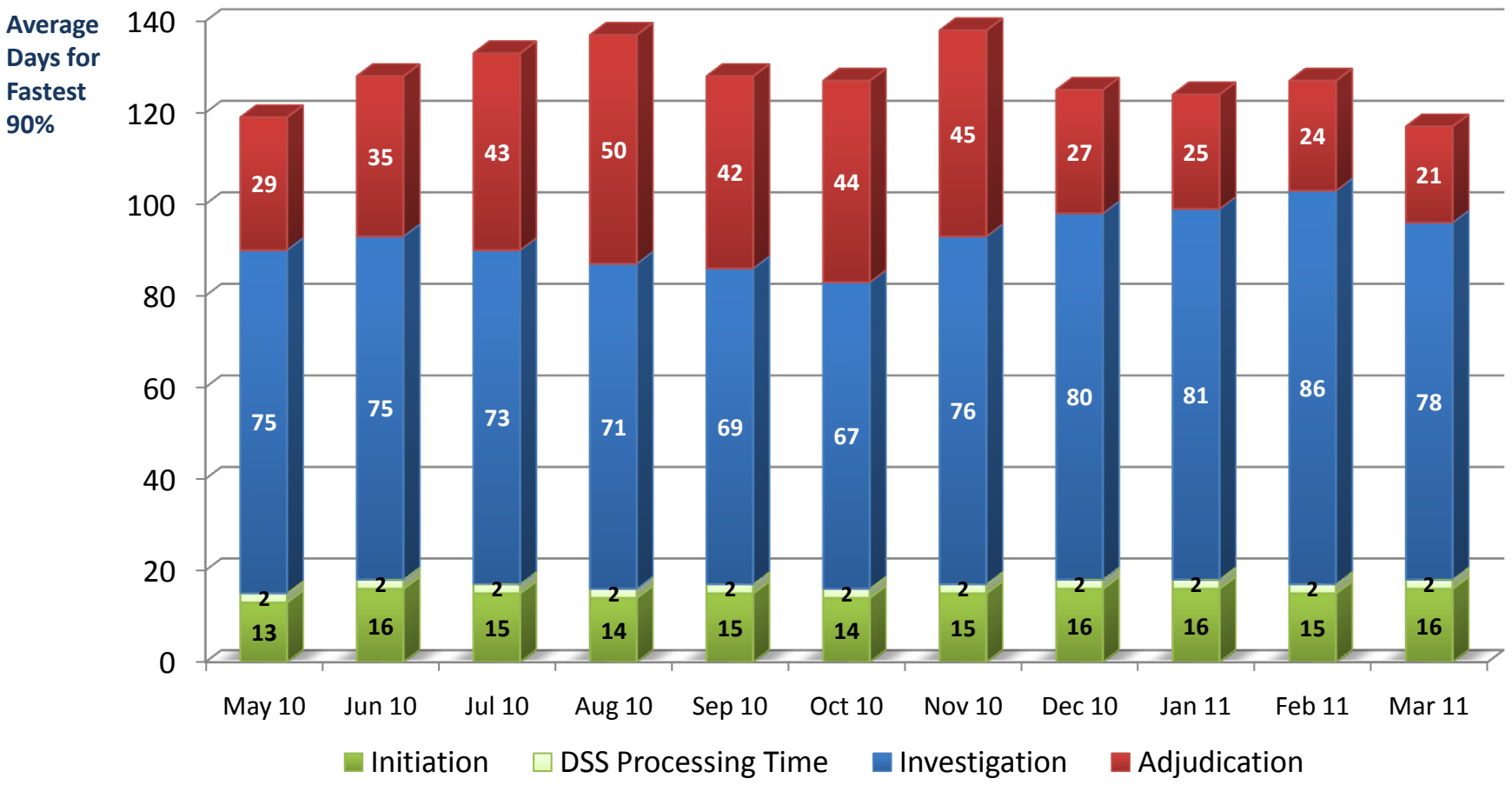
*The adjudication timelines include collateral adjudication by DISCO and SCI adjudication by other DoD adjudication facilities

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



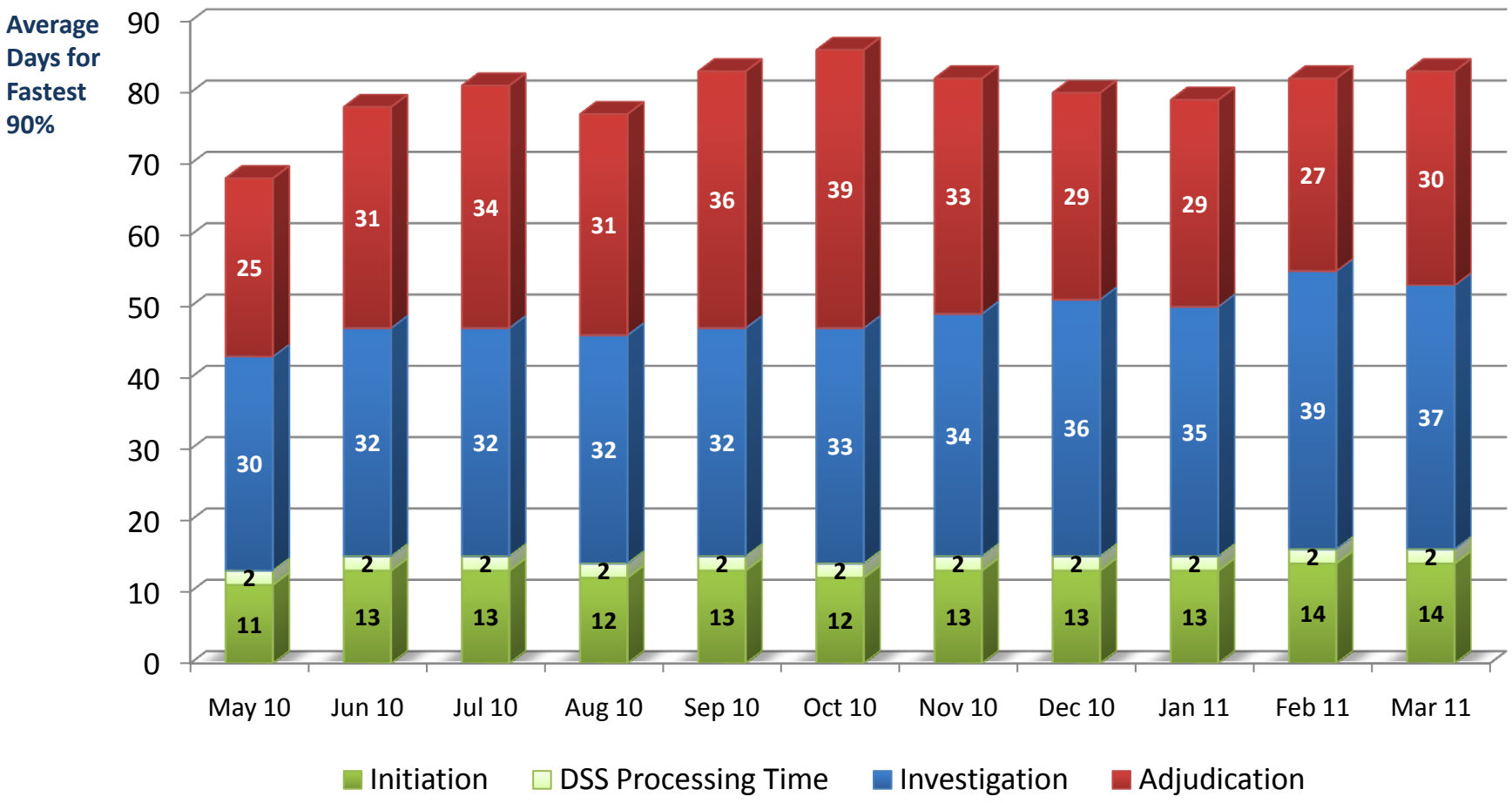
	May 10	Jun 10	Jul 10	Aug 10	Sep 10	Oct 10	Nov 10	Dec 10	Jan 11	Feb 11	Mar 11
100% of Reported Adjudications	7,903	8,531	6,037	10,235	9,233	9,994	9,729	9,662	9,087	8,100	11,678
Average Days for fastest 90%	79 days	89 days	92 days	87 days	91 days	95 days	97 days	87 days	89 days	91 days	92 days

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



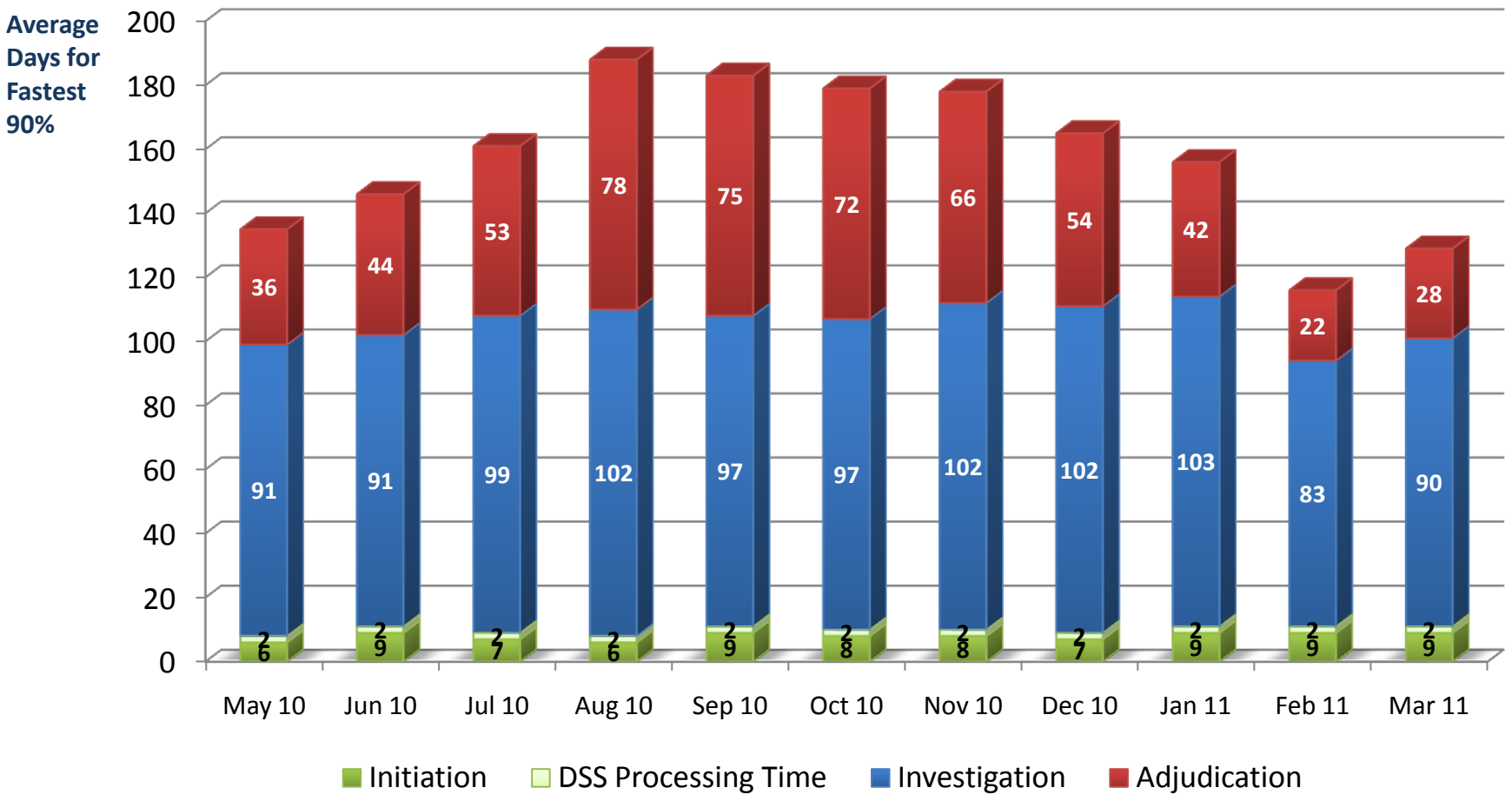
	May 10	Jun 10	Jul 10	Aug 10	Sep 10	Oct 10	Nov 10	Dec 10	Jan 11	Feb 11	Mar 11
100% of Reported Adjudications	1,825	1,935	1,330	1,975	1,964	2,282	2,669	1,781	2,035	1,776	2,943
Average Days for fastest 90%	119 days	128 days	133 days	137 days	128 days	127 days	138 days	125 days	124 days	127 days	117 days

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



	May 10	Jun 10	Jul 10	Aug 10	Sep 10	Oct 10	Nov 10	Dec 10	Jan 11	Feb 11	Mar 11
100% of Reported Adjudications	6,078	6,596	4,707	8,260	7,269	7,712	7,060	7,881	7,052	6,324	8,735
Average Days for fastest 90%	68 days	78 days	81 days	77 days	83 days	86 days	82 days	80 days	79 days	82 days	83 days

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



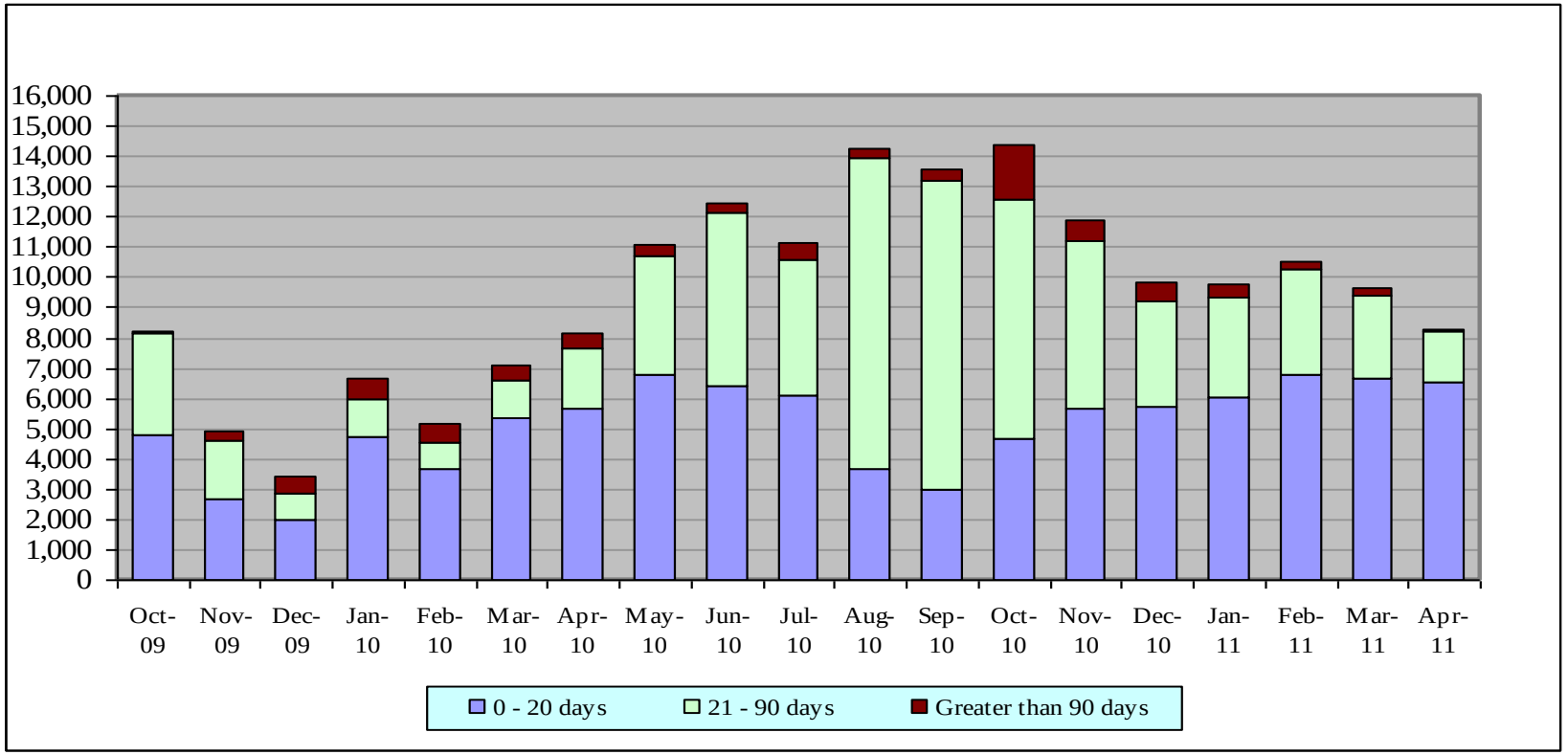
	May 10	Jun 10	Jul 10	Aug 10	Sept 10	Oct 10	Nov 10	Dec 10	Jan 11	Feb 11	Mar 11
Reported Adjudications	1,513	1,917	1,423	1,170	1,497	2,197	2,008	2,522	2,869	3,133	1,902
Average Days for fastest 90%	135 days	146 days	161 days	188 days	183 days	179 days	178 days	165 days	156 days	116 days	129 days

Attachment #2- DISCO PCL Presentation

Defense Industrial Security Clearance Office

FY11 Adjudication Inventory

SSBI/NACLC Initial Clearance Adjudications



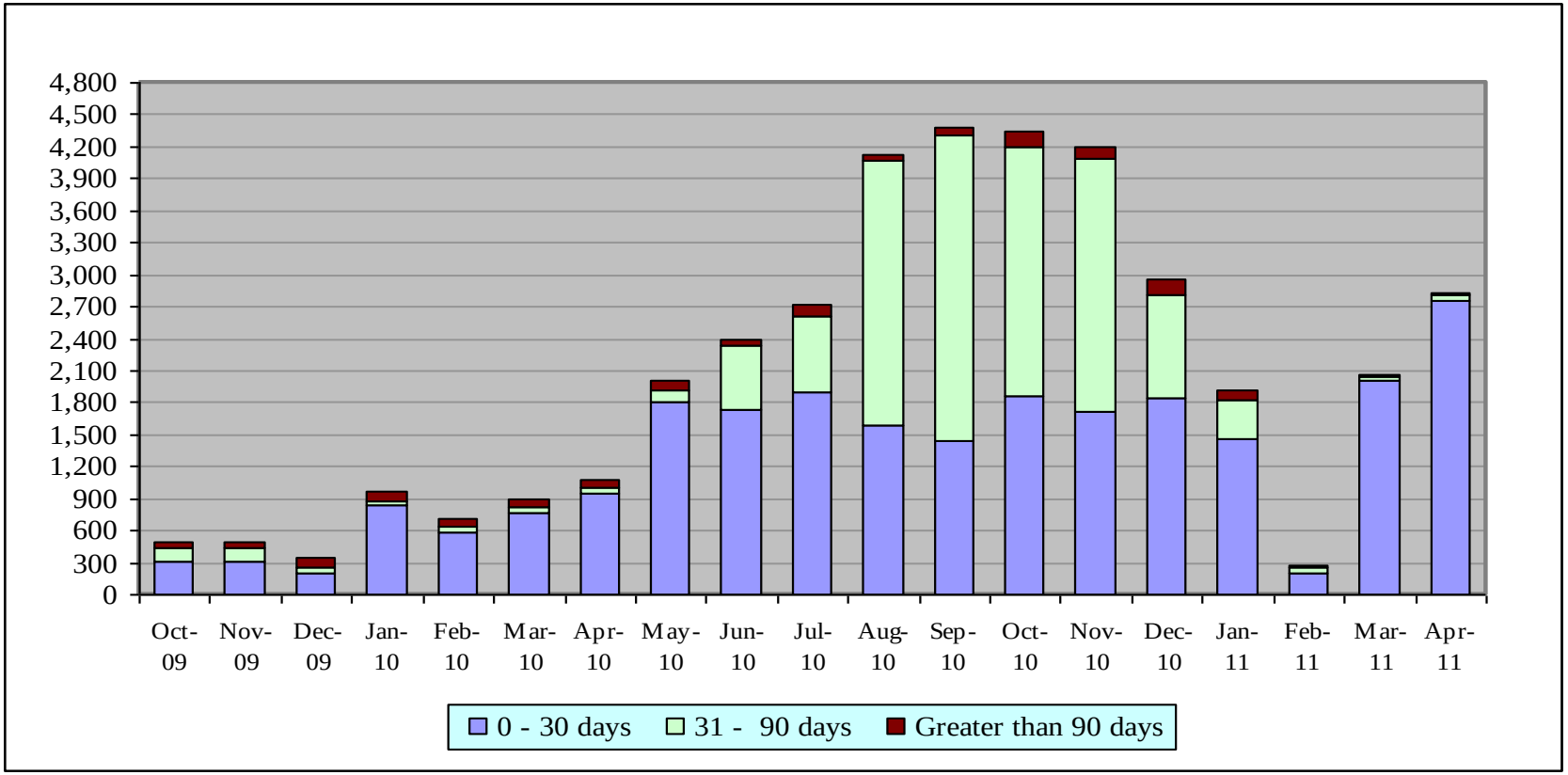
Category (Initial)	Oct-09	Nov-09	Dec-09	Jan-10	Feb-10	Mar-10	Apr-10	May-10	Jun-10	Jul-10	Aug-10	Sep-10	Oct-10	Nov-10	Dec-10	Jan-11	Feb-11	Mar-11	Apr-11
0 - 20 days	4,797	2,650	2,002	4,752	3,656	5,331	5,642	6,759	6,414	6,087	3,666	2,975	4,661	5,643	5,709	6,020	6,782	6,635	6,526
21 - 90 days	3,349	1,987	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	2,781	1,723
Greater than 90 days	91	269	557	653	591	550	505	374	315	599	315	379	1,799	670	593	414	192	218	55
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	9,634	8,304

Source: JPAS and CATS

Defense Industrial Security Clearance Office

FY11 Adjudication Inventory

SSBI/NACLC Periodic Reinvestigation Clearance Adjudications

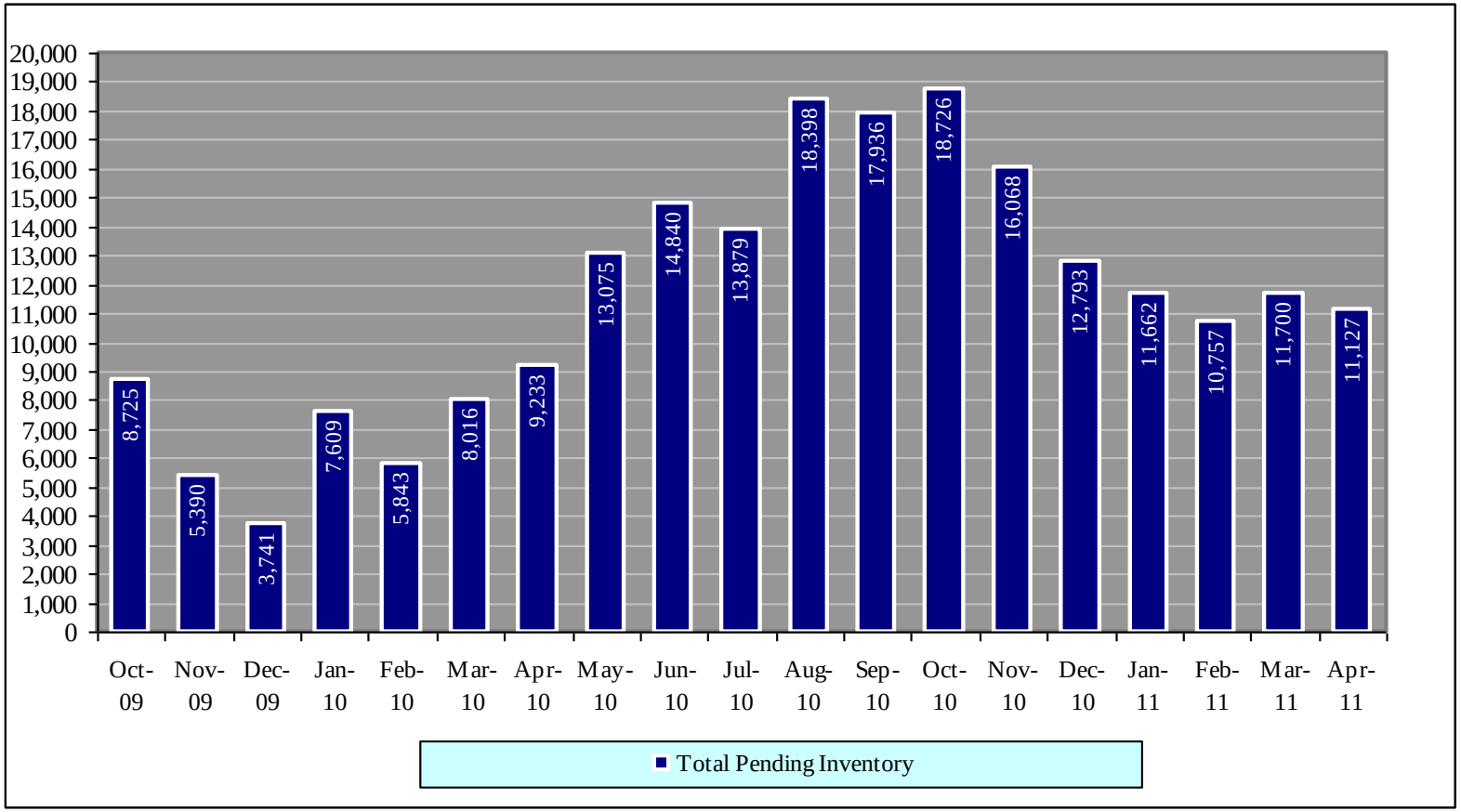


Category (PR)	Oct-09	Nov-09	Dec-09	Jan-10	Feb-10	Mar-10	Apr-10	May-10	Jun-10	Jul-10	Aug-10	Sep-10	Oct-10	Nov-10	Dec-10	Jan-11	Feb-11	Mar-11	Apr-11
0 - 30 days	308	312	201	831	586	761	946	1,812	1,733	1,890	1,583	1,437	1,868	1,718	1,843	1,454	201	2,005	2,757
31 - 90 days	133	135	54	53	47	56	55	113	599	722	2,496	2,877	2,331	2,373	967	380	52	32	52
Greater than 90 days	47	37	87	82	73	71	73	82	51	111	50	58	142	108	145	79	13	29	14
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	2,066	2,823

Source: JPAS and CATS

Defense Industrial Security Clearance Office
FY11 Adjudication Inventory

SSBI/NACLC Periodic Reinvestigation Clearance Adjudications



- Initial and Periodic Reinvestigation inventory combined has reduced 41% since the start of FY11.

FY11 INDUSTRY CASES AT OPM

Investigation Inventory

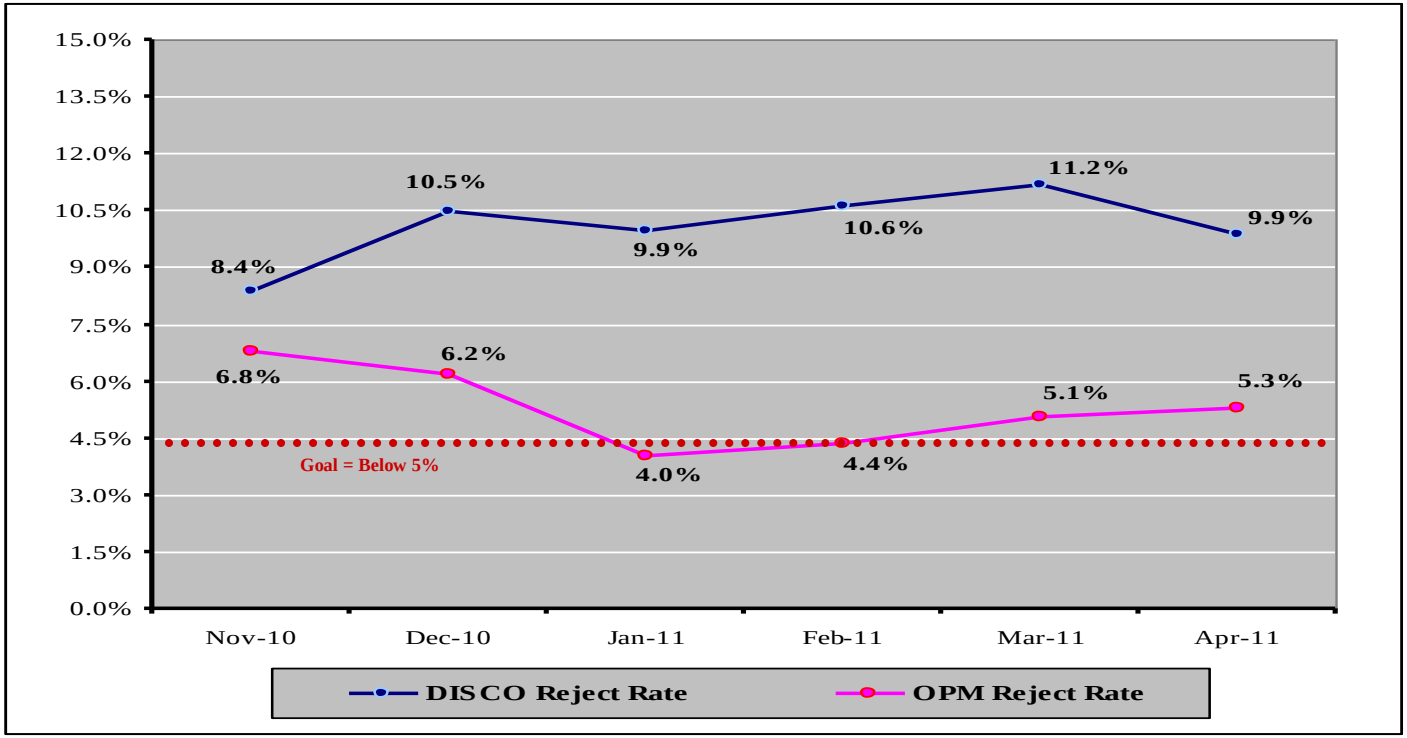
Case Type	FY09				FY10				FY11			Delta Q1FY10 vs Apr FY11
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Apr-11	
NACLC	13,209	13,982	13,900	12,307	11,730	11,685	13,016	13,556	13,118	13,243	12,977	11%
SSBI	6,626	6,687	6,944	6,561	6,782	7,012	6,561	6,178	6,308	5,578	5,568	-18%
SSBI-PR	3,772	4,160	4,692	3,703	4,096	4,521	4,859	5,115	5,436	7,521	6,625	62%
Phased PR	5,430	2,771	2,476	2,640	3,158	3,629	3,665	4,248	4,781	5,148	4,727	50%
Total Pending	29,037	27,600	28,012	25,211	25,766	26,847	28,101	29,097	29,643	31,490	29,897	16%

Overall increase of 16% for NACLC, SSBI, SBPR and PPR case types from 1QFY10 through April 2011.

Source: OPM Customer Support Group

FY11 REJECT RATE

Initial and Periodic Reinvestigation Clearance Requests



November 2010 to April 2011:

- **DISCO Received 79,558** investigation **requests**
  - **Rejects – DISCO rejected 8,076 (10.2% on average since November 2010)** investigation requests to FSOs for re-submittal
- **OPM Received 88,682** investigation **requests**
  - **Rejects – OPM rejected 4,908 (5.5% on average since November 2010)** investigation requests to DISCO (then to FSO's) 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 Reports

FY11 REJECTS

DISCO Rejections by Facility Category

Month	FACILITY CATEGORY						
	A	AA	B	C	D	E	OTHERS
Oct	0.6%	0.2%	0.5%	0.9%	3.2%	5.7%	0.1%
Nov	0.5%	0.1%	0.5%	0.9%	3.2%	5.3%	0.0%
Dec	0.6%	0.2%	0.5%	1.1%	3.6%	6.0%	0.2%
Jan	0.7%	0.2%	0.6%	1.2%	4.3%	6.8%	0.2%
Feb	0.7%	0.2%	0.6%	1.2%	4.4%	7.7%	0.2%
Mar	0.6%	0.2%	0.6%	1.2%	5.6%	9.0%	0.2%
Apr	0.5%	0.1%	0.5%	1.1%	3.9%	7.5%	0.2%
May [1]	0.2%	0.1%	0.2%	0.5%	1.7%	3.2%	0.2%
Grand Total	**4.3%**	**1.1%**	**4.0%**	**8.1%**	**30.0%**	**51.2%**	**1.2%**

100%

[1] As of May 09, 2011

DISCO Case Rejections

- More than 80% originate from smaller Category D and E facilities

Source: e-Qip

FY11 REASONS - DISCO

Case Rejections

#	REASON	% Rejected	% Accounted
1	Missing employment information for the submitting agency	**26%**	26%
2	Missing complete and accurate information concerning listed debts or bankruptcy	**26%**	51%
3	Request ID Number does not match e-QIP and Certification and/or Release(s)	**9%**	60%
4	Missing legal exemption for not registering with the Selective Service	**7%**	68%
5	Non-receipt of Certification or Release Forms	**6%**	74%
6	Missing information on relative born abroad	**5%**	79%
7	Missing social security number of spouse	**4%**	83%
8	Missing social security number for adult co-habitant	**4%**	87%
9	Missing information for former spouse	**2%**	89%
10	Missing references, character, residential, employment or educational	**2%**	**91%**
11	Missing documentation of U.S. Citizen born abroad	2%	93%
12	Missing information pertaining to arrest	1%	94%
13	Missing passport information with recent foreign travel	1%	96%
14	Current residence and employment are not within commuting distance	1%	96%
15	Missing complete and accurate information concerning listed drug use	1%	97%
16	Missing complete and accurate information concerning listed foreign passport	1%	98%
17	Illegible or missing information on release forms	1%	98%
18	Missing 7 years consecutive employment history (10 years for SSBI)	1%	99%
19	Missing 7 years consecutive residence history (10 years for SSBI)	0%	99%
20	Missing complete and accurate information concerning listed foreign travel	0%	100%
21	Missing complete and accurate information concerning listed foreign financial interests	0%	100%
22	Discrepant place of birth.	0%	100%
		100%	

- 50% are attributable to missing current employment activity and financial information
- Top 10 reasons account for 91% of DISCO's case rejections

FY11 REASONS - OPM

Case Rejections

#	REASON	% Rejected
1	**Missing fingerprint cards**	**68%**
2	Illegible or missing information on release forms	16%
3	Discrepant place of birth.	4%
4	Discrepant date of birth.	3%
5	Missing references, character, residential, employment or educational	2%
6	Discrepant social security number	1%

- **OPM case rejections are persistently due to missing fingerprint cards.**

Attachment #3- DAA C&A Presentation

Defense Security Service

Industrial Security Field Operations (ISFO)

Office of the Designated Approving Authority (ODAA)

May 2011

Defense Security Service

Overview:

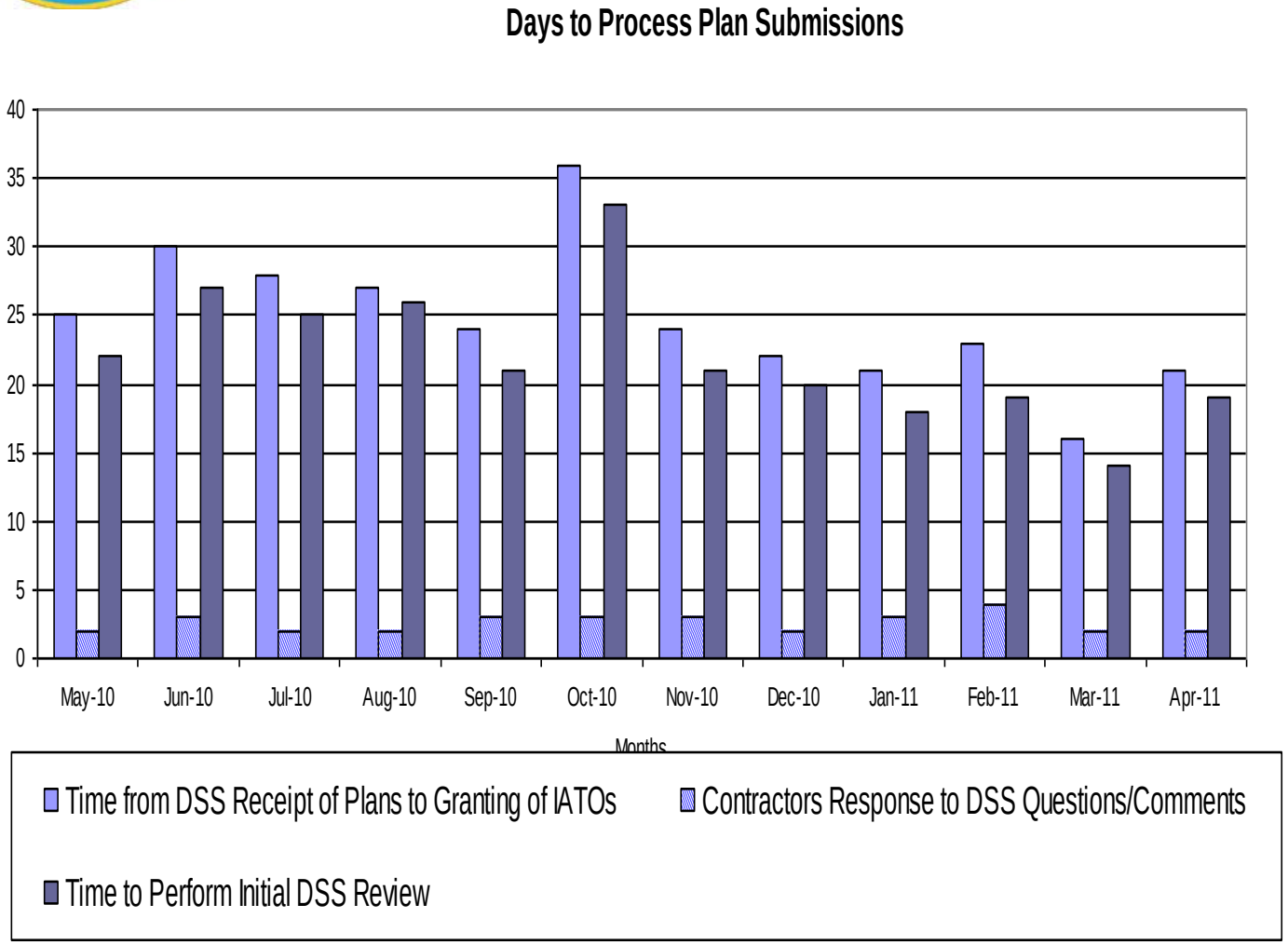
- Certification & Accreditation (C&A)
- ODAA Metrics
  - Timeliness and Consistency
  - Security Plan Review
  - Security Plan Review Errors
  - System Validation
  - Plan Submission Denials and Rejections
  - 2nd IATO Metrics

Defense Security Service

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.**

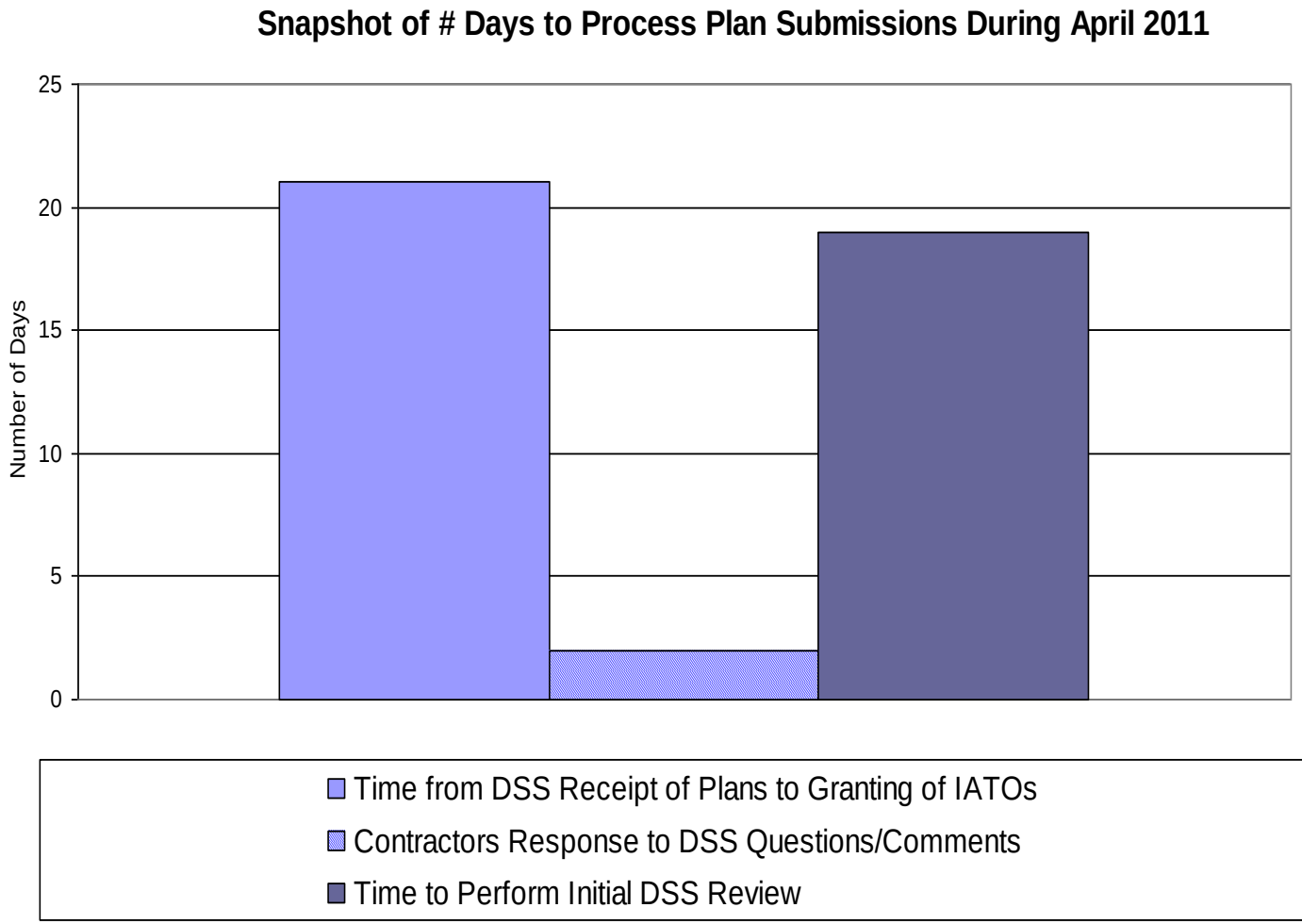
ODAA Improving Accreditation Timeliness and Consistency



(May 2010 – Apr 2011 Metrics)

- 4805 IATOs Issued
- The average number of days to issue an IATO for a system after plan submission was 25 Days
- The average number of days for a system under IATO to go to ATO status was 82

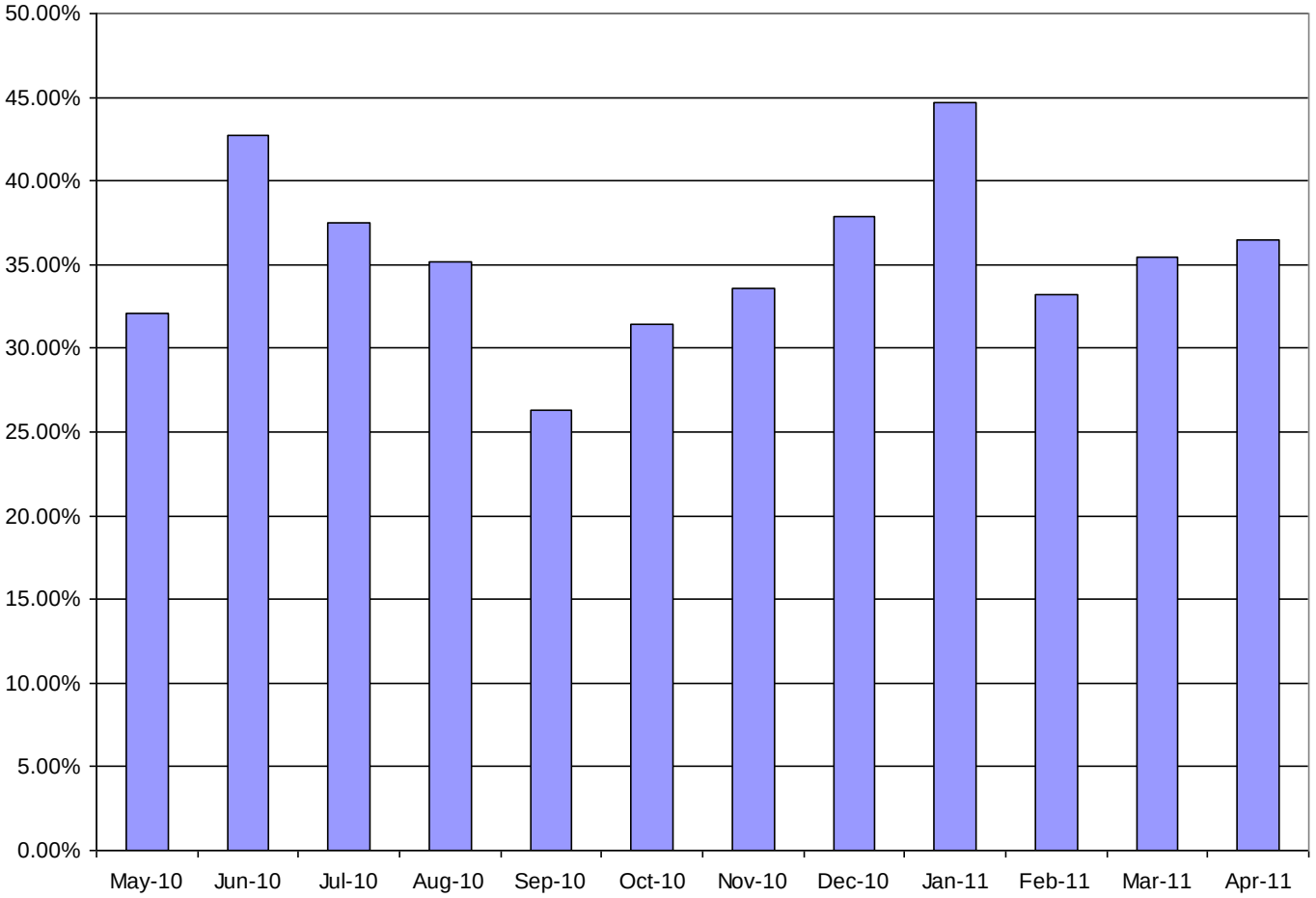
ODAA Improving Accreditation Timeliness and Consistency



- 370 IATOs granted
- The average number of days to issue an IATO after submission of a plan was 21 days

Security Plan Review Metrics

Plans With Errors/Corrections Noted During Review



May 2010 – Apr 2011

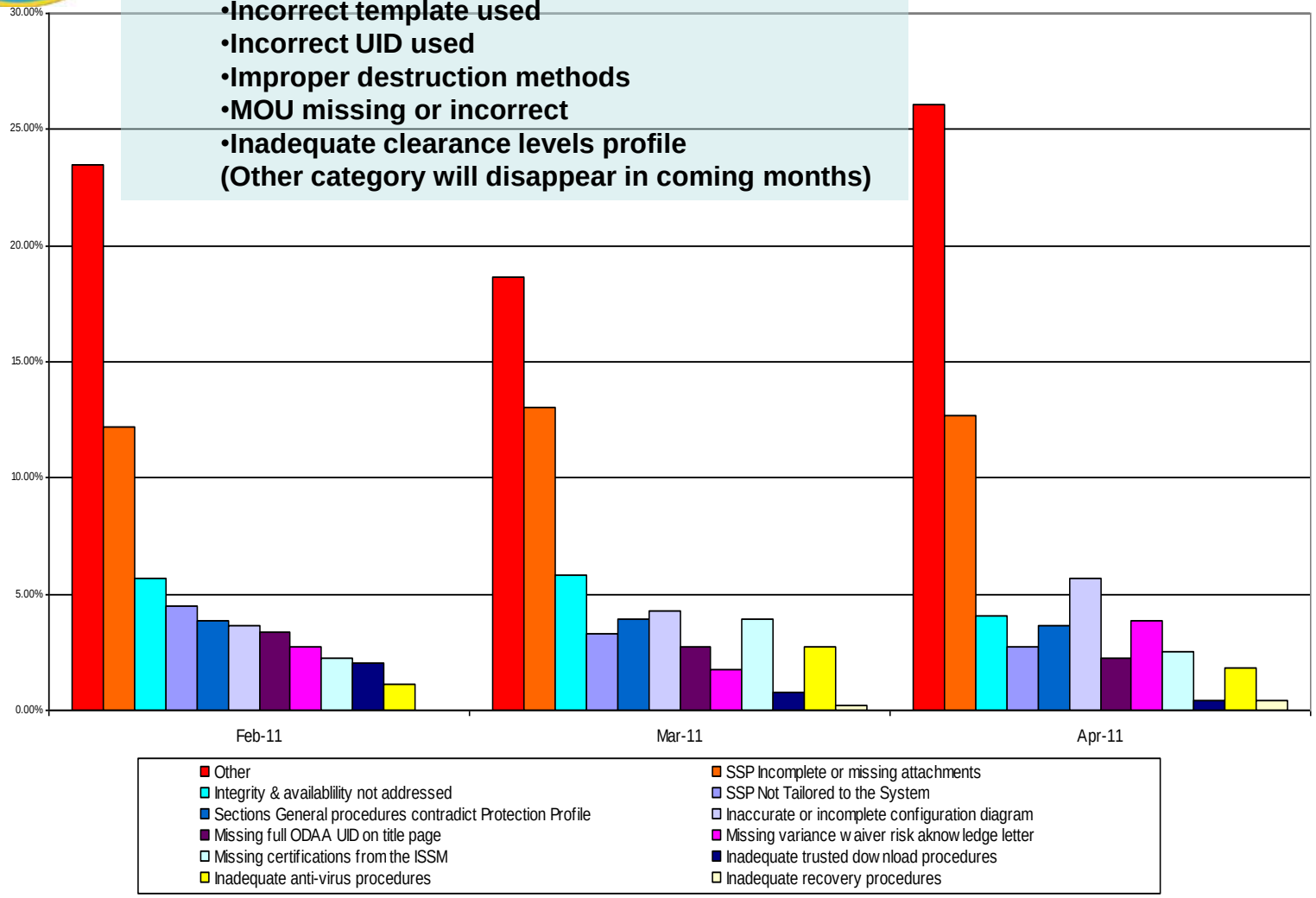
- Received/reviewed 5229 plans
- 4805 IATOs issued
- 424 IATOs denied due to plan corrections needed (processed after corrections made)
- 36.0% of the plans submitted required corrections prior to the onsite validation for ATO

Security Plan Review Common Errors

Other Errors Include

- **Incorrect template used**
- **Incorrect UID used**
- **Improper destruction methods**
- **MOU missing or incorrect**
- **Inadequate clearance levels profile**

(Other category will disappear in coming months)



Security Plan Review Common Errors by Facility Category

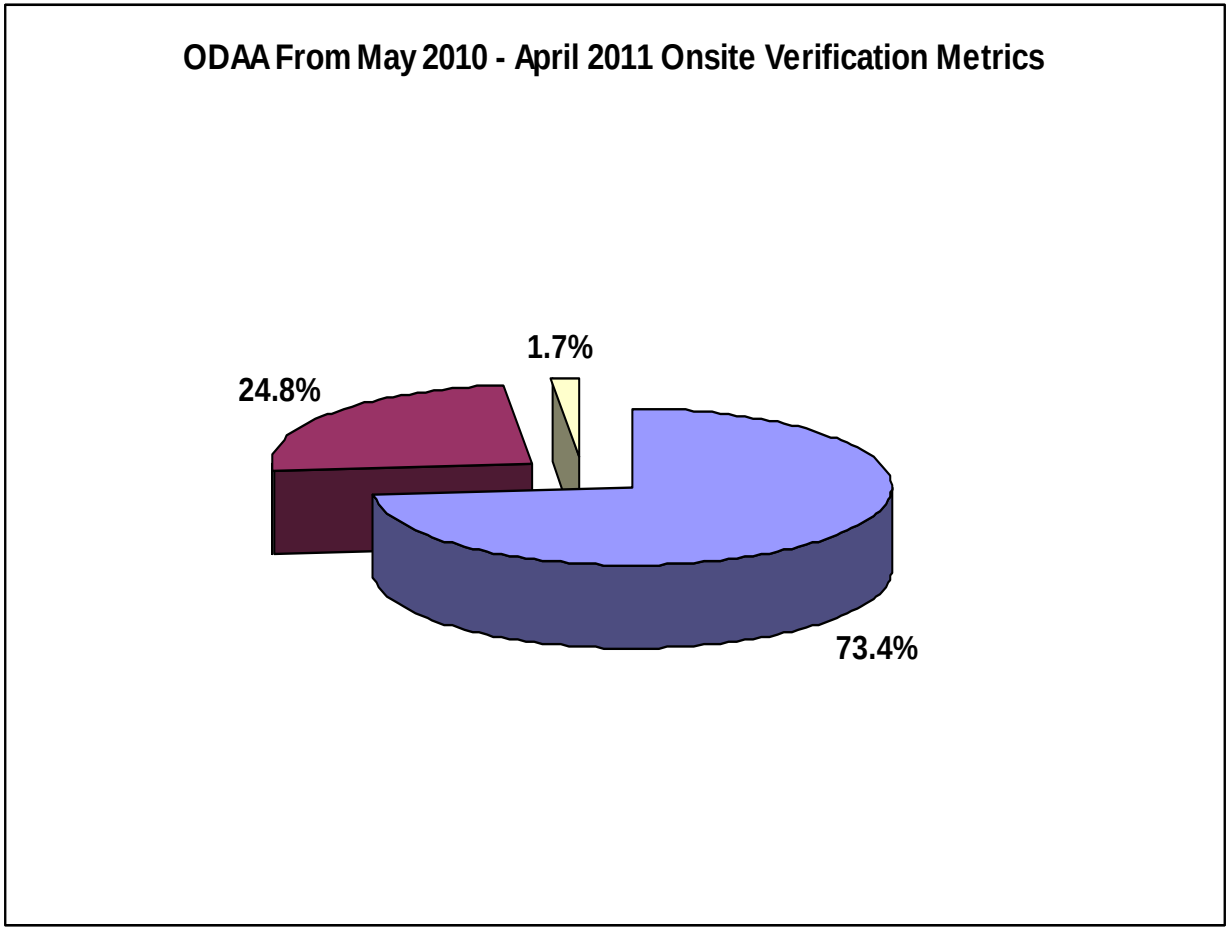
Number of Plans Submitted (11/2010 – 2/2011 Numbers)		133	273	180	214	422
	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
SSP Is incomplete or missing attachments	191	26.32%	4.76%	10.00%	17.76%	16.59%
Integrity & Availability not addressed completely	182	11.28%	12.82%	12.78%	15.89%	15.17%
Inaccurate or Incomplete Configuration diagram/system description	94	15.79%	5.86%	8.33%	3.74%	7.58%
Other	82	3.76%	4.40%	6.11%	3.74%	10.43%
Sections in General Procedures contradict Protection Profile	70	12.78%	3.66%	2.78%	3.27%	6.16%
SSP Not Tailored to the System	64	0.75%	4.03%	11.11%	7.01%	3.79%

Security Plan Review Common Errors by Facility Category (cont'd)

	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Missing full ODAA UID on Title Page	50	0.00%	2.20%	**5.00%**	1.87%	**4.98%**
Missing certifications from the ISSM	32	2.26%	2.20%	1.11%	1.40%	3.55%
Missing variance/waiver/risk acknowledgement letter	30	**3.76%**	1.47%	3.33%	0.47%	2.61%
Inadequate anti-virus procedures	28	2.26%	0.73%	2.22%	0.47%	4.03%
Inadequate trusted download procedures	15	1.50%	0.73%	0.56%	0.47%	1.18%
Inadequate recovery procedures	3	0.00%	0.00%	0.56%	0.00%	0.47%
Total Errors %	**841**	**12.72%**	**13.91%**	**13.67%**	**14.27%**	**38.41%**
Total Errors	**841**	**107**	**117**	**115**	**120**	**323**

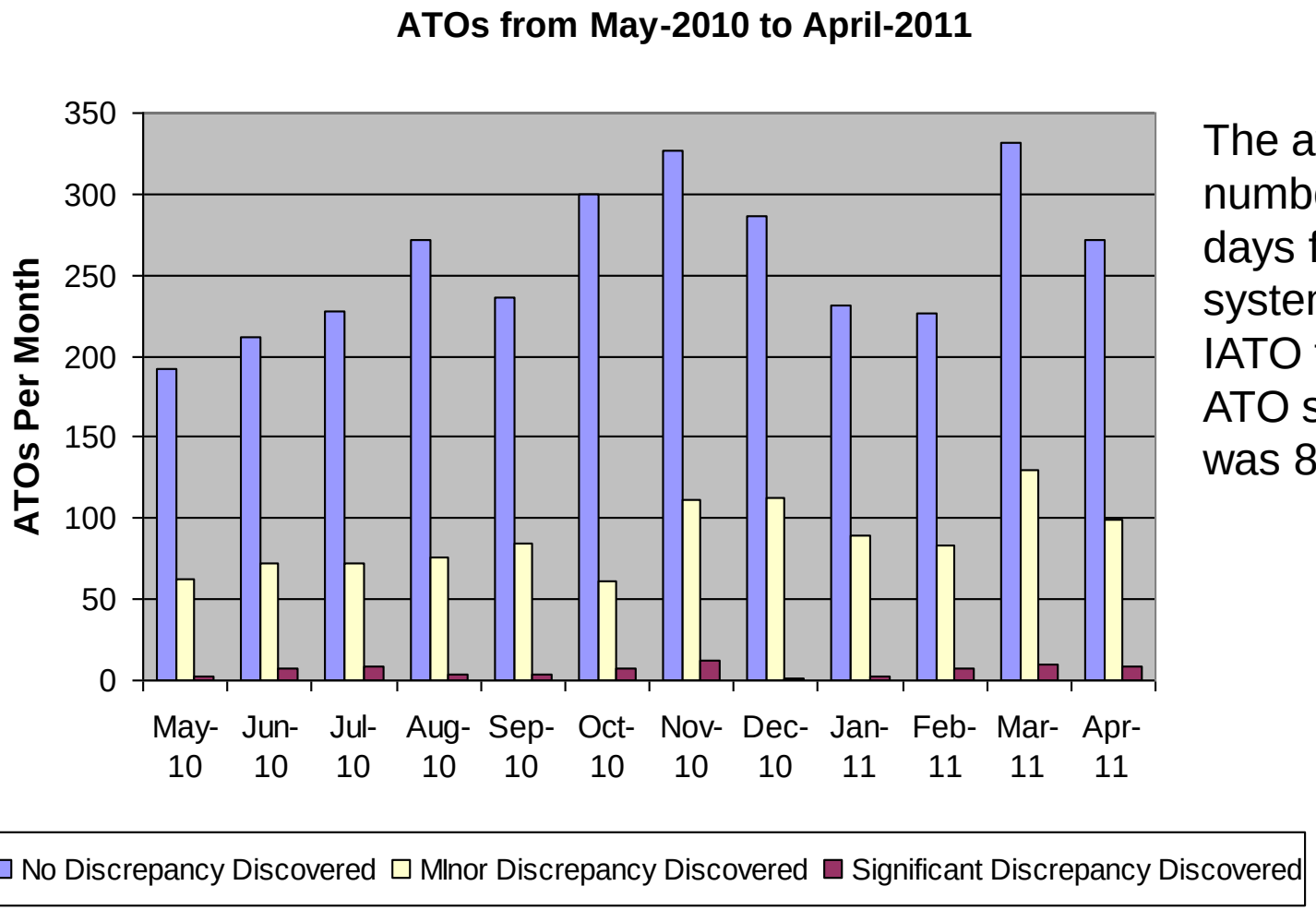
System Validation Metrics

26.5% of Systems Required Correction



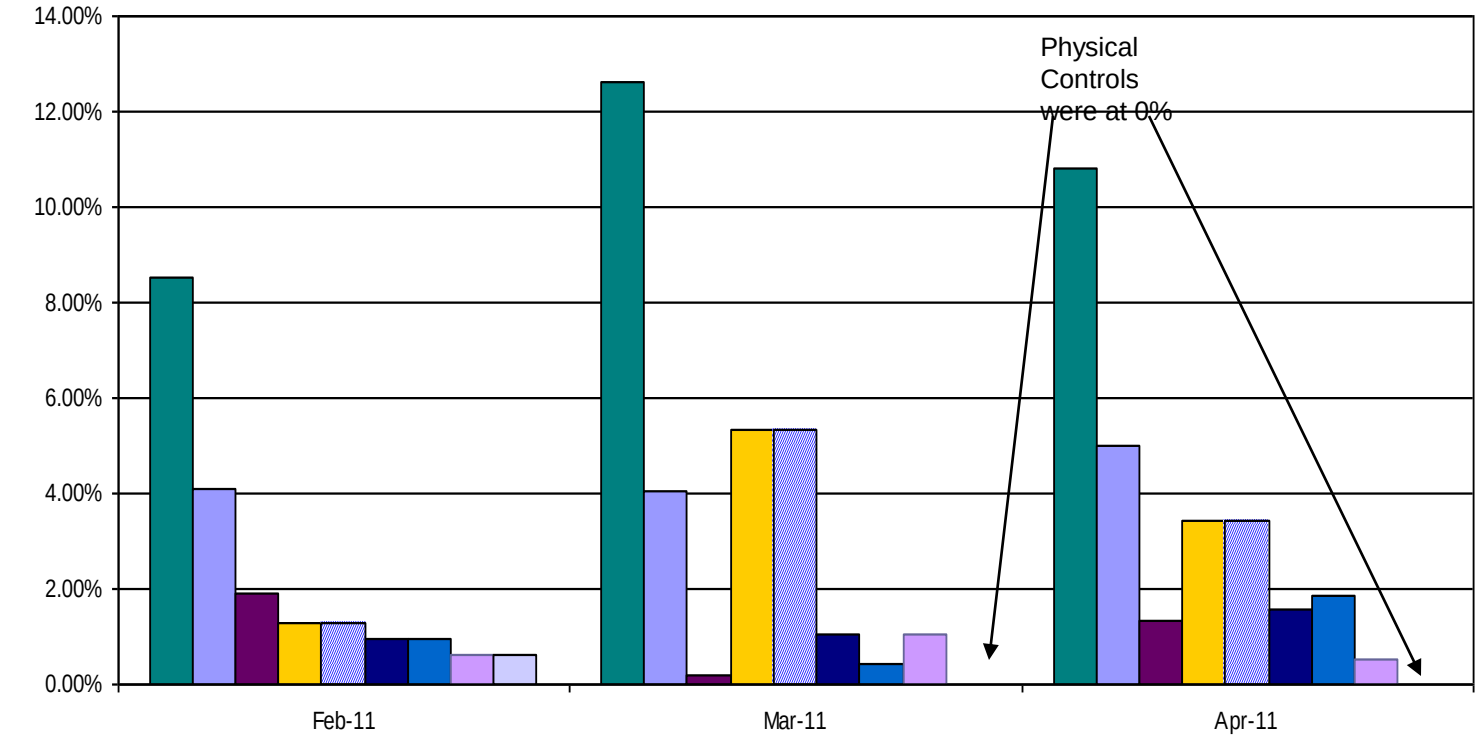
- 3115 systems (73.4%) had no discrepancies identified during the onsite validation
- 1052 systems (24.8%) had minor discrepancies identified and corrected during the onsite validation
- 74 systems (1.7%) had significant discrepancies identified that could not be resolved (second validation visit required)

System Validation Metrics by Month



The average number of days for a system under IATO to go to ATO status was 82.

Common System Validation Discrepancies



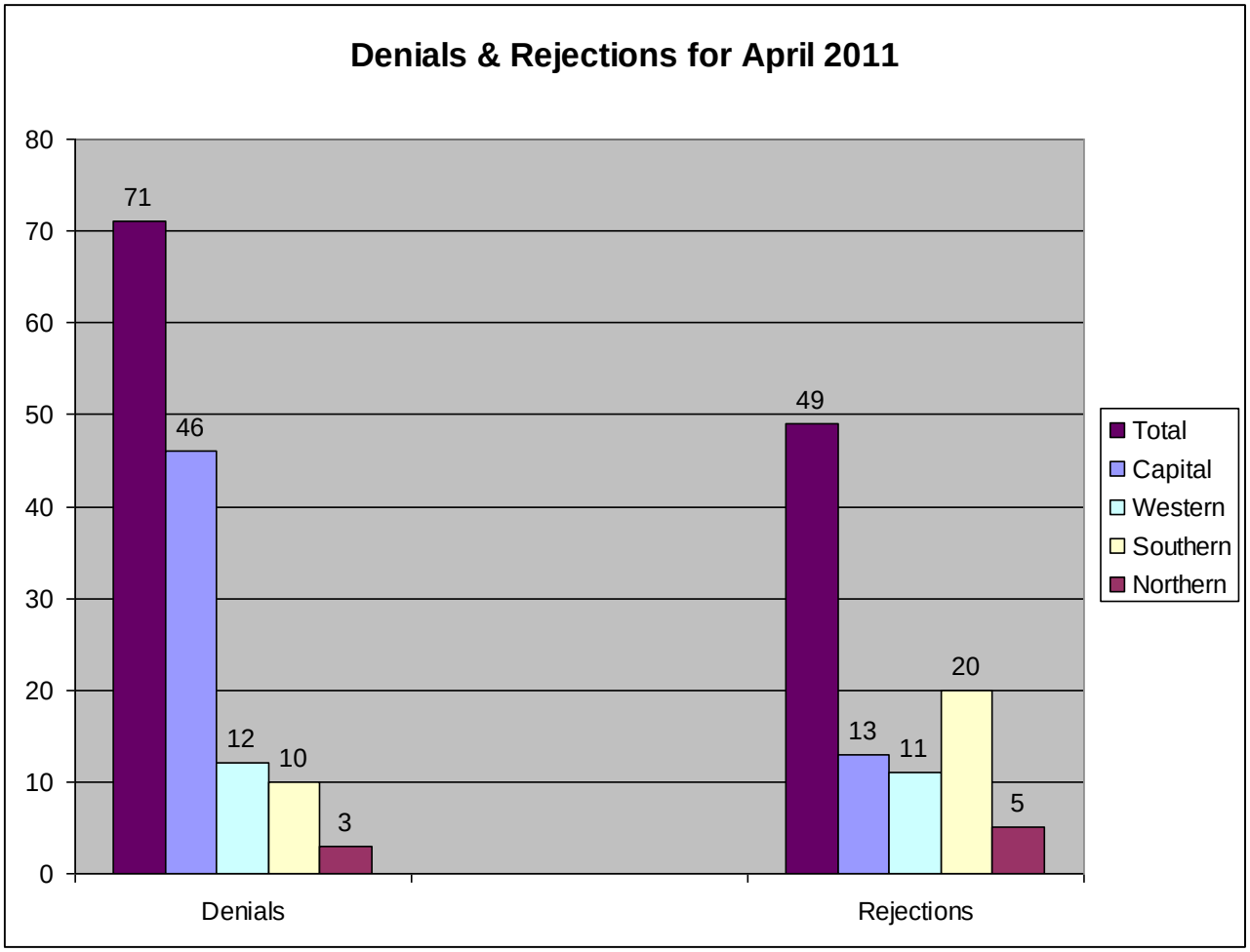
System Validation Discrepancies by Facility Category

Systems Validated by Facility Category (11/2010 – 2/2011 Numbers)		160	409	210	241	404
	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Auditing	**114**	**2.50%**	**3.18%**	**2.86%**	**8.30%**	**16.34%**
Security Relevant Objects not protected	**59**	**1.25%**	0.24%	**2.38%**	**2.90%**	9.90%
Other	**43**	0.00%	**2.69%**	**1.43%**	**6.64%**	**2.97%**
Bios not Protected	**22**	0.00%	0.49%	**1.43%**	**2.07%**	2.72%
Topology not correctly reflected in (M)SSP	**22**	0.00%	0.49%	**1.43%**	**2.07%**	2.72%
Session Controls	20	**2.50%**	0.00%	**3.33%**	1.24%	1.49%
Configuration Management	18	**3.13%**	**0.98%**	0.48%	0.41%	1.49%
Root/Admin Account misconfigured	17	0.00%	0.49%	0.95%	0.00%	**2.97%**
Inadequate anti-virus procedures	10	0.00%	0.49%	0.48%	0.41%	1.49%
Physical Controls	9	**1.25%**	0.00%	0.48%	0.83%	0.74%

System Validation Discrepancies by Facility Category (cont'd)

	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
SSP Does Not Reflect How the System is Configured	8	0.00%	0.49%	0.00%	0.00%	1.49%
I & A	7	0.00%	0.00%	0.00%	1.24%	0.99%
Trusted Download Review	6	0.00%	0.24%	0.00%	0.41%	0.99%
RAL Not Provided	4	0.00%	0.49%	0.95%	0.00%	0.00%
Different System Type	2	0.00%	0.00%	0.00%	0.41%	0.25%
All Users are Configured as Administrators	2	0.63%	0.24%	0.00%	0.00%	0.00%
NSP Not Provided/Referenced for a WAN Node	1	0.00%	0.24%	0.00%	0.00%	0.00%
Compilation	1	0.00%	0.00%	0.00%	0.00%	0.25%
PL Not Adequately Addressed	1	0.00%	0.00%	0.48%	0.00%	0.00%
POA&M not Implemented	1	0.00%	0.00%	0.00%	0.00%	0.25%
Total Errors %	**367**	**4.90%**	**11.99%**	**9.54%**	**17.71%**	**51.77%**
Total Errors	**367**	**18**	**44**	**35**	**65**	**190**

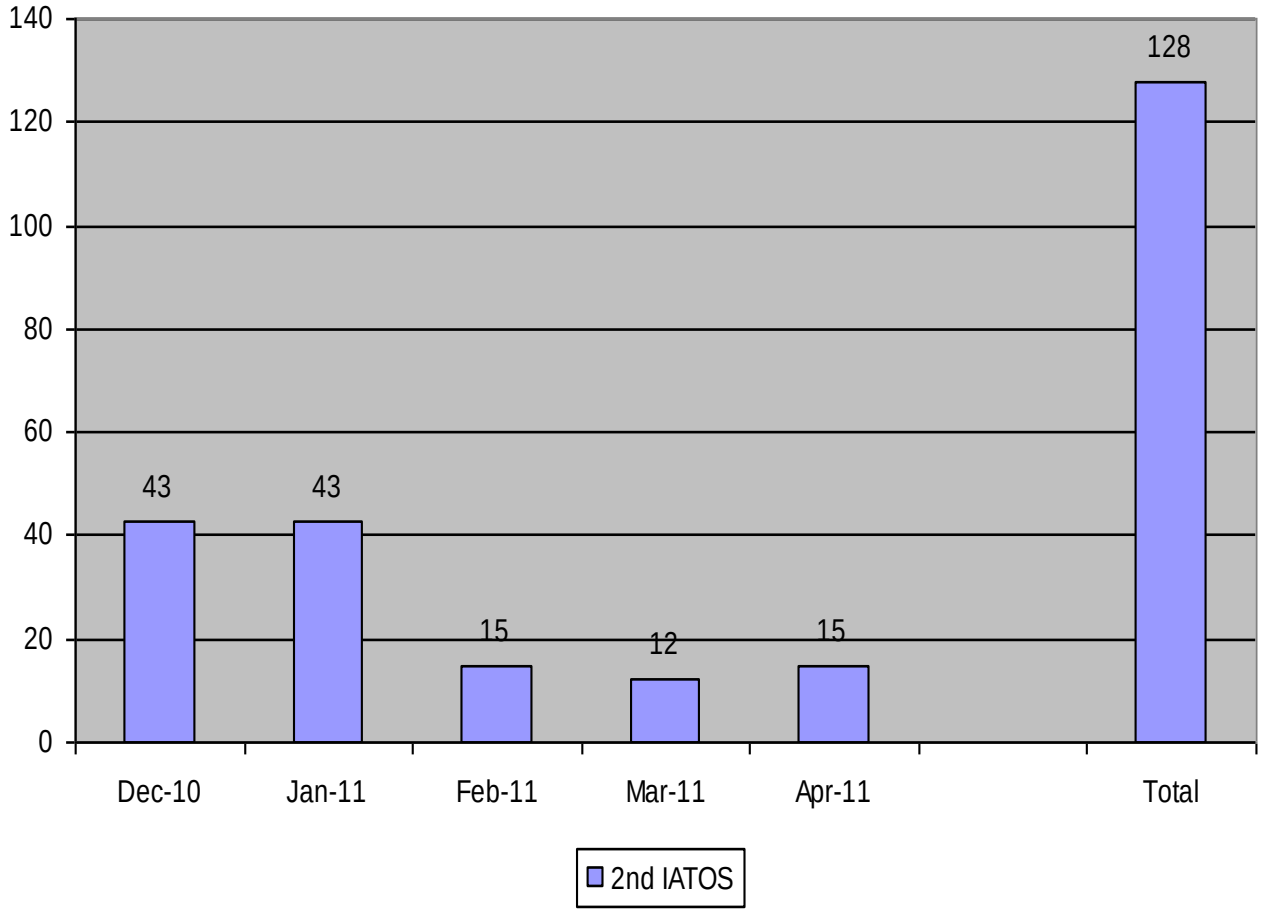
Plan Submission Denials & Rejections



- Denials - Plans were received and reviewed. An IATO could not be issued until corrections were made to the plans.

- Rejections - Plans not submitted in accordance with the ISFO Process Manual and not entered into the ODAA database. Plans are returned to the ISSM and must be resubmitted correctly for processing.

Second IATOs Issued



Most Common Reasons for Issuing Second IATOs

- Corrections not made or Plan of Action and Milestone (POAM) items not addressed
- Onsite rescheduled due to ISSP and/or ISSM availability

Attachment #4- SLTPS Presentation

Implementation of the Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Within the NISP

June 20, 2011

Homeland Security

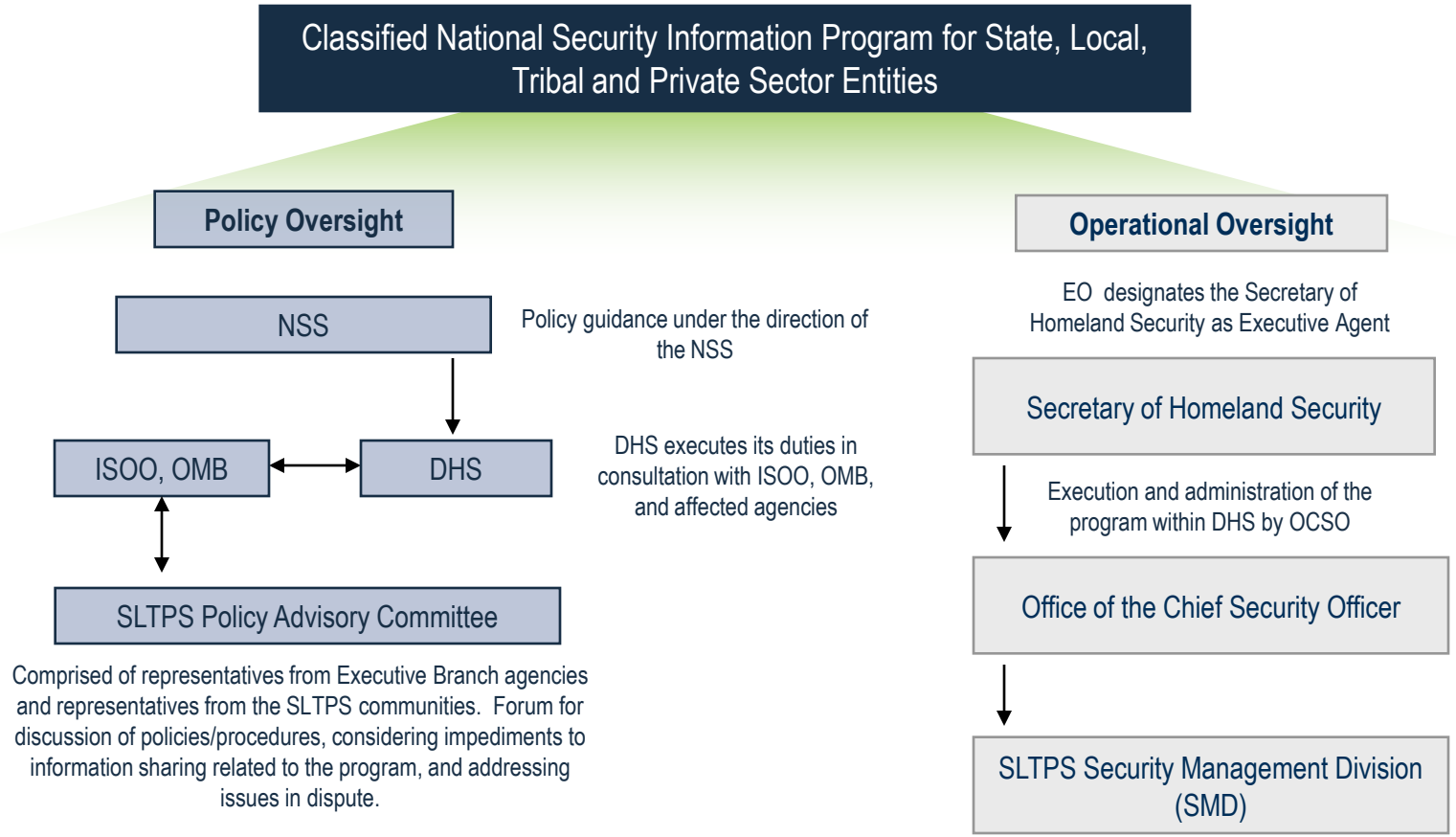
Why the Program was Established

- No singular overarching program or policy existed within the Executive Branch to address security standards associated with access to and safeguarding of classified information shared with the State, local, tribal, and private sector (SLTPS) communities.
- The application of various security policies and procedures on the SLTPS community by the Executive Branch is inconsistent and causes controversy and confusion which in-turn discourages or impedes information sharing among Federal agencies and SLTPS communities.

Areas of Concern	
1. Granting of security clearances	• Appropriate working level clearances for SLTPS partners • Timeliness and quality of the SLTPS security clearance processes
2. Reciprocity of clearances, standards, certifications	• Security clearances, standards, and certifications issued by one agency are not necessarily accepted by another agency • No single database to capture and track SLTPS personnel clearances
3. Deployment of classified capabilities to SLTPS locations	• Unclear and inconsistent safeguarding requirements for classified information
4. Certification of SLTPS secure facilities	• Lack of uniform certification standards for facilities where classified capabilities are deployed • No single database to capture and track secure facilities
5. Security oversight	• Lack of a centralized governance structure to monitor program implementation
6. Security training	• Lack of standardized initial and refresher training requirements and accountability for completion

Solution: Classified National Security Information Program for State, Local, Tribal and Private Sector Entities

- Executive Order 13549, signed by the President on August 18, 2010, establishes a Classified National Security Information Program for State, Local, Tribal and Private Sector Entities, to standardize the implementation, management, and oversight for access to and safeguarding of classified information shared with SLTPS partners.



Homeland Security

As Executive Agent DHS will:

- Issue an Implementing Directive in consultation with affected agencies and the concurrence of DOD, DOJ, ODNI, and ISOO
- Provide overall program management and oversight
- Certify, inspect, and monitor SLT facilities where classified is stored
- Process security clearance applications for DHS and, upon agreement, other agencies
- Document and track SLTPS security clearance status in consultation with OPM, DOD, and ODNI
- Develop and maintain SLT security profiles on locations where classified information is stored
- Develop SLTPS standardized security training in consultation with the SLTPS Policy Advisory Committee
- Serve as vice-chair of the SLTPS Policy Advisory Committee
- Establish the SLTPS Security Management Division

Homeland Security

Inter-relationship with Other Orders and Authorities:

- EO will be implemented consistent with existing executive branch policy and standards as promulgated through:
  - EO 13526, “Classified National Security Information,” Jan 5, 2010
  - EO 12968, “Access to Classified Information,” Aug. 7, 1995 (as amended by EO 13467 in 2008)
  - EO 12829, as amended, “National Industrial Security Program,” Jan. 6, 1993 (as amended by EO 12885 in 1993)
  - EO 13388, “Further Strengthening the Sharing of Terrorism information to Protect Americans,” Oct. 27, 2005
  - EO 13467, “Reforming Processes Related to Suitability for Government, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information,” Jun. 30, 2008
- EO is a support mechanism that compliments the statutory authorities and responsibilities of the Program Manager for the Information Sharing Office, the National Counterterrorism Center, the Federal Bureau of Investigation, and the DHS Office of Intelligence & Analysis relative to information sharing.

The EO 13549 and the National Industrial Security Program

EO 13549:

- Developed to ensure security standards are consistently applied in accordance with multiple EOs to include EO 12829, as amended ("National Industrial Security Program")
- States that Private Sector facilities where classified information is to be stored shall adhere to the standards established by the DOD pursuant to EO 12829
- States that the NISP shall govern access to and safeguarding of classified information released to contractors, licensees and grantees of State, Local and Tribal entities
- States that the EO does not change the requirements of EOs 13526, 12968, 13467 or 12829 as amended

  "Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Defense under Executive Order 12829, as amended"

Homeland Security

The Classified National Security Program for SLTPS Interactions with the Private Sector

Private Sector Security Clearances

- The granting of security clearances for Private Sector (PS) personnel who do not fall under the purview of Executive Order 12829 are processed in the same manner as SLT, and limited to the minimum number necessary to support critical infrastructure and the security of the homeland
- Eligibility for a PS security clearances is determined by a sponsoring agency and does not apply to any corporation, company, contractor, licensee, grantee, or individual that has or intends to enter into a contractual or consulting agreement with the Federal government pursuant to EO 12829
- Security clearances may be granted to PS personnel involved in ensuring that public and private preparedness and response efforts are integrated as part of the Nation's Critical Infrastructure or Key Resources (CIKR) and include:
  - Corporate owners and operators determined to be part of the CIKR
  - Subject matter experts selected to assist the Federal or State CIKR
  - Personnel serving specific leadership positions of CIKR coordination, operations, and oversight
  - Employees of corporate entities relating to the protection of CIKR

Additional Interactions with the Private Sector

The Limited Deployment of Secure Telephone Equipment (STE) to Uncleared PS Facilities

Deployment of STE and associated encryption devices does not constitute on-site physical storage of classified information. Therefore these devices may be deployed to selected PS facilities that are not cleared under the purview of the NISP, when the following conditions are met:

- The sponsoring agency validates its intent to share classified information with the intended recipient
- The device is encrypted no higher than the collateral Secret level
- DHS or a Federal agency completes a risk assessment regarding the deployment of the device at the PS facility to include a determination of foreign ownership
- If there is foreign ownership, the NSA Information Assurance Directorate will determine the acceptability of the deployment
- Verification of the individual's security clearance and the completion of a statement of understanding
- Validation the room meets the minimum security requirements for deployment and key storage
- Note taking and connecting and configuring the STE to send or receive documents is prohibited

On-site physical storage of classified information by PS entities falls under the purview of EO 12829, "National Industrial Security Program," and the NISPOM

SLT Classified Contracting Under the NISP

The Implementing Directive codifies a process in which SLT may enter into classified contracts under the security cognizance of DSS and the requirements of the NISPOM. The criteria include:

- The SLT entity has a defined counter-terrorism or homeland security mission and is provided classified access by DHS or another Federal agency
- The SLT entity submits a request to DHS or an office in another Federal agency with responsibility for information sharing and direct knowledge of the SLT activities
- Classified contracts are limited to companies with a FCL issued by an authorized Federal agency under the NISP
- Companies issued classified contracts under these procedures are not permitted to sub-contract without prior approval
- Access to classified information for SLT contracts is at the Secret level
- Contract employees must possess an appropriate personnel security clearance (PCL)
- DHS or the sponsoring Federal agency enters into an agreement with the contractor
- When the above requirements are met, DHS or another Federal agency issues a DD Form 254, "Contract Security Classification Specification"

Thereafter, the contractor is under the security cognizance and oversight of DSS and continues to be subject to the requirements of the NISPOM.

Homeland Security

Benefits of the Program:

- A governance structure with policy and operational oversight that specifically addresses the security aspects for access to and safeguarding of classified information by SLTPS personnel
- An advisory committee comprised of Federal and SLTPS representation to advise on all matters of the Program
- Clear eligibility requirements for SLTPS access to classified information
- Reciprocity of security clearances issued to SLTPS personnel
- Consistent requirements for the physical custody and safeguarding of classified information and capabilities at SLTPS facilities, to include fusion centers
- Centralized databases for all SLTPS personnel and facility security records
- An implementing directive that describes and defines specific requirements, restrictions, and other safeguards
- A robust security training, education, and awareness program

Homeland Security

Current Status:

- EO signed by the President on August 18, 2010 (Implementation Date February 14, 2011)
- SLTPS PAC member nominees submitted to ISOO on September 27, 2010, first PAC meeting held in January 11, 2011
- HSIN SLTPS Security Administration Community of Interest developed in April 2011
- Initial and ongoing discussions with OPM, DOD, and ODNI on security clearance tracking began in 2010
- Approval within DHS for the establishment of the Security Management Division April 2011
- Implementing Directive completed with concurrence from DOD, DOJ, ODNI and ISOO in April 2011
- Implementing Directive in final coordination with Secretary of Homeland Security

Homeland Security

Future Actions

- Maintain implementing directive
- Develop internal SOP's
- Open HSIN Security COI to SLTPS and Federal community
- Implement SLT security agreements
- Implement Private Sector statements of understanding
- Establish agency out-reach
- Coordinate agreements with other agencies – i.e., security clearances and facility oversight
- Develop/publish educational products
- Develop/implement facility security profile data base
- Coordinate methodology for documenting/tracking SLTPS security clearances
- Prepare/coordinate compliance review checklists
- Implement compliance review program

Attachment # 5-CUI Presentation

CONTROLLED UNCLASSIFIED INFORMATION

Executive Order 13556, "Controlled Unclassified Information" (CUI)

- Signed by President Obama on November 4, 2010
- Identifies the National Archives as the Executive Agent
- Establishes a standardized system for managing unclassified information that requires controls

CONTROLLED UNCLASSIFIED INFORMATION

Process

- Agency category proposals submitted to Executive Agent by May 3, 2011
- Controlled Unclassified Information Notice 2011-01 published on June 9, 2011
- CUI Registry will be published by November 4, 2011
- Agency plans for compliance due December 6, 2011
- Phased Implementation Deadlines will be set following review of agency compliance plans

NATIONAL ARCHIVES

Contact Information

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

(202) 357-6870 (voice)
(202) 357-6871/6872 (fax)
cui@nara.gov
www.archives.gov/cui

Attachment # 6- Combined Industry Presentation

NATIONAL INDUSTRIAL SECURITY PROGRAM

POLICY ADVISORY COMMITTEE

(NISPPAC)

INDUSTRY PRESENTATION

JUNE 20, 2011

Outline

- Current Membership
  - NISPPAC
  - Industry MOU's
- Charter
- Working Groups
- Areas of Interest

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	Cloud Security Associates	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**
NCMS	**Tony Ingenito**
NDIA	**Jim Hallo**
Tech America	**Kirk Poulsen**

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**
  - **PKI Enabling JPAS**
  - **Potential BRAC Impacts**
- **Automated Information System Certification and Accreditation**
  - **Industrial Security Field Operations Manual**
  - **End-to-End processing time metrics**
- **NISPOM Review**

- **DoD SAP Manual Review**

Industry Areas of Interest

- **Information Sharing – Threat**
- **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**
  - **CUI Reform**

Industry Areas of Interest

- **IT Security Strategy**
  - **Implement – DFAR regarding IT security DIB-wide**
- **Insider Threat Programs**
  - **Repercussions from Wiki-Leaks**
  - **Increased focus on counterintelligence**
  - **Governance and governance gaps**
- **Data Spills**
  - **Costs & Impact**
  - **Damage to National Security**

Thank You