NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

SUMMARY MINUTES OF THE MEETING

The NISPPAC held its 42nd meeting on Wednesday, July 11, 2012, at 10:00 a.m. at the National Archives and Records Administration, 700 Pennsylvania Avenue, NW, Washington, DC 20408. John Fitzpatrick, Director, Information Security Oversight Office (ISOO) chaired the meeting, which was open to the public. These minutes were finalized and certified on October, 15, 2012.

I. Welcome and Administrative Matters

Mr. Fitzpatrick welcomed the attendees, and reminded everyone that NISPPAC meetings are recorded public events. He then asked Greg Pannoni, Associate Director of ISOO and NISPPAC Designated Federal Official (DFO) to review old business.

Refer to Attachment 1 for a list of meeting attendees.

II. Old Business

Mr. Pannoni noted that there were three open items from the last meeting. The first was a request that both the Personnel Security Clearance Working Group (PCLWG) and the Certification and Accreditation Working Group (CAWG) develop an observations and takeaway chart that provides a more complete and informative picture. The second item was for the PCLWG to report on the results of its dialogue with the Defense Industrial Security Clearance Office (DISCO) regarding common concerns on issues related to fingerprint processing. The final item was for DISCO to provide options to track the progress on issues relating to the Joint Personnel Adjudications System (JPAS). The Chair then called for the working group updates. He reminded the Committee that over the past year we've been trying to reflect the broadest possible characterization of the industry clearance experience, so we're adding the metrics from the Department of Energy (DOE), to the reports from the Office of Personnel Management (OPM), the Defense Security Service (DSS), and the Office of the Director of National Intelligence (ODNI).

III. Working Group Updates

A) The PCLWG Report

Colleen Crowley, OPM, (see presentation at Attachment 2) indicated a continued overall downward trend for both investigations and adjudications timeliness and a slight increase in the timeliness for periodic reinvestigations (PRs) with the average for the fastest 90% of Top Secret investigations continuing to average about 80 days. She noted that initial Top Secret and Secret investigations averaged about 40 and 31 days respectively. Finally, she described Top Secret PRs adjudication times as up slightly, due to significant increases in the number of requests. The Chair asked if there were specific factors causing the PRs to trend upwards and she stated that this factor was affected by increased senior leadership emphasis on identifying and fast tracking those people identified as due for a PR.

Laura Hickman, DISCO reported (see presentation at Attachment 3) that the case inventory of initial investigations that were pending adjudication showed a downward trend through the 2nd quarter of FY2012. She advised that DISCO's full case inventory contained approximately 4,000 suspended cases, including initial investigations and PRs, and a category called "other suspended inventory." She explained that "other suspended inventory" includes any adjudication action requiring additional commitment of resources and tracking. She described such cases as "reopens to OPM," where a completed investigation was received, but requires additional information before an adjudication can be completed. These cases are then suspended, and "reopened" back to OPM as part of the original investigation. She explained the other type of case as a "reimbursable suitability investigation" (RSI) which differs in that DISCO pays for any additional investigative work. Mr. Pannoni asked if OPM and DISCO could come to an understanding of exactly what information is required in order to reduce the need for reopens and RSIs. Ms. Hickman explained that an anomaly requiring an RSI often results from an unusual incident, such as an incident report, or from an event occurring since the original investigation, while a "reopen" may occur for a myriad of reasons, such as an inability to interview the subject while deployed overseas. She agreed that there may be some incidences wherein the process could be streamlined. Stan Sims, DSS, added that the best hope was for reducing the time requirements in the "reopen" process, but that the RSI process would be less likely to yield significant reductions, because many of the items DISCO determined to require additional inquiry simply did not surface during the initial investigation, and now require additional information. Mr. Pannoni acknowledged that there will always be some cases that require additional investigation, especially in the case of counterintelligence concerns, but suggested that OPM and DISCO could find proactive ways of improving initial investigative coverage to preclude the need for the additional investigative effort. The Chair suggested that the working group focus on the status of these factors, so that it can better assess the process and reduce the overall timelines. Ms. Crowley asserted that OPM's goal is to eliminate the need for "reopens," and to deliver a product that meets the adjudicative agency's needs in the first instance. She noted that OPM is working to provide more structure to the investigative output, so that it's very clear what information needs to be provided to the adjudicator and that these changes in formatting will promote more product visibility, provide for continued improvements, and ultimately reach our goal of zero "reopens." She added that these changes will be piloted in August 2012, and that OPM will report their progress made at a future NISPPAC meeting.

Ms. Hickman then discussed the number of open investigations, noting that there has been a significant increase in PRs in FY2012. While describing the lower reject rates for the Electronic Questionnaires for Investigations Processing (e-QIP) as good news, in that both OPM and DISCO processes have achieved results far below required limits, she attributed much of this success to the new version of the Standard Form (SF) 86, with the "branching questions" that provide more flexibility and improve validations, and that result in an investigation that is more complete and accurate. Next, she explained that DISCO rejections, tracked by facility category, are lower for companies that have centralized processes, and that the most frequent reason for rejections continues to be missing employment information. She noted that the number one reason for rejections by OPM continues to be failure to submit fingerprint cards within the required 14-day period, and inferred that companies that have deployed electronic fingerprint devices play a major role in the reduction of the submission time rates.

Chuck Tench, DSS, reported on the status of the employment of the electronic fingerprinting process. He noted that all Central Adjudication Facilities (CAFs) were beginning to use electronic submission formats. He reminded the Committee of the DoD memo that requires conversion to electronic fingerprinting by December 2013, and that the Secure Web Fingerprint Transmission (SWFT) application process, which is provided through the Defense Manpower Data Center (DMDC), was set up to meet that requirement. He noted that the National Classification Management Society (NCMS) is conducting a survey to capture industry's needs in this area, and that DISCO conducts monthly webinars to assist industry with questions on the SWFT implementation process. Furthermore, he mentioned new options on the DSS website (http://www.dss.mil/documents/disco/electronic-fingerprint-capture.pdf) that provide guidance on self-help electronic fingerprint capture, complete with procedures and strategies designed to assist industry users through the process. While echoing the good news presented by OPM and DISCO regarding the use of the electronic fingerprinting, he pointed out that thus far only 12% of FY2012 submissions to OPM were via SWFT and cautioned that there is a lot of work to be done if the requirement is to be met by the end of 2013. He noted that DMDC is currently completing the equipment registration process in an average of 48 days. Mr. Pannoni noted that while a 48-day turnaround is impressive, that everyone must understand that there is still a two month preparation time, to which Mr. Tench concurred and observed that a lot of time is being lost waiting for industry action and communication back to DMDC. Mr. Sims urged that everyone take the December 2013 implementation date seriously, and begin the process soon so as to avoid creating an inoperable bottleneck. He reiterated that DMDC is ready to meet the needs of its customers, but if too many companies put off this requirement until the deadline then they will be unable to service everyone's needs. Mr. Tench then explained the enhancements being made to SWFT, such as providing a rapid notification of receipt, decreasing response time, making modifications that permit support of multiple case codes, authorizing bulk fingerprint loads, and adapting the system to accept Smartcard login. In addition, he noted that they are leveraging the use of the existing Public Key Infrastructure (PKI) structure for JPAS access, which will include enhancements such as additional call center hours, an on-line registration process, and an e-mail inquiry service (swft@osd.pentagon.mil).

Charles Sowell, ODNI, provided an update (see presentation at Attachment 4) of the industry performance metrics for the intelligence community (IC). He thanked industry for the continued strong relationship between themselves and the IC community, and summarized recent meetings as frank and open discussions to identify potential solutions for ongoing clearance challenges such as timeliness, mobility, and reciprocity issues. He noted that 94% of all IC security clearance cases for contractors continue to be handled through OPM and represented 5.5% of the US Government workload. Further, combined Top Secret and Secret PRs increased only in initiations, while both investigation and adjudication timeliness decreased over the previous year. He explained that less than 1% of the total number of Top Secret and Secret initial case workload is from the other delegated agencies inside the IC, and that they reported slight increases in initiations and slight decreases in both investigations and adjudications. He noted that there were dramatic decreases in initiations and investigations timeliness, and slight increases in adjudication timeliness for combined Top Secret and Secret PRs. He reminded the members that un-submitted PRs are creating reciprocity problems for both government and industry and that, with the likelihood of smaller budgets, this trend is apt to continue, and that security issues have been superseded by suitability issues. The Chair asked if there had been any effort to collect data on un-submitted PRs and Mr. Sowell explained that there has been some initial analysis of this anomaly using Scattered Castles, while simultaneously working with DMDC to match similar data through JPAS. He noted that the community is concerned with the scope of the problem in light of the recent policy changes that have occurred or that are poised to take place. He cited the recent Code of Federal Regulations (CFR) 731 requirement for a five-year reinvestigation standard for suitability, and Secret level clearances, as well as new Homeland Security Presidential Directive (HSDP)-12 requirements as examples. He added that ODNI has commissioned a study to capture the magnitude of this complex problem, and in time to find practical solutions. The Chair noted that these facts, especially when coupled with the Intelligence Reform and Terrorism Prevention Act's (IRTPA) reporting requirements for security clearances, make it even more important that the working group and the Committee keep this dialogue open. Mr. Sowell concurred, and informed the Chair that a new security clearance process report had been recently released, and offered to brief the results of that report at the next NISPPAC meeting. He noted that the methodology used to describe the overall number of clearance determinations changed in this year's report and now includes eligibility determinations. Mr. Pannoni asked if there is value in measuring the crossover issues affecting reciprocity and suitability between collateral and SCI clearances, as well as the timeliness of the process. Mr. Sowell responded that the capability to track reciprocity issues was now being built into Scattered Castles, because the IC agrees that while it is indeed critical that we measure reciprocity actions, we are not presently capable of determining clearance frequency. The Chair then asked the working group to find an effective means to report this anomaly at the next NISPPAC meeting.

Mark Pekrul, DOE, presented an overview of his agencies security clearance activity (see presentation at Attachment 5). He noted that their security clearance investigations are conducted by OPM and then DOE adjudicates clearances through eight nation-wide facilities that make no distinction between industry and federal employee cases. He stated that DOE Headquarters handles all Administrative Reviews (denial or revocation actions) and appeal functions. He reminded the members that a "Q" clearance is DOE's equivalent of Top Secret/National Security Information (NSI), and an "L" clearance is the equivalent of Secret/NSI. He presented metrics showing the number of cleared contractor access authorizations for both "Q" clearances and "L" clearances. He noted that DOE does not track contractor and federal employee clearances separately, but rather as one homogeneous group, and that all IRTPA timeliness goals have been met since 2009. Finally, as of April 2012, he noted that there are approximately 1,300 pending investigations across all DOE sites, the bulk of which are managed at Headquarters and the National Nuclear Security Administration.

In response to the first of two questions, Mr. Pekrul noted that there were both contractor and federal employees performing adjudicative analyses, but that final review and approval was only the purview of a federal official. In response to a second question, he stated that polygraph exams were conducted by DOE's Office of Intelligence and Counterintelligence, and while he was unfamiliar with their reciprocity policies he knew they used the federal polygraph standards and would provide them at the next NISPPAC meeting. The Chair agreed that this would be valuable information, as it would help us to establish a common understanding of polygraph requirements. The Chair then thanked the PCLWG for its comprehensive reports.

B) The CAWG Report (See presentation at Attachment 6)

Randy Riley, DSS, noted that the CAWG, in an effort to enhance granularity, has evolved its data collection process in terms of both content and presentation, with a focus on the system security plan (SSP) review process, the on-site system validation process, and the capture of process vulnerabilities and deficiencies. He reminded the members that DSS is responsible for approving cleared contractor information systems that process classified data, and works with industry to ensure that system security controls that limit the risks of compromising NSI are in place. He noted that the timeliness of SSP reviews has not changed significantly over the last 12 months, remaining consistent at around 5,000 plans that were accepted and reviewed. With regard to tracking plan deficiencies, he noted that with only a few exceptions the bulk continues to come from the smaller companies. He explained that any deficiencies documented during these reviews are provided to the Information System Security Manager (ISSM) for action, as well as in the roll-up reports available to multi-site ISSMs upon request.

Mr. Riley noted that during the period of April 2011 through May 2012, there were 1,460 SSPs identified as requiring correction prior to their on-site validation visit, and that these constituted the primary desktop review of problem areas. He stated that 870 SSPs were granted an Interim Authority to Operate (IATO) with corrections required, and stressed that improvements are needed in this area. Finally, he cited 537 SSPs that were denied an IATO because they contained too many significant deficiencies, and stressed that this area needs aggressive attention. Also, 216 SSPs were rejected (not submitted in accordance with requirements, not entered into the Office of the Designated Approving Authority process, and returned to the ISSM with accompanying submission guidance) during the period.

Mr. Riley provided data detailing the 10 most common SSP deficiencies and noted that while we have reviewed this process at past meetings, these new metrics reflect some notable improvements, especially in the area of integrity and availability, where this deficiency slipped from number four to number five. He reminded the Committee that it is in these kinds of metrics where the working group is modifying its tracking procedures, and that over the next few reports we should be able to better illustrate the results in their magnitude and description. In reply to a question concerning the affect of Microsoft Windows 7 upgrades on reporting, he explained that this process would be seamless, as there is no requirement to separate this data from other system data. In response to a question regarding the tracking of deficiencies, he explained that this reporting procedure includes all errors cited during desktop reviews which reveal a deficiency, including minor corrections cited during an IATO issuance, as well as those that resulted in immediate rejections. Mr. Pannoni inquired if the integrity and availability deficiency that was reported as slipping from the fourth to fifth position might, by now, actually be zero, or very close to zero. Mr. Riley explained that they modified the SSP template last year to default the integrity and availability element as "not required by contract," which should have eliminated the condition altogether, but that some ISSMs have been changing the "default" back to making it a condition. He cited a failure of some to understand the item's meaning as the need for enhanced education on the issue and noted that one possible fix being considered is to inject pop-up help tips which would provide detailed instructions in some of the more obscure areas. Finally, he explained that occasionally a second IATO must be issued, generally because some administrative anomaly exists, and that they allow for continued system operation until the specific anomalies are resolved. He noted that while these anomalies vary in both reason and complexity, they do continue to decrease in numbers.

Mr. Riley then described the system validation process as the actual hands-on examination of the system for final accreditation, and noted a 32% increase in the number of systems that go Straight to ATO (SATO) over the past year. In addition, the CAWG will also be studying the IATO process in search of more efficient methods of identifying specific conditions under which we can selectively issue an IATO.

Mr. Riley then discussed validation results (determining if all systems are properly configured) and the actual number of vulnerabilities against the total number of systems ("average vulnerability per on-site"), which have remained steady over the past 12 months. Mr. Pannoni observed that even though there are a number of changes in the vulnerability categories, we continue to see that "inadequate auditing controls" and "security relevant objects not protected" remain the driving factors accounting for almost 50% of all discrepancies.

Mr. Riley summarized that while the SSPs were generally being processed and reviewed in a timely manner, we need to focus on reducing deficiencies and system vulnerabilities, and that the most troublesome factor is the 2% of the systems denied an ATO. He reminded the members that the most common SSP deficiencies are missing attachments, documentation errors, and integrity and availability requirements, and that while on-site validations are being completed in a timely manner, we need to continue to focus on reducing the most common system vulnerabilities identified during validation, which include auditing controls, configuration management, and failure to protect security relevant objects. Finally, he stated that above all we will continue to focus on the SATO process, as that reduces risk and increases efficiency. The Chair thanked the CAWG for their work, and called for Scott Conway, industry, for the combined industry presentation.

III. New Business

A) The Combined Industry Presentation (see presentation at Attachment 7)

Mr. Conway, Industry Spokesperson, noted that this would be the final meeting for both himself and Marshall Sanders, as industry representatives on the NISPPAC, and announced that Fred Riccardi had been selected as the new Industry Spokesperson. He mentioned that the nomination process had begun and that the two new members should be present at the November meeting. He then introduced the new representatives of the Memorandum of Understanding (MOU) organizations. He expressed industry's concern that another partial government shutdown could adversely impact the continued funding of necessary personnel security clearances. Mr. Sims responded that senior DoD leadership is highly motivated to protect the integrity of that program.

Mr. Conway then recapped issues raised in industry's most recent stakeholders' meeting, notably those concerning future E-QIP and JPAS changes, including the possibility of a return of a JPAS quick-change confrontation board. He noted that the PCLWG meeting held during the recent NCMS Seminar was very helpful to industry, and proposed that a member of the NCMS JPAS team be added to that group so that industry could address JPAS issues as they arise.

Mr. Conway expressed industry's concern over access issues with the U.S. Navy's RAPIDGate system, which provides credential-holders access into DoD, Department of Homeland Security and National Aeronautics and Space Administration facilities. Windy Kay, Navy, offered assistance and Mr. Pannoni offered NISPPAC resources to distribute information to industry. Mr. Conway noted that industry rendered comments on proposed National Industrial Security Program Operating Manual (NISPOM) changes and plans to attend a meeting later in July to review proposed text and format changes, and that industry was concerned about the multiple reporting of suspicious contacts, and asked if there is a single point of contact for reporting such issues. Mr. Sims promised that DSS would review this issue, but with numerous agencies receiving these reports, the best to hope for will be a reduction in the duplication of efforts.

Mr. Conway reiterated industry's concern over numerous issues related to Special Access Programs (SAPs) and requested continuation of the SAP Working Group (SAPWG) to help resolve ongoing issues. Mr. Pannoni reminded the Committee that there would be another meeting of the government portion of the SAPWG in late July, and then a joint government/ industry meeting before the next NISPPAC meeting. Mr. Conway also noted that industry anticipates continued discussions on issues related to Executive Order (E.O.) 13587, *"Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*," as well as E.O. 13556, "*Controlled Unclassified Information (CUI)."*

At the conclusion of his remarks, Mr Fitzpatrick recognized both Mr. Conway and Mr. Sanders for their service to the NISPPAC and presented them each a book on the history of the National Archives.

B) The DSS Director's Update

Mr. Sims noted that DSS normally hosts a government stakeholders' meeting and an industry stakeholders' forum prior to each NISPPAC meeting and will continue to invite the Director of ISOO and the NISPPAC Designated Federal Official as observers to these meetings. He noted that in these meetings ongoing policy issues and concerns are examined. One such topic was CUI and the ambiguities within the cyber domain inherent in protecting intellectual property and other sensitive but unclassified information. He noted that DSS is already assisting industry in development of positive measures to protect their networks even as such policy is being developed. He then provided an update of activities impacting both the government and industry, the first being the consolidation of the DoD central adjudication facilities (CAF) currently scheduled for completion by October 1, 2012. He reiterated his desire to make this transition as transparent as possible and envisioned no change in DSS's role as the DoD agency responsible for industrial security clearances. The second initiative is automation of the Department of Defense (DD) Form 254, "Department of Defense Contract Security Classification Specification." He noted that DSS has partnered with the Department of the Army to rework this process and develop a form that will reduce the inherent vulnerabilities in the current procedures.

C) The DoD Update

Stephen Lewis, OUSD(I), noted two NISPOM changes. The first being a conforming change, or an interim issuance regarding industrial implementation of E.O. 13526. Among these were markings, and training for derivative classifiers. The second involved a change in the NISPOM, Chapter 10, "International Security Requirements," and specifically the implementation of the Defense Trade Cooperation Treaty between the United States and the United Kingdom. He noted that once Chapter 10 of the NISPOM is completed that the final draft document would be forwarded for coordination to the NISPPAC, its working groups, and other NISP stakeholders. He explained that following a return to DoD for the formal coordination process, that it would undergo coordination with the NISP Cognizant Security Agencies (CSA), and then the required *Federal Register* process. He also noted that DoD and DMDC are discussing changes in light of the recent Defense Enrollment Eligibility Reporting System overwrite of JPAS data, JPAS governance issues, and possible ways in which to enhance communications as they transition JPAS to the Defense Information System for Security.

Mr. Pannoni reminded the members of the October 1, 2012, date for the abolition of non-Government Services Administration (GSA)-approved security containers for storage of classified information. He asked if DSS had conducted a final review since at last report there were approximately 2,000 non-GSA-approved containers in use by industry. Kathy Branch, DSS, responded that there is a survey currently in progress to determine the number and location of any non-GSA-approved storage containers, and that its results would be presented at the next NISPPAC meeting. Mr. Lewis noted that an Industrial Security Letter (ISL) was forthcoming that expands open storage options, and may mitigate the need to purchase new GSA-approved containers. The Chair suggested that since there have been previous requirements for interim reports, that we should get ahead of possible high-level, or congressional status requests, and that we use DSS's forthcoming status report as a basis for responding to any such request.

Kimberly Baugher, Department of State (STATE), noted that DoD has not yet adopted the new U.S. Federal Bridge Certification Authority requirements, and that this has caused difficulty for STATE employees attempting to access JPAS. She asked if DoD would extend the timeframe for making this change. Mr. Lewis responded that there is no longer a user ID and/or password requirement, and therefore DoD will take that function off-line. Additionally, she noted that STATE had received changes in the National Interest Determination(s) process from ODNI and suggested that they had exceeded the parameters of national policy and DoD agreed to investigate the issue and report results at a future NISPPAC meeting.

D) DoD's Defense Industrial Data (DIB) and Cyber Security and Information Assurance (CS/IA) Program (see presentation at Attachment 8).

The chair then introduced Ms. Vicki Michetti, Deputy Director, DIB CS/IA who introduced the DIB CS/IA program as well as the background and circumstances that prompted its initiation. Citing a climate of excessive incidences of exploited, lost, or otherwise compromised DoD weaponry and program technology, the Deputy Secretary of Defense created the CS/IA program in 2007 to mitigate these unacceptable circumstances. She explained that the program operates under the authority of the DoD's Chief Information Officer (CIO), and derives its responsibilities from United States Code, Title 44 and the Federal Information Security Management Act. She noted that they have teamed with complementary programs, agencies, and industry to build the program, and that in today's complex environment the program continues to work hand-in-hand with other agency resources, especially DSS and the Defense Information Systems Agency's IA vendor program.

Ms. Michetti stated that the program includes four interrelated activities. The first is a signed framework agreement, between the DoD CIO and an individual defense industrial-base company's CIO that codifies the roles, responsibilities, and the other actions required to implement the program and support the voluntary information sharing activities on which it rests. The second is the actual information sharing piece, wherein DoD provides both unclassified and classified cyber security and information assurance expertise. She described the unclassified expertise as information that companies can use to help protect their own networks, and the classified expertise as providing sophisticated information about present and evolving threat activity. The third activity involves industry's reporting of cyber-threat incidences that are shared network-wide on the presumption that actual threats faced by one company are likely to be shared by others. The fourth activity is the damage assessment process. That is, whenever an incident occurs and there is reasonable evidence of loss or compromise of DoD unclassified weaponry or valuable technological information we assess the nature, amount, and degree of damage, and whether there are suitable mitigating or alternative actions that should be taken to resolve the threat.

She then explained that in 2010 the program extended its reach to further enhance the DIB information-sharing program by including a small number of internet service providers, who in turn could utilize classified information to act on behalf of companies participating in the program. She further explained that the program has evolved to where all these activities have been codified into an interim final rule. She noted that this action represented a significant milestone, allowing movement from a small, pilot program, to one available to all cleared contractors who wish to participate. In addition, she noted that with active support from the current administration, DoD has been able to raise the security bar and measurably improve incidence response quality and timeliness in moving from reactive to proactive cyber security and information assurance. She cautioned that the CS/IA program has not reached its full potential, and that there are already plans for future expansion. She noted that since this program is voluntary, each company must make individual decisions regarding program participation and the resources it is willing to commit. However, she stated that they are now able to demonstrate success and ever-increasing interagency interest. She cited DHS for building the capability to extend their model across other critical information infrastructure sectors. She then directed the Committee's attention to a hyperlink for the Interim Final Rule. In response to a question from Mr. Sanders, Ms. Michetti noted that the only information they share with the acquisition process is the damage assessment report, and that it is shared only as a tool for possible use in mitigating adversarial actions. The Chair thanked Ms. Michetti for her presentation.

IV. Closing Remarks and Adjournment

The Chair reminded those assembled that the meeting was opened to the public, and asked if any guests and/or other members wanted to provide additional comments/questions or concerns. Recognizing none, he reminded the Committee that the next two NISPPAC meetings are scheduled for November 14, 2012, and March 20, 2013, respectfully, with the working groups typically meeting roughly six to eight weeks prior. In addition, he noted that any member or guest could get clarification of any NISPPAC business by reaching out to Mr. Pannoni, and David Best, ISOO, or through their Agency's ISOO liaison. The meeting adjourned at 11:58 am.

Refer to Attachment 9 for the action items from this meeting.

Attachment #1- NISPPAC Attendees

Attachment 1
NISPPAC MEETING ATTENDEES

The following individuals were present at the July 11, 2012, NISPPAC meeting:

John Fitzpatrick,	Information Security Oversight Office	Chairman
Greg Pannoni,	Information Security Oversight Office	Designated Federal Officer
Eric Dorsey	Department of Commerce	Member
Timothy Davis	Department of Defense	Member
Richard Hohman	Office of the Director of National Intelligence	Member
Richard Donovan	Department of Energy	Member
Drew Winneberger	Defense Security Service	Member
Kimberly Baugher	Department of State	Member
Steven Long	Department of the Navy	Member
Patricia Stokes	Department of the Army	Member
Dennis Hanratty	National Security Agency	Member
Scott Conway	Industry	Member
Shawn Daley	Industry	Member
Richard Graham	Industry	Member
Frederick Riccardi	Industry	Member
Michael Witt	Industry	Member
Ros Baybutt	industry	Member
Steven Kipp	Industry	Member
Marshall Sanders	Industry/ MOU Representative	Member
Christal Fulton	Department of Homeland Security	Alternate
Jeffrey Moon	National Security Agency	Alternate
Booker Bland	Department of the Army	Alternate
Stephen Lewis	Department of Defense,	Alternate
Kathleen Branch	Defense Security Service	Alternate
George Ladner	Central Intelligence Agency	Alternate
James Hallo	MOU Representative	Attendee
Mark Rush	MOU Representative	Attendee
Mitch Lawrence	MOU Representative	Attendee
Colleen Crowley	Office of Personnel Management	Presenter
Stan Sims	Defense Security Service	Presenter
Laura Hickman	Defense Security Service	Presenter
Charles Tench	Defense Security Service	Presenter
Randy Riley	Defense Security Service	Presenter
Mark Pekrul	Department of Energy	Presenter
Charles Sowell	Office of the Director of National Intelligence	Presenter
Vicki Michetti	Department of Defense	Presenter
Kishla Braxton	Department of Commerce	Attendee
Lisa Gearhart	Department of Defense	Attendee
Michael Bodin	Department of Energy	Attendee
Larry Small	Department of Energy	Attendee
Tracy Brown	Defense Security Service	Attendee

Keith Minard	Defense Security Service	Attendee
Diane Craig	Defense Security Service	Attendee
Tracy Kindle	Defense Security Service	Attendee
Jay Buffington	Defense Security Service	Attendee
Christine Beauregard	Defense Security Service	Attendee
Windy Kay	Department of the Navy	Attendee
Valora Van Horn	Industry	Attendee
Sam Davis	Industry	Attendee
Tabetha Chandler	Industry	Attendee
Jim Ewls	Industry	Attendee
Keith Marino	Industry	Attendee
Robert Harney	Industry	Attendee
Gregory Thompson	Industry	Attendee
David Best	Information Security Oversight Office	Staff
Robert Tringali	Information Security Oversight Office	Staff

The following members/alternates were not present at the July 11, 2012, NISPPAC meeting:

Deborah Scholz	Department of the Air Force	Member
Darlene Fenton	Nuclear Regulatory Commission	Member
Anna Harrison	Department of Justice	Member
Kathy Healey	National Aeronautics & Space Administration	Alternate

Attachment 2- OPM PCL Presentation

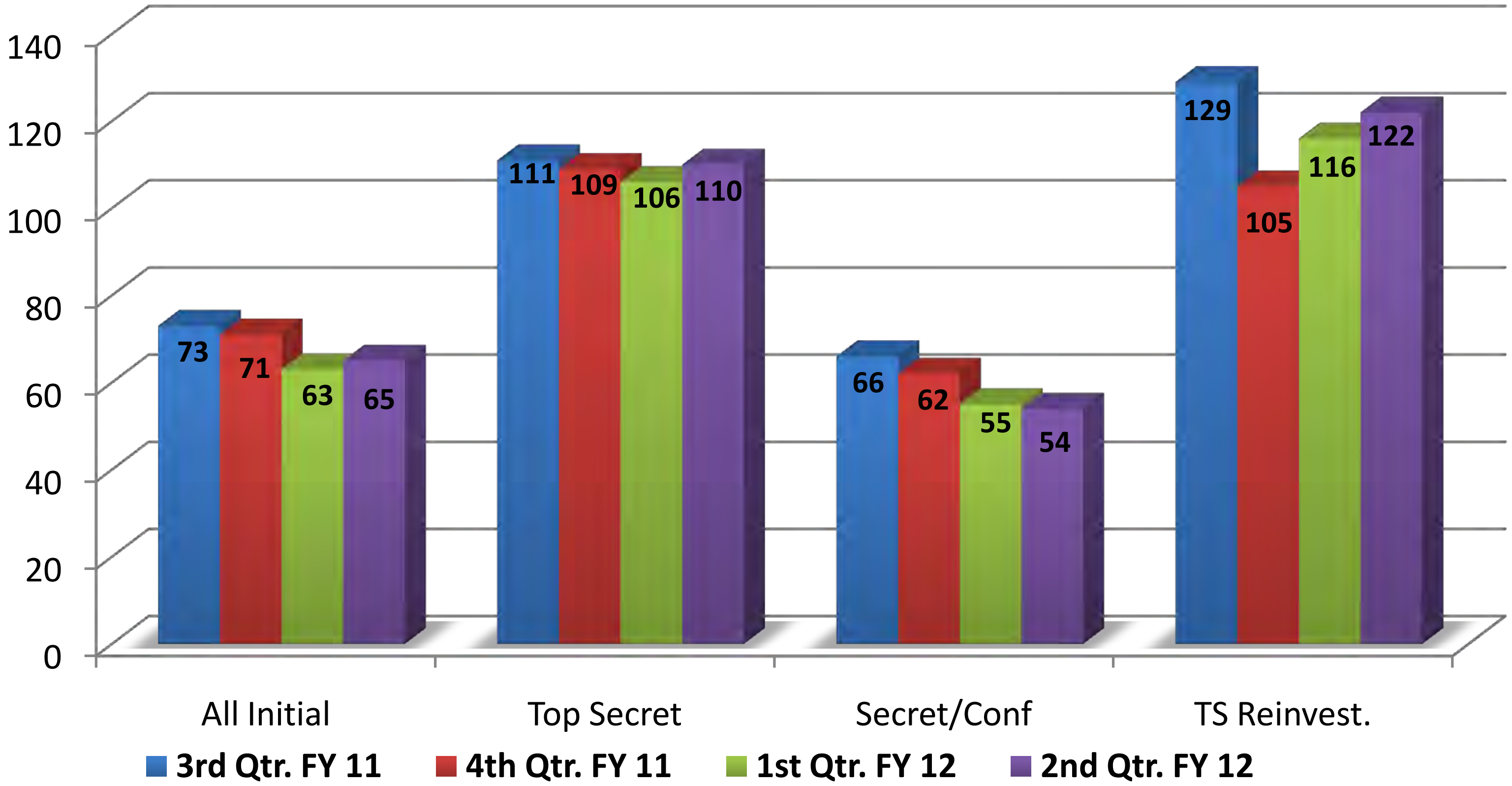
a New Day for Federal Service

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

Highlights

- End to End timeliness for 90% Secret/Confidential continuing downward trend
- Continuing downward trend in adjudication times this fiscal year for 90% Initial TS and ALL Secret/Confidential Clearances
- Uptick in investigation times for TS Reinvestigations - increased number of requests

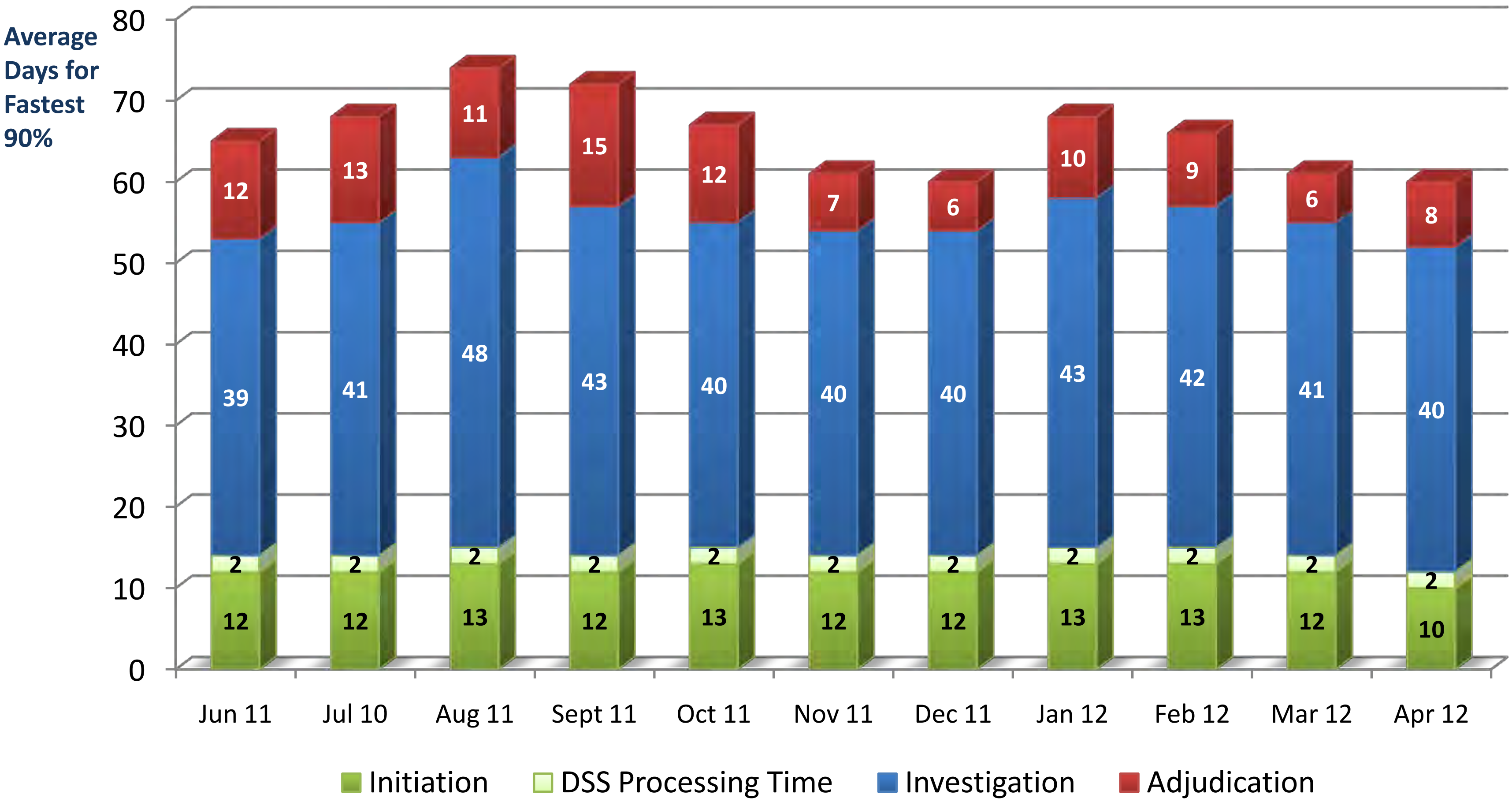
Average Days of Fastest 90% of Reported Clearance Decisions Made*



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 3rd Q FY11	35,989	5,755	30,234	12,071
Adjudication actions taken – 4th Q FY11	24,212	4,887	19,325	6,164
Adjudication actions taken – 1st Q FY12	32,020	5,383	26,637	8,279
Adjudication actions taken – 2nd Q FY12	30,985	5,975	25,010	11,487

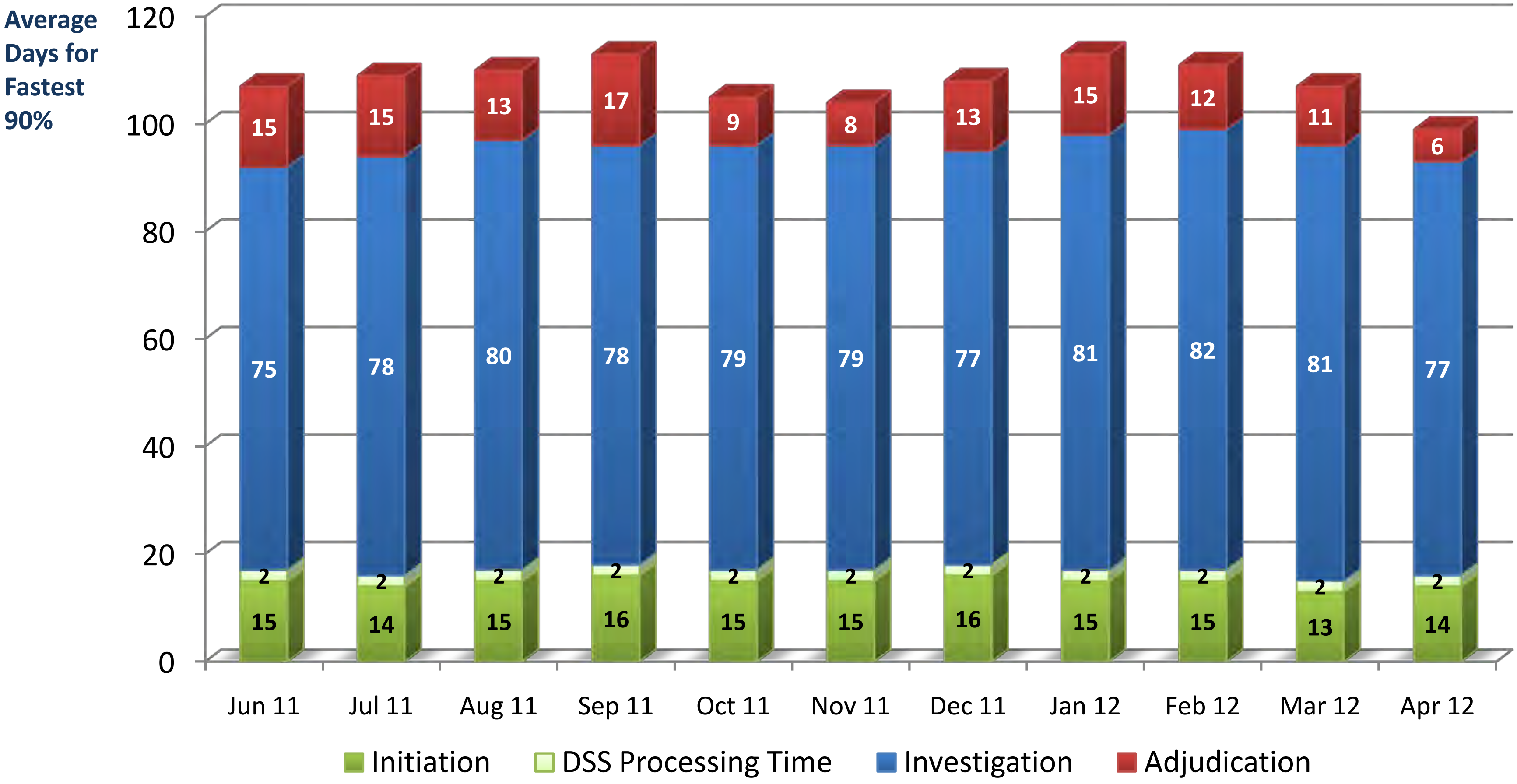
*The adjudication timelines include collateral adjudication by DISCO and SCI adjudication by other DoD adjudication facilities

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



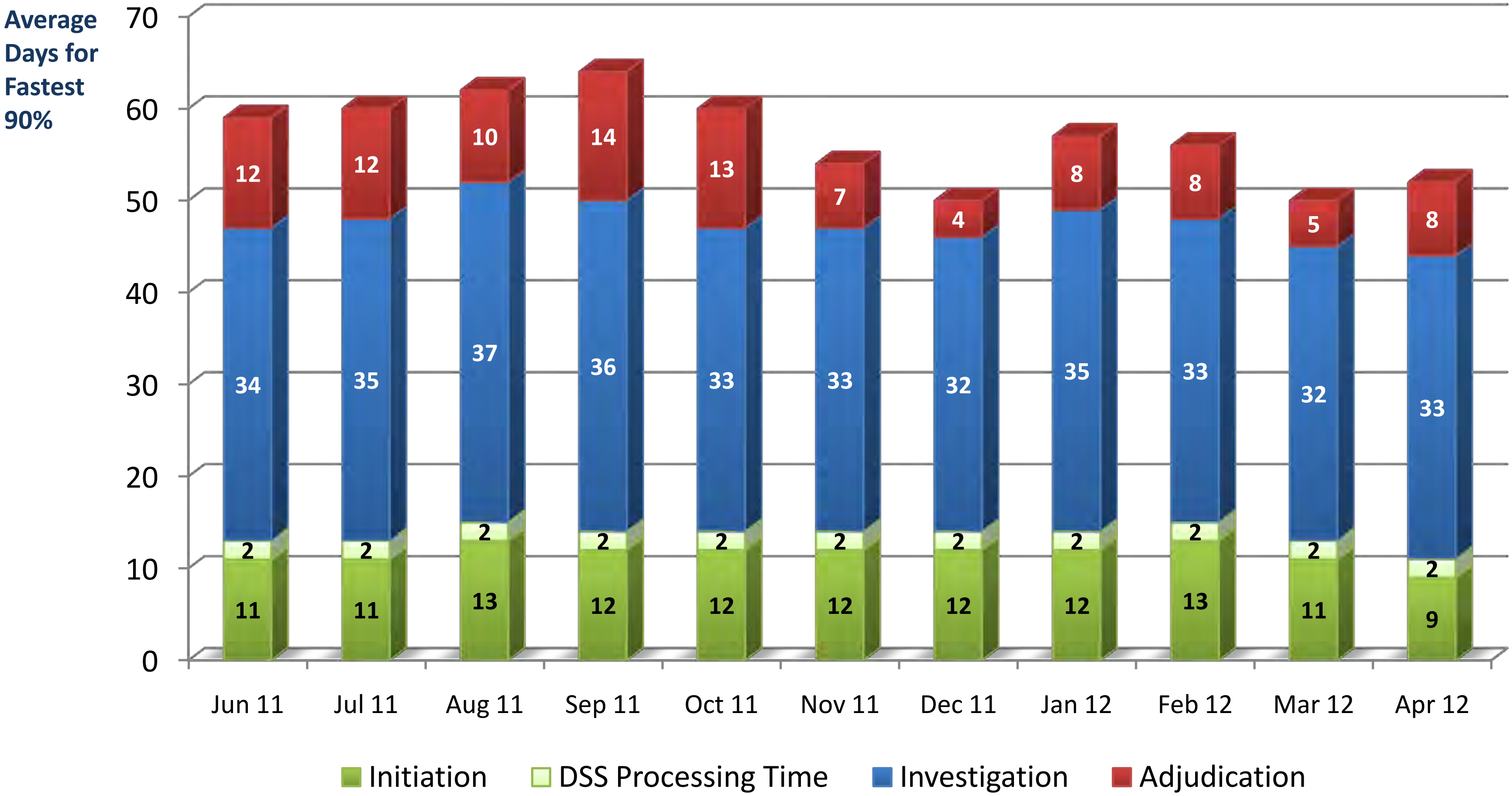
	Jun 11	Jul 11	Aug 11	Sept 11	Oct 11	Nov 11	Dec 11	Jan 12	Feb 12	Mar 12	Apr 12
100% of Reported Adjudications	12,358	8,917	8,952	5,116	12,158	9,776	10,106	10,768	8,940	10,769	8,755
Average Days for fastest 90%	65 days	68 days	74 days	72 days	67 days	61 days	60 days	68 days	66 days	61 days	60 days

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



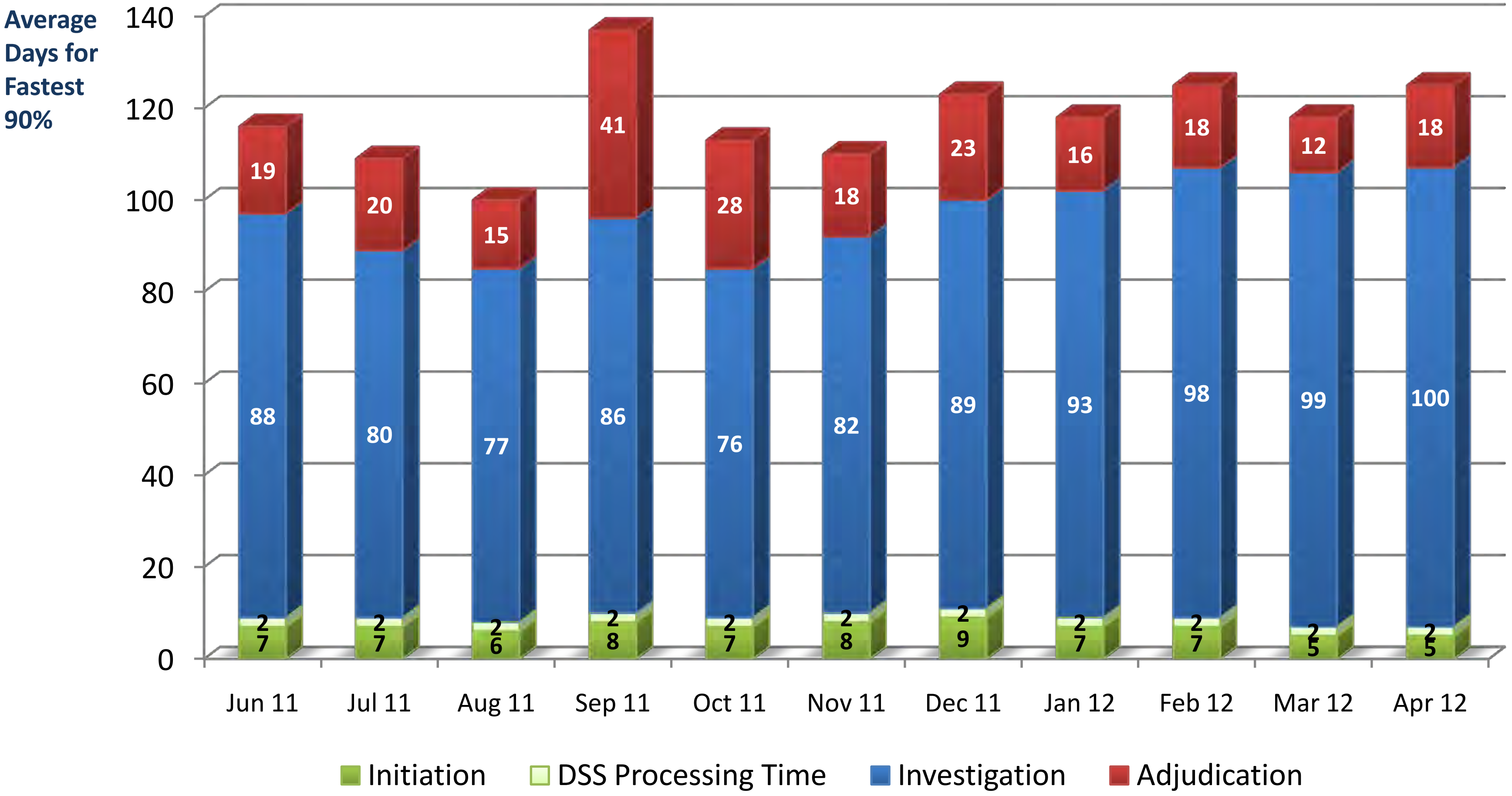
	Jun 11	Jul 11	Aug 11	Sept 11	Oct 11	Nov 11	Dec 11	Jan 12	Feb 12	Mar 12	Apr 12
100% of Reported Adjudications	1,743	1,511	2,166	898	2,035	1,514	1,837	2,077	1,688	2,099	1,519
Average Days for fastest 90%	107 days	109 days	110 days	113 days	105 days	104 days	108 days	113 days	111 days	107 days	99 days

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



	Jun 11	Jul 11	Aug 11	Sept 11	Oct 11	Nov 11	Dec 11	Jan 12	Feb 12	Mar 12	Apr 12
100% of Reported Adjudications	10,615	7,406	6,786	4,218	10,123	8,262	8,269	8,691	7,252	8,670	7,236
Average Days for fastest 90%	59 days	60 days	62 days	64 days	60 days	54 days	50 days	57 days	56 days	50 days	52 days

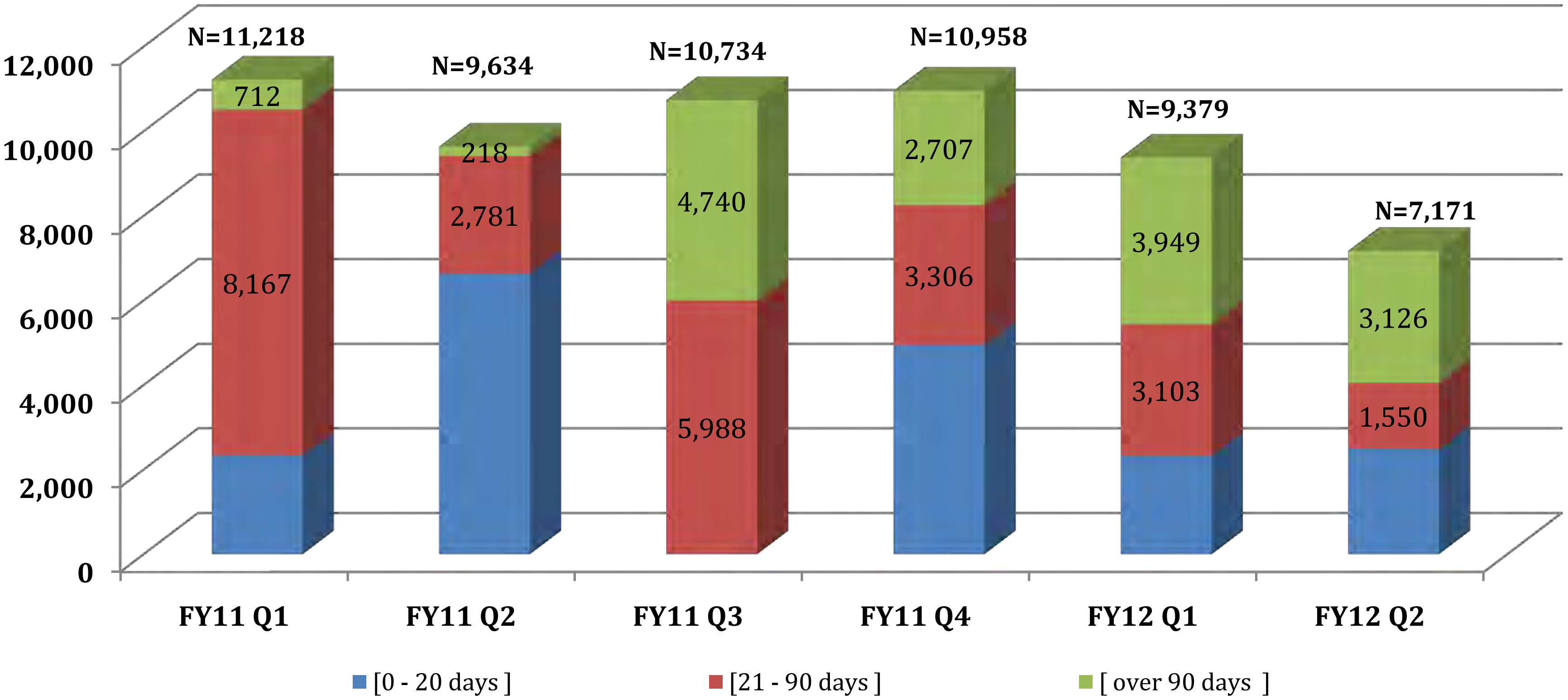
Industry's Average Timeliness Trends for 90%
Top Secret Reinvestigation Security Clearance Decisions



	Jun 11	Jul 11	Aug 11	Sept 11	Oct 11	Nov 11	Dec 11	Jan 12	Feb 12	Mar 12	Apr 12
100% of Reported Adjudications	5,585	1,841	3,051	921	3,278	2,046	2,958	4,276	2,726	4,087	2,813
Average Days for fastest 90%	116 days	109 days	100 days	137 days	113 days	110 days	123 days	118 days	125 days	118 days	125 days

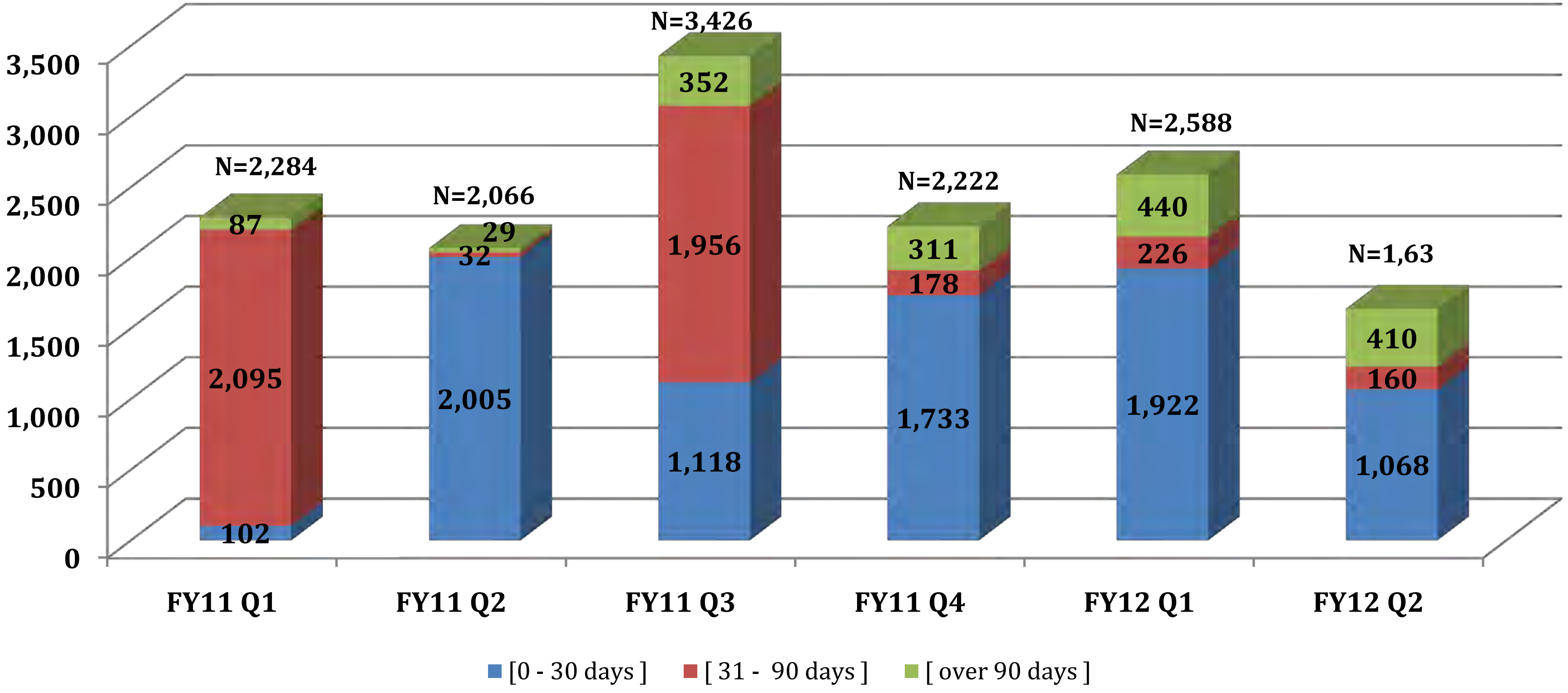
Attachment #3- DISCO PCL Presentation

Defense Industrial Security Clearance Office (DISCO)
FY11-FY12 Initial Pending Adjudications
SSBI / NACLC



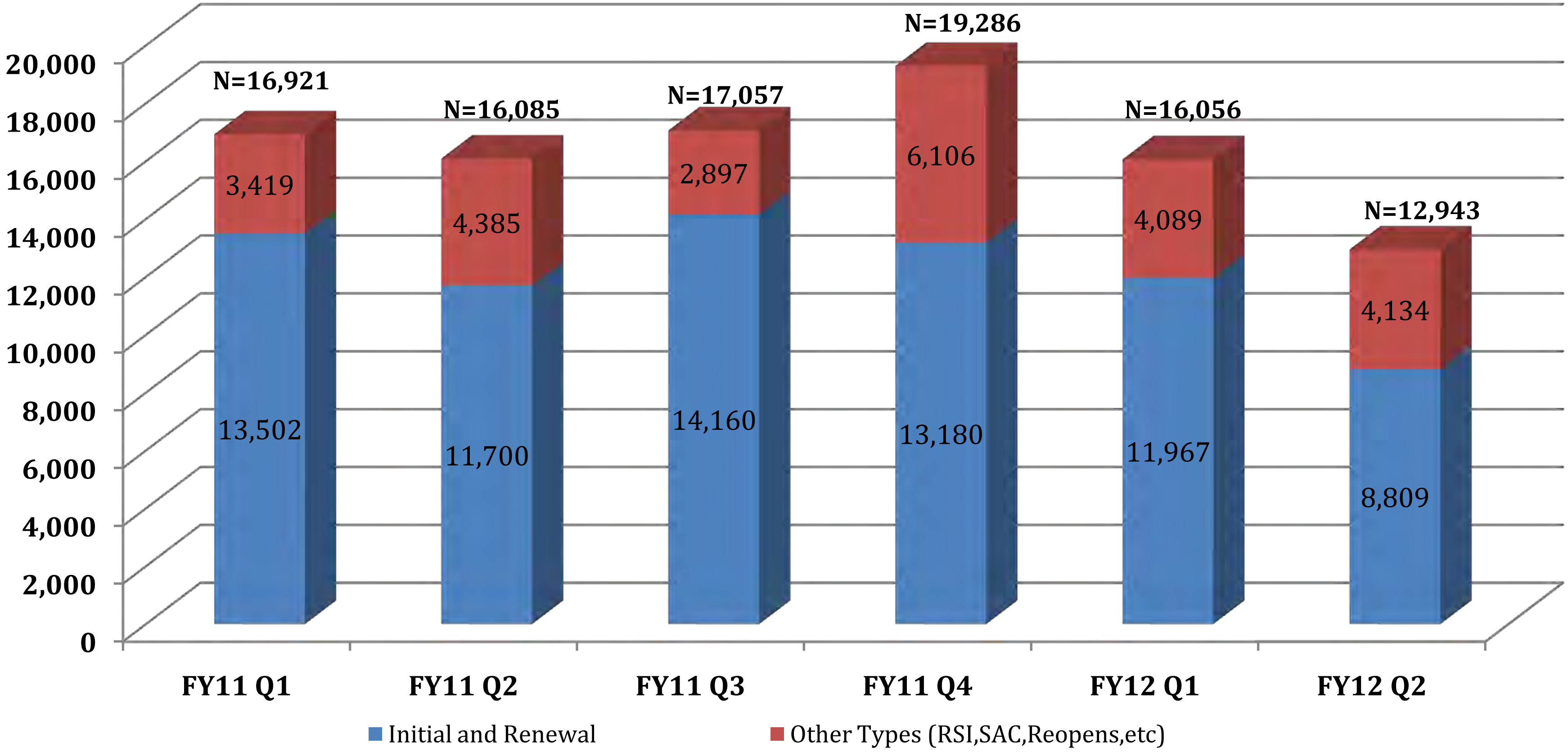
Case Type	Day Category	FY11 Q1	FY11 Q2	FY11 Q3	FY11 Q4	FY12 Q1	FY12 Q2
Initial (SSBI and NACLC)	[0 - 20 days]	2,339	6,635	6	4,945	2,327	2,495
	[21 - 90 days]	8,167	2,781	5,988	3,306	3,103	1,550
	[over 90 days]	712	218	4,740	2,707	3,949	3,126
Initial Total		**11,218**	**9,634**	**10,734**	**10,958**	**9,379**	**7,171**

Defense Industrial Security Clearance Office (DISCO)
FY11-FY12 Renewal Pending Adjudications
SBPR / PPR



Case Type	Day Category	FY11 Q1	FY11 Q2	FY11 Q3	FY11 Q4	FY12 Q1	FY12 Q2
Renewal (SBPR and PPR)	[0 - 30 days]	102	2,005	1,118	1,733	1,922	1,068
	[31 - 90 days]	2,095	32	1,956	178	226	160
	[over 90 days]	87	29	352	311	440	410
Renewal Total		**2,284**	**2,066**	**3,426**	**2,222**	**2,588**	**1,638**

Defense Industrial Security Clearance Office (DISCO)
FY11-FY12 Overall Pending Adjudications
SSBI / NACLC / TSPR / Other (Suspended Cases)



Case Type	FY11 Q1	FY11 Q2	FY11 Q3	FY11 Q4	FY12 Q1	FY12 Q2
Initial and Renewal	13,502	11,700	14,160	13,180	11,967	8,809
Other (RSI, SAC, Reopens, etc)	3,419	4,385	2,897	6,106	4,089	4,134
Total	**16,921**	**16,085**	**17,057**	**19,286**	**16,056**	**12,943**

Defense Industrial Security Clearance Office (DISCO)
FY12 Overall Pending Adjudications
Other Cases

Case Status	Grand Total
DISCO REO to OPM	1,079
DISCO RSI to OPM	770
With case owner	648
Pending CONUS information	384
Awaiting files	311
Pending CAF assignment	214
Awaiting files - other	179
Pending CI review	100
I/S awaiting appeal	160
Pending OPM investigation	83
Awaiting files - DSS	59
I/S awaiting CAF files	46
Pending DISCO review	21
Rotational duty	21
I/S pending RFI	18
DOHA REO/RFI to OPM	11
I/S awaiting SUSP decision from HQ	13
Awaiting citizenship verification	7
Pending clearance verification	4
Awaiting foreign passport dest	2
Incident report, pending RFI	2
STDP citizenship verification	1
Interim revisit	1
Grand Total	**4,134**

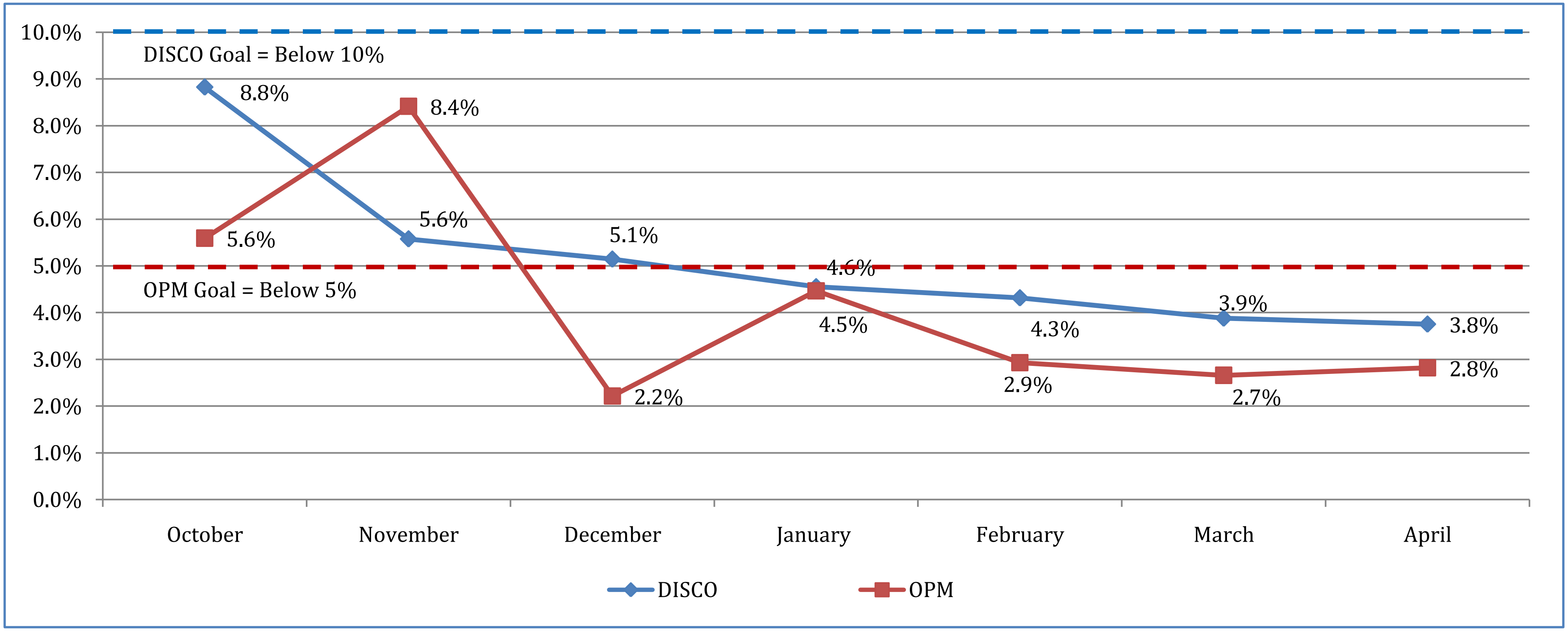
Defense Industrial Security Clearance Office (DISCO)
FY11-FY12 Industry Cases Pending at OPM

Case Type	FY10				FY11				FY12			Change Fy12Q1 vs FY12 April
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Apr-12	
NACLC	11,730	11,685	13,016	13,556	13,118	13,243	13,861	12,929	10,990	12,902	12,253	11%
SSBI	6,782	7,012	6,561	6,178	6,308	5,578	6,274	5,821	5,292	5,629	5,470	3%
SSBI-PR	4,096	4,521	4,859	5,115	5,436	7,521	4,662	4,349	4,750	5,467	6,077	28%
Phased PR	3,158	3,629	3,665	4,248	4,781	4,097	4,097	5,768	8,937	11,805	12,801	43%
Total Pending	**25,766**	**26,847**	**28,101**	**29,097**	**29,643**	**31,490**	**28,894**	**28,867**	**29,969**	**35,803**	**36,601**	**22%**

Source: OPM Customer Support Group

Takeaway: NACLC, SSBI, TSPR inventory combined increased 22% over Q1FY12.

Defense Industrial Security Clearance Office (DISCO)
FY12 DISCO and OPM Reject Rates
Initial and Periodic Reinvestigation Clearance Requests



Source: JPAS / OPM / DISCO Monthly Reports

- FY12 - DISCO Received 120,695 investigation requests as of April 30, 2012
  - Rejects – DISCO rejected 5,847 (4.8% on average) investigation requests for FSO re-submittal

- FY12 - OPM Received 112,792 investigation requests
  - Rejects – OPM rejected 4,673 (4.2% on average) investigation requests to DISCO (then FSO) for re-submittal
  - 59% of rejections - Unacceptable fingerprint cards and fingerprint cards not submitted within timeframe

Defense Industrial Security Clearance Office (DISCO)
FY12 DISCO Case Rejections by Facility Category

Month	Facility Category						
	A	AA	B	C	D	E	Others
October	1.3%	0.6%	0.8%	2.7%	6.8%	12.6%	0.1%
November	0.7%	0.3%	0.4%	1.3%	3.7%	6.8%	0.1%
December	0.8%	0.3%	0.5%	1.2%	3.6%	6.9%	0.1%
January	0.4%	0.3%	0.4%	0.8%	3.5%	6.9%	0.0%
February	0.6%	0.4%	0.4%	1.2%	3.6%	6.6%	0.0%
March	0.4%	0.5%	0.3%	1.1%	3.6%	6.5%	0.0%
April	0.5%	0.3%	0.4%	1.0%	3.2%	5.5%	0.0%
Grand Total	**4.6%**	**2.6%**	**3.2%**	**9.4%**	**28.1%**	**51.8%**	**0.3%**

Source: JPAS/e-QIP

<u>DISCO Case Rejections</u>

79.9% of cases rejected by DISCO originate from smaller Category D and E facilities

Defense Industrial Security Clearance Office (DISCO)
FY12 Reasons for Case Rejection by DISCO

TOP 10 REASONS FOR DISCO REJECTION OF INVESTIGATION REQUEST

Reason	Count	Percent
Missing employment information	1,023	39%
Missing relative information	255	10%
Missing Selective Service registration or legal exemption	225	9%
Missing financial information	215	8%
Missing cohabitant information	195	8%
Missing spouse information	156	6%
Missing education reference	143	6%
Missing employment reference	106	4%
Missing employment record information	43	2%
Missing character reference	39	2%
Total	**2,400**	**92%**

- 49% are attributable to missing current employment activity and family member information
- Top 10 reasons account for 92% of DISCO's case rejections

Defense Industrial Security Clearance Office (DISCO)
FY12 Reasons for Case Rejection by OPM

TOP 10 REASONS FOR OPM REJECTION OF INVESTIGATION REQUEST		
Reason	**Count**	**Percent**
Fingerprint card not submitted within required timeframe (14 days)	777	59%
Certification / Release forms illegible	169	13%
Certification / Release forms not meeting date requirements	126	10%
Discrepancy with applicant's place of birth	80	6%
Discrepancy with applicant's date of birth	35	3%
Certification / Release form number incorrect	31	2%
Missing Certification / Release forms	19	1%
Missing reference information	16	1%
Incorrect/inaccurate social security number	16	1%
Missing employment information	10	1%
Total	**1,279**	**98%**

eFP Implementation Options

- USD/I memo – implement NLT December 2013
- Secure Web Fingerprint Transmission application – est. 2009
- Working with USD/I to gain access to deployed electronic fingerprint devices with DoD
- Conduct monthly webinars (4th Tuesday) to assist Industry with questions on implementation – Initial Webinar 24 July 2012 (1330-1430)

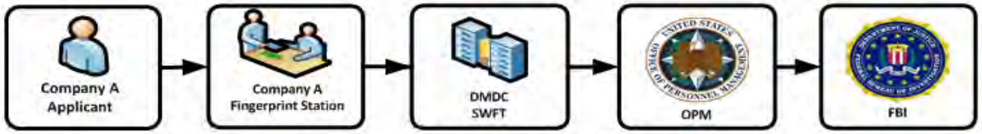


Figure 1 – Company Purchases Equipment

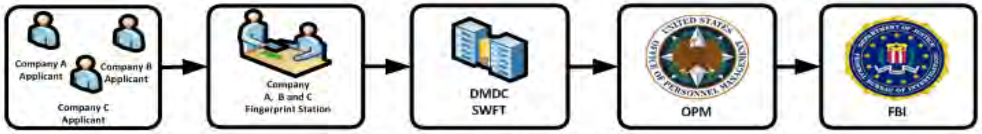


Figure 2 – Companies Sharing Resources

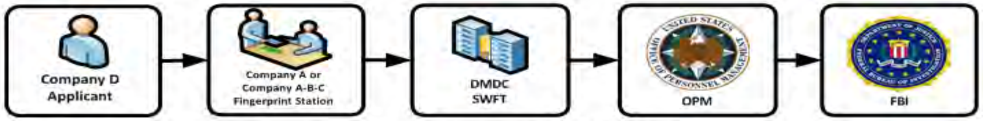


Figure 3 – Company(s) Offering Service

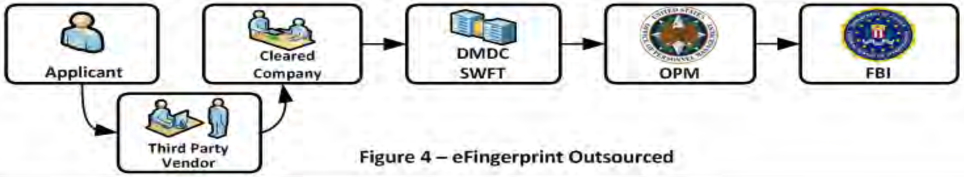
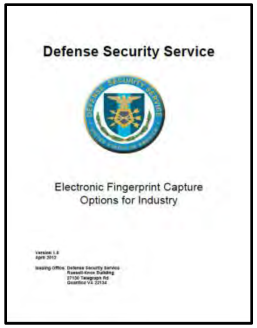


Figure 4 – eFingerprint Outsourced



Defense Security Service

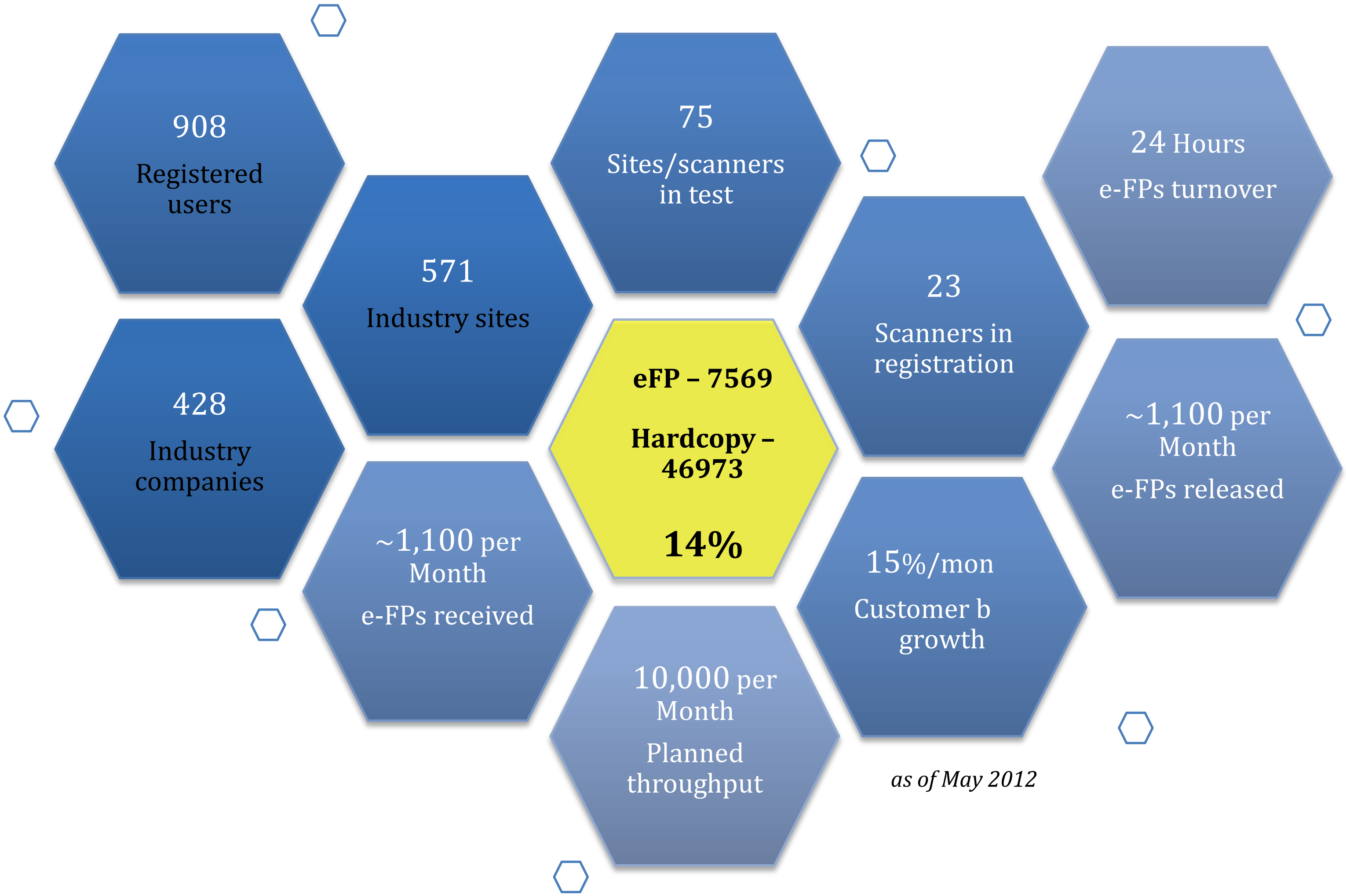
Electronic Fingerprint Capture
Options for Industry

Version 1.0
April 2012

Issuing Office: Defense Security Service
Russell-Knox Building
27130 Telegraph Rd
Quantico VA 22134

http://www.dss.mil/documents/disco/electronic-fingerprint-capture.pdf

Fingerprints By the Digits – FY12



908
Registered users

428
Industry companies

571
Industry sites

~1,100 per Month
e-FPs received

75
Sites/scanners in test

eFP – 7569

Hardcopy – 46973

14%

10,000 per Month
Planned throughput

23
Scanners in registration

15%/mon
Customer b growth

24 Hours
e-FPs turnover

~1,100 per Month
e-FPs released

as of May 2012

Customer Service and Way Ahead

- SWFT Software enhancements
  - OPM–SWFT– Submission Site release status feedback
  - Support for multiple Cage Codes
  - Bulk upload of e-fingerprints
  - Smart card logon
  - Online self-registration
- Online documentation: https://www.dmdc.osd.mil/psawebdocs
- Email inquiries: swft@osd.pentagon.mil
- Call Center available Mon-Fri 6 am – 6 pm EST

Attachment #4- ODNI PCL Presentation

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

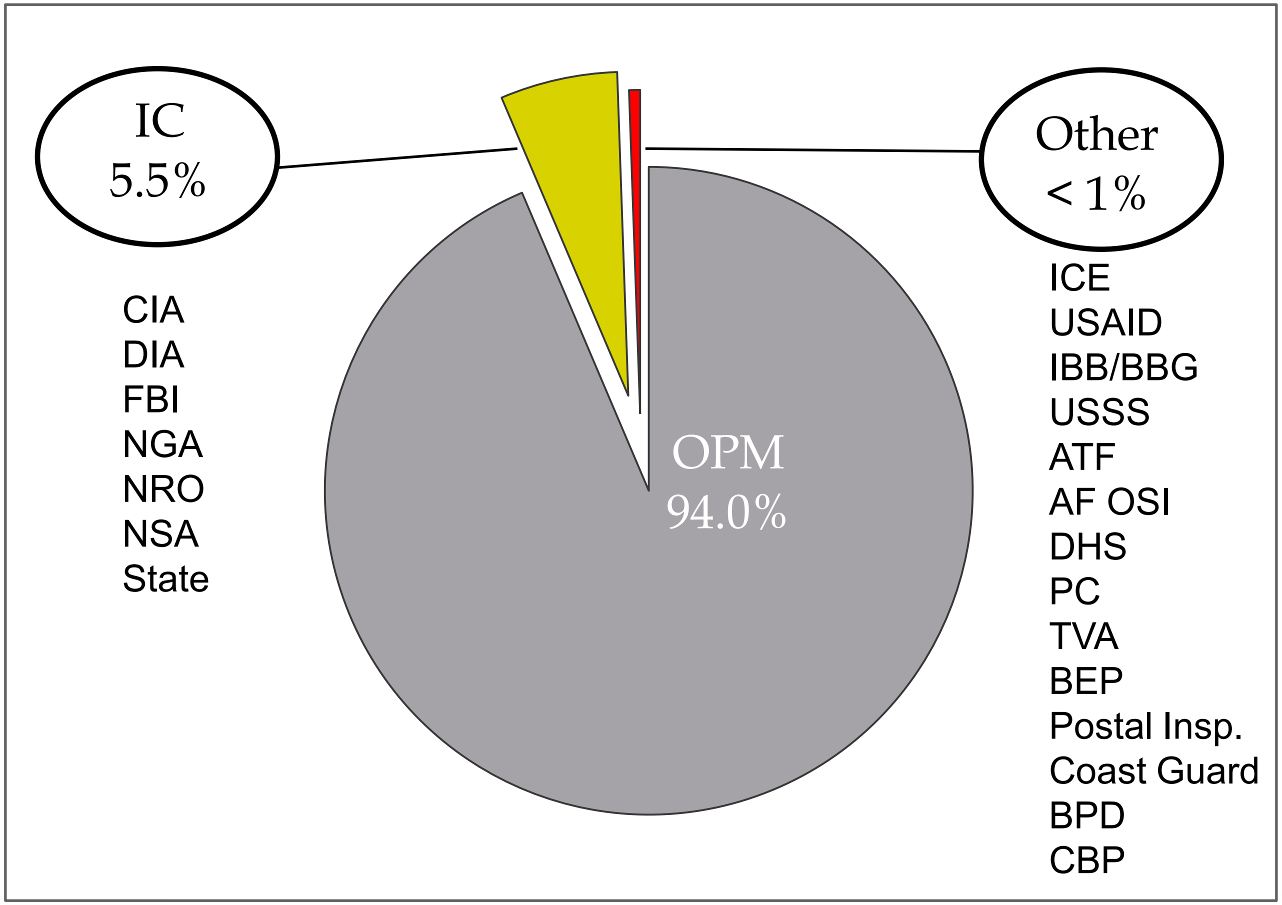
Industry Performance Metrics

ONCIX/Special Security Directorate

LEADING INTELLIGENCE INTEGRATION

NISPPAC
11 July 2012

Overall Volume by ISP



CIA
DIA
FBI
NGA
NRO
NSA
State

ICE
USAID
IBB/BBG
USSS
ATF
AF OSI
DHS
PC
TVA
BEP
Postal Insp.
Coast Guard
BPD
CBP

Intelligence Community Timeliness for Industry

There are 5 IC agencies that report metrics as delegated ISPs (5.5% of USG workload)

- Initials
  - There was a slight increase in investigative timeliness due to 3 our 5 agencies experiencing an increase in their investigative timeliness for initial investigations.
  - There was a slight increase in adjudicative timeliness due to one agency experiencing a 10-day increase while all other agencies stayed the same or experienced a slight decrease.
- Periodic Reinvestigations
  - All agencies were within the goal of 150 days
  - Adjudication Phase: Since Q4 FY11, agencies have been moving toward the 30-day goal.

Other Delegated Investigative Service Provider's (ISP) Timeliness for Industry

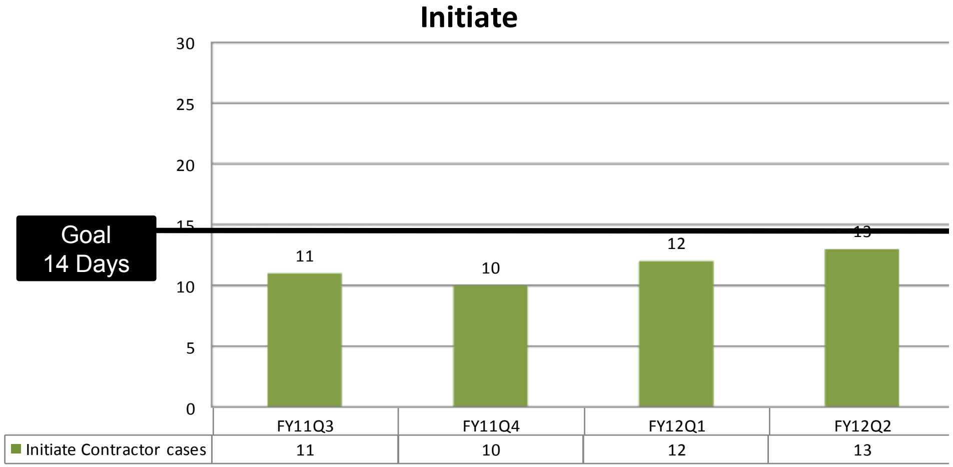
Only 3 of the 14 Delegated ISPs conducted initial investigations on contractors, while only one agency conducted periodic reinvestigations on contractors (less than 1% of USG workload)

- Initials – Metrics were based on a total of 16 cases
- Periodic Reinvestigations – There was a large decrease in investigative timeliness from 153 days to 69 days, however this was solely based on 4 reported cases.

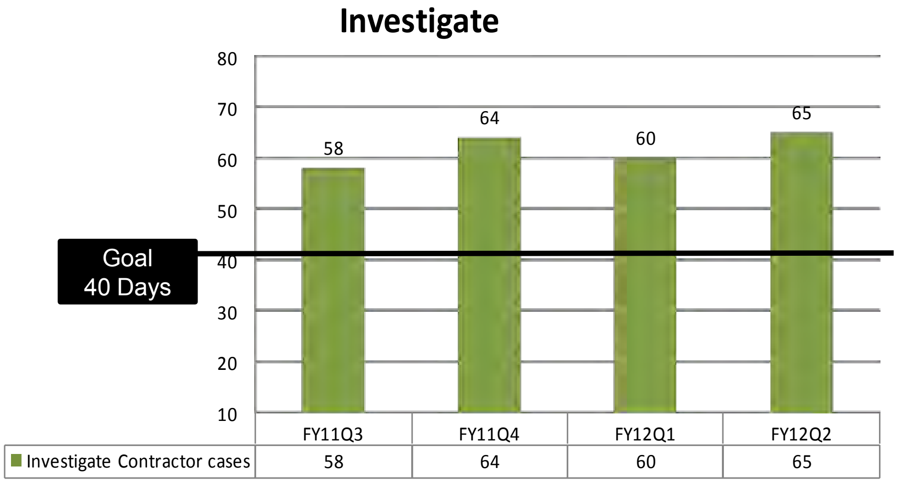
Intelligence Community

Combined Top Secret and Secret Initials

(5.5% of USG Workload)



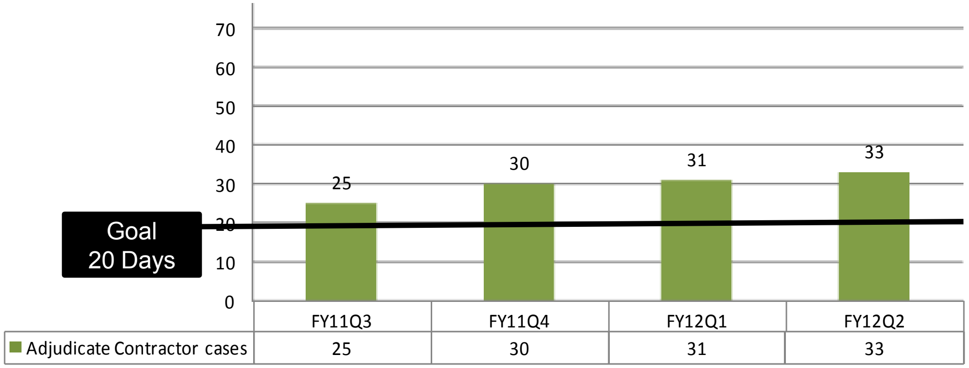
	FY11Q3	FY11Q4	FY12Q1	FY12Q2
🟩 Initiate Contractor cases	11	10	12	13



	FY11Q3	FY11Q4	FY12Q1	FY12Q2
🟩 Investigate Contractor cases	58	64	60	65

Timeliness:

for Contractors

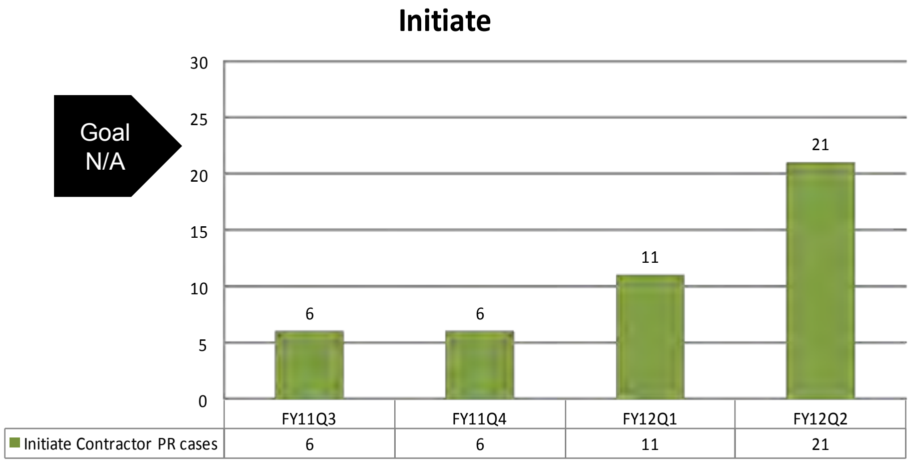


	FY11Q3	FY11Q4	FY12Q1	FY12Q2
🟩 Adjudicate Contractor cases	25	30	31	33

Intelligence Community

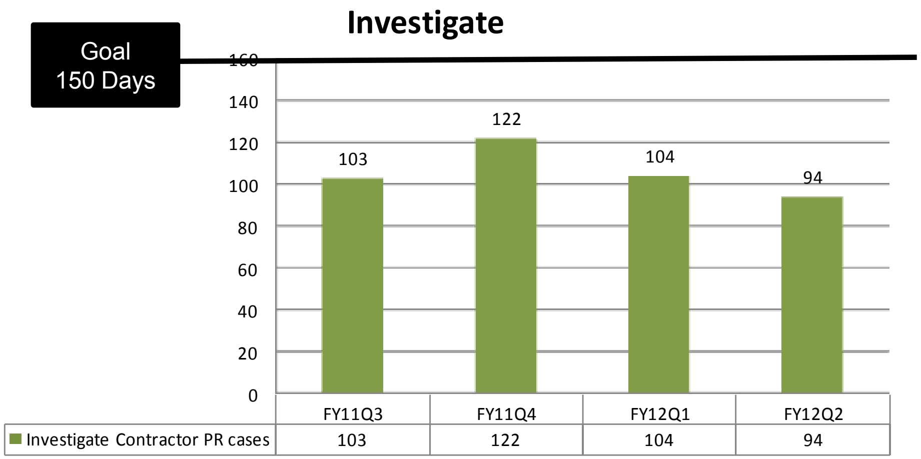
Combined Top Secret and Secret Periodic Reinvestigations

(5.5% of USG Workload)



Goal N/A

	FY11Q3	FY11Q4	FY12Q1	FY12Q2
🟩 Initiate Contractor PR cases	6	6	11	21

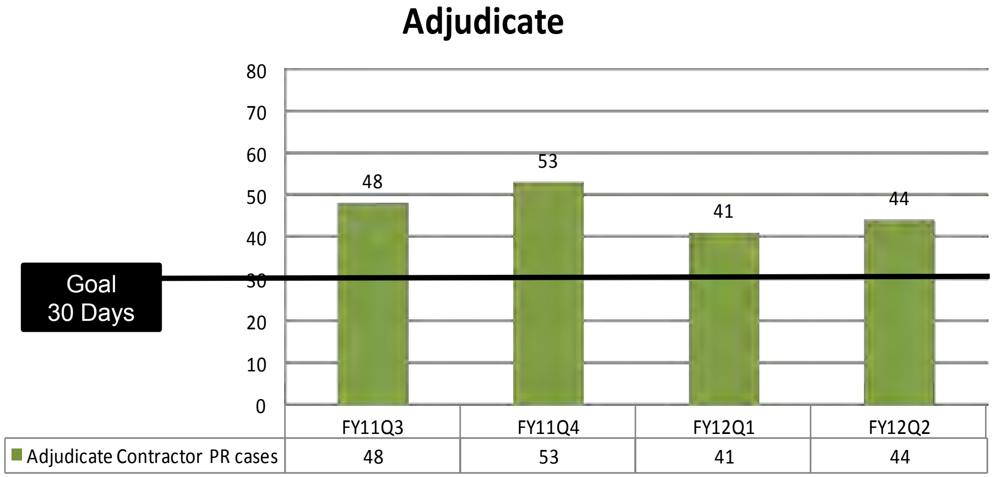


Goal 150 Days

	FY11Q3	FY11Q4	FY12Q1	FY12Q2
🟩 Investigate Contractor PR cases	103	122	104	94

Timeliness:

for Contractors



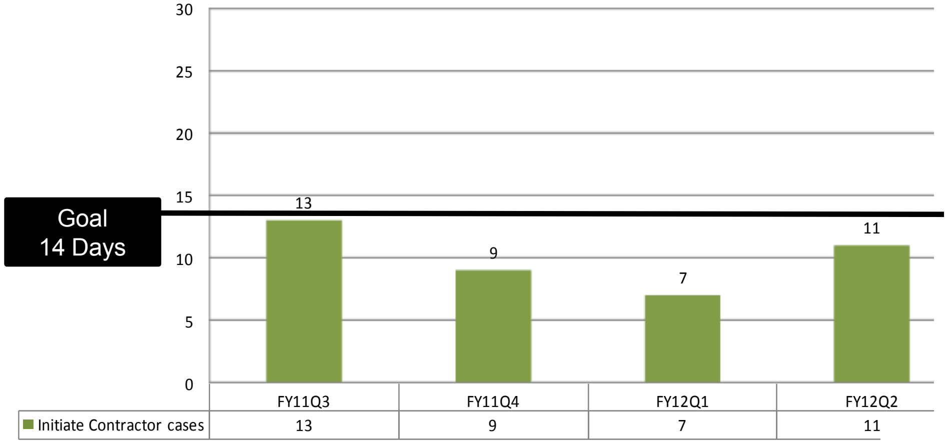
Goal 30 Days

	FY11Q3	FY11Q4	FY12Q1	FY12Q2
🟩 Adjudicate Contractor PR cases	48	53	41	44

Other Delegated

(Less than 1% of USG Workload Combined Top Secret and Secret Initials)

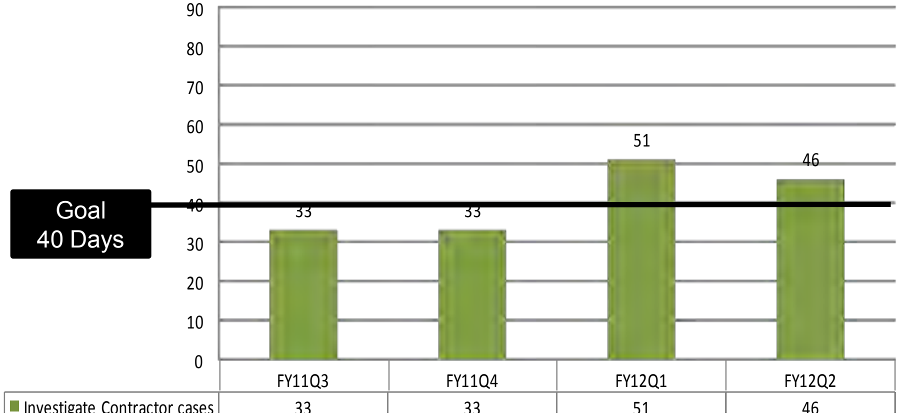
Initiate



Goal
14 Days

	FY11Q3	FY11Q4	FY12Q1	FY12Q2
🟩 Initiate Contractor cases	13	9	7	11

Investigate



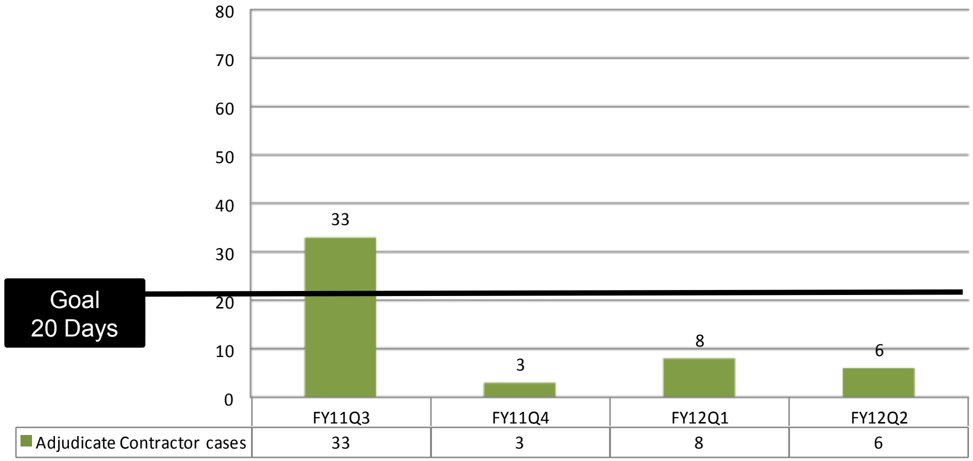
Goal
40 Days

	FY11Q3	FY11Q4	FY12Q1	FY12Q2
🟩 Investigate Contractor cases	33	33	51	46

Timeliness:

for Contractors

Adjudicate

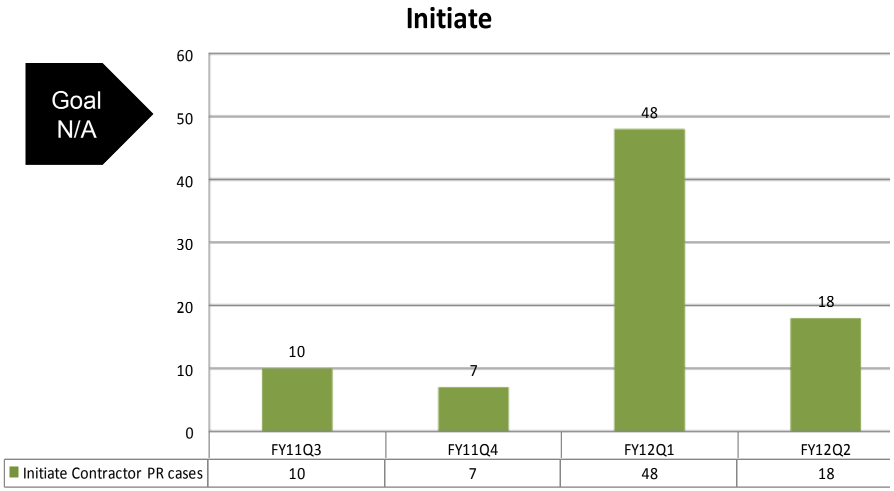


Goal
20 Days

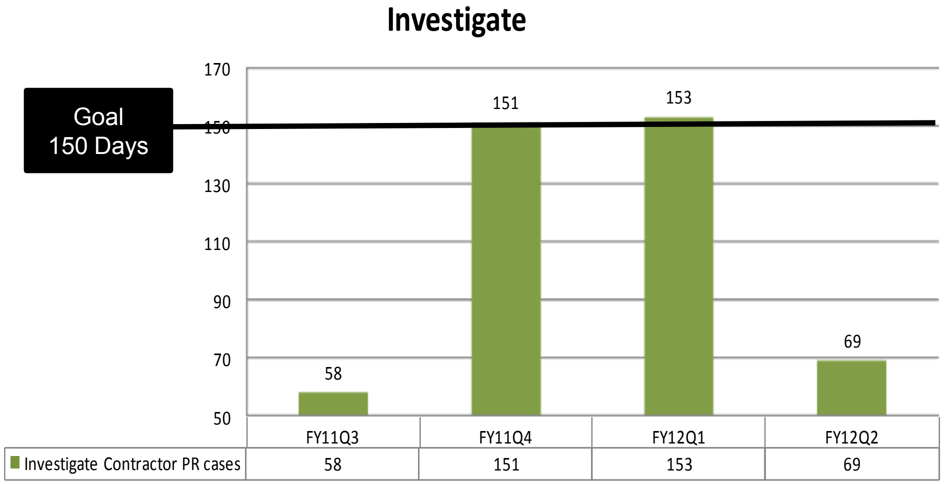
	FY11Q3	FY11Q4	FY12Q1	FY12Q2
🟩 Adjudicate Contractor cases	33	3	8	6

Other Delegated

(Less than 1% of USG Workload Combined Top Secret and Secret Periodic Reinvestigations)



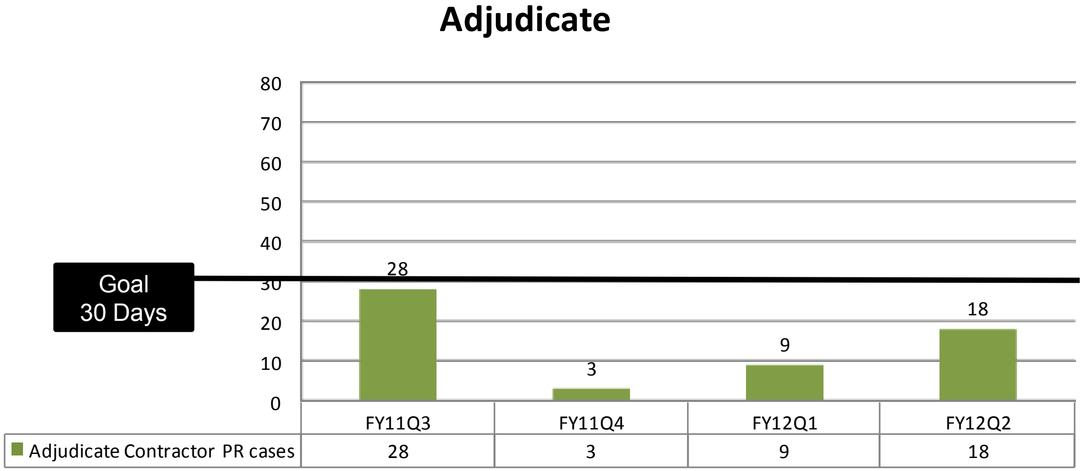
	FY11Q3	FY11Q4	FY12Q1	FY12Q2
🟩 Initiate Contractor PR cases	10	7	48	18



	FY11Q3	FY11Q4	FY12Q1	FY12Q2
🟩 Investigate Contractor PR cases	58	151	153	69

Timeliness:

for Contractors



	FY11Q3	FY11Q4	FY12Q1	FY12Q2
🟩 Adjudicate Contractor PR cases	28	3	9	18

Attachment #5- DOE PCL Presentation

HSS

Office of Health, Safety and Security

U.S. Department of Energy

Personnel Security Brief

April 2012

Personnel Security Overview

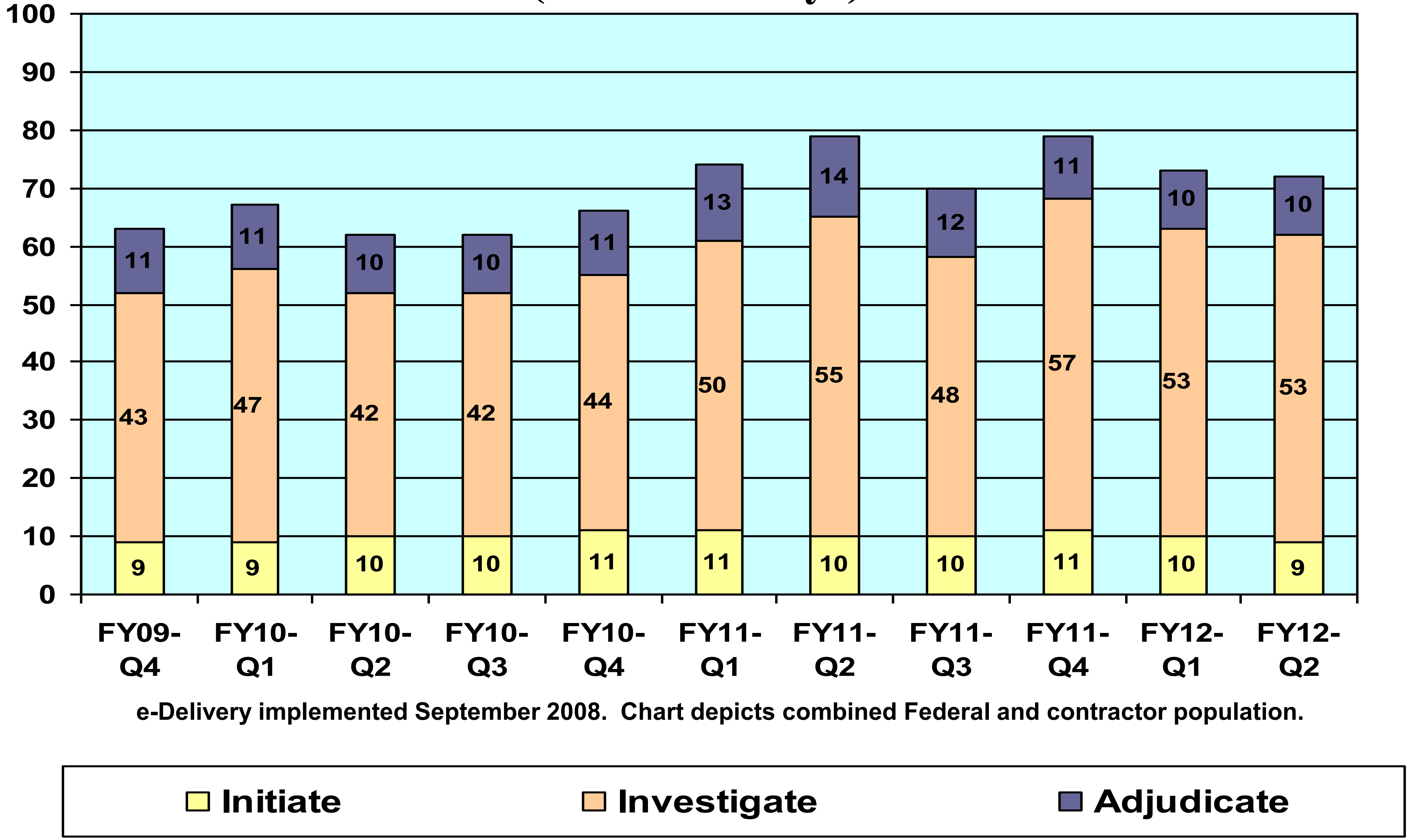
HSS
Office of Health, Safety and Security

- DOE adjudicates both Federal and contractor staff
- Eight adjudicative facilities
- Policy, administrative review, and appeal functions centralized at Headquarters
- Cleared contractors, as of April 2, 2012:

  -63,925 Q access authorizations

  -23,871 L access authorizations
- Have met IRTPA initial security clearance adjudicative goals since April 2009

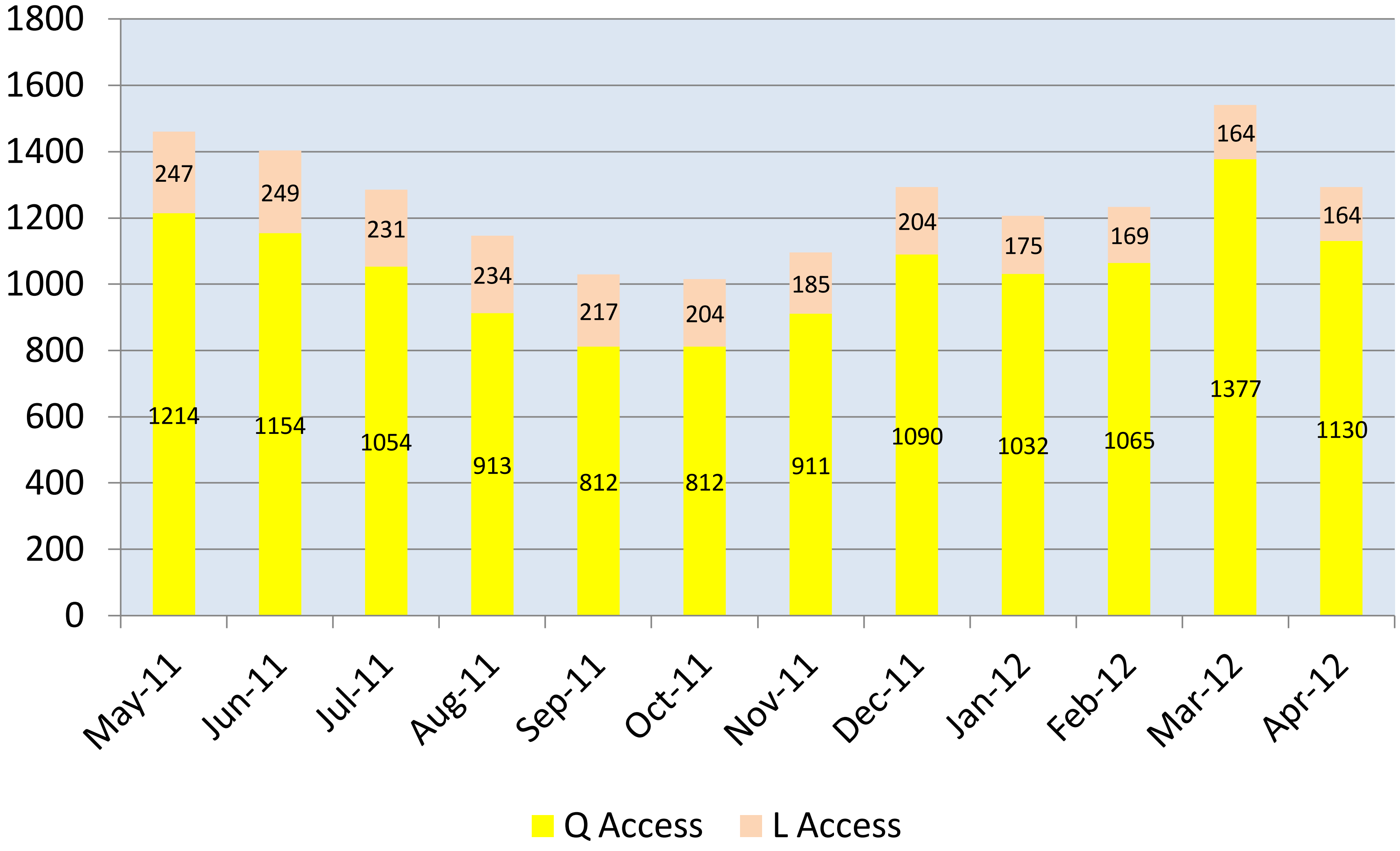
DOE’s Average End-to-End Timeliness Trends for 90% Initial Q/TS and All L/S/C Security Clearances
(Goal: 74 Days)



e-Delivery implemented September 2008. Chart depicts combined Federal and contractor population.

DOE TOTAL CASE INVENTORY – Last 12 Months

(Federal and Contractor Adjudications Pending as of the Last Day of the Month)



Attachment #6- ODAA C&A Presentation

Industrial Security Field Operations (ISFO)

Office of the Designated Approving Authority (ODAA)

May 2012

Defense Security Service

Overview:

- Security Plan Reviews
  - Security Plan Processing Timeliness
  - Top Ten Deficiencies Identified in Security Plans
  - Security Plan Denial and Rejection Rates
  - Second IATOs Issued
- System Onsite Validations
  - Timeliness
  - Top Ten Vulnerabilities

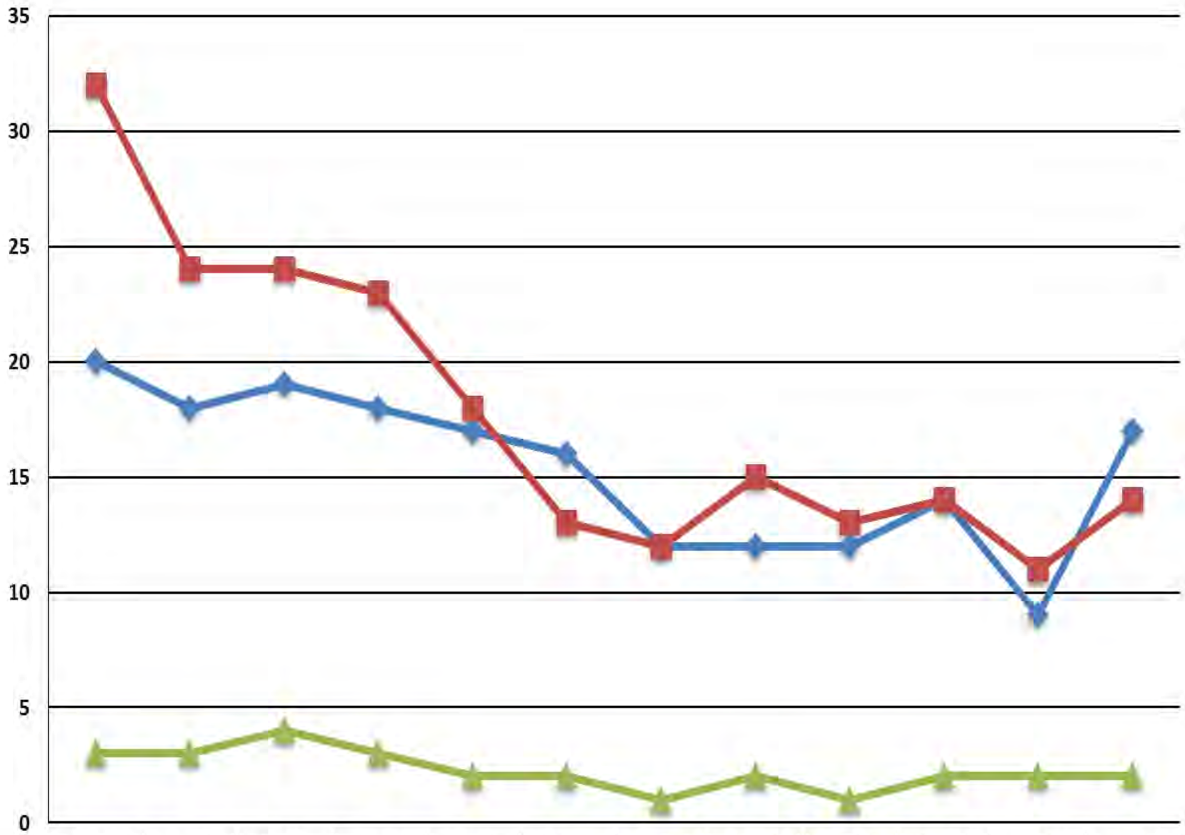
Defense Security Service

Certification & Accreditation

- DSS is the primary government entity responsible for approving cleared contractor information systems to process classified data.
- Work with industry partners to ensure information system security controls are in place to limit the risk of compromising national security information.
- **Ensures adherence to national industrial security standards.**

Security Plan Review Timeliness

May 2011 - April 2012



	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Jan-12	Feb-12	Mar-12	Apr-12
Time from DSS Reciept of plans to Granting of IATOs	20	18	19	18	17	16	12	12	12	14	9	17
Time from DSS Reciept of plans to Granting of SATOs	32	24	24	23	18	13	12	15	13	14	11	14
Industry Response Time to DSS Questions, Comments	3	3	4	3	2	2	1	2	1	2	2	2

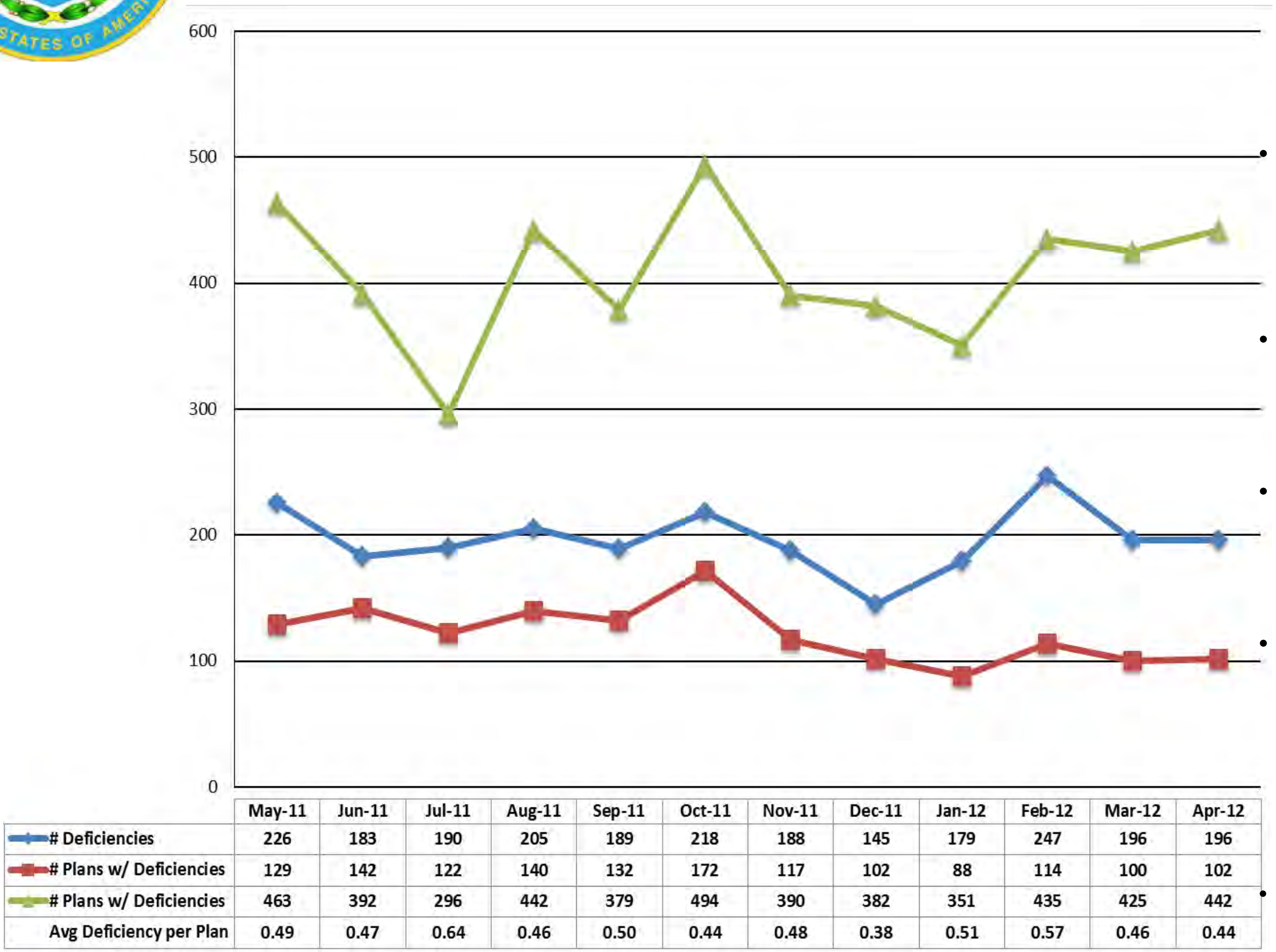
- 2865 Interim approvals to operate (IATOs) were issued during the preceding 12 month period
- Across the 12 months, it took 16 days on average to issue an IATO after a plan was submitted
- For the 1489 systems processed "Straight to ATO (SATO)" during the 12 months, it took an average of 17 days to issue the ATO

Last Months Snapshot

- 221 IATOs were granted in April with an average turnaround time of 17 days
- 174 SATOs were granted in April with an average turnaround time of 14 days

Results of Security Plan Reviews

May 2011 - April 2012

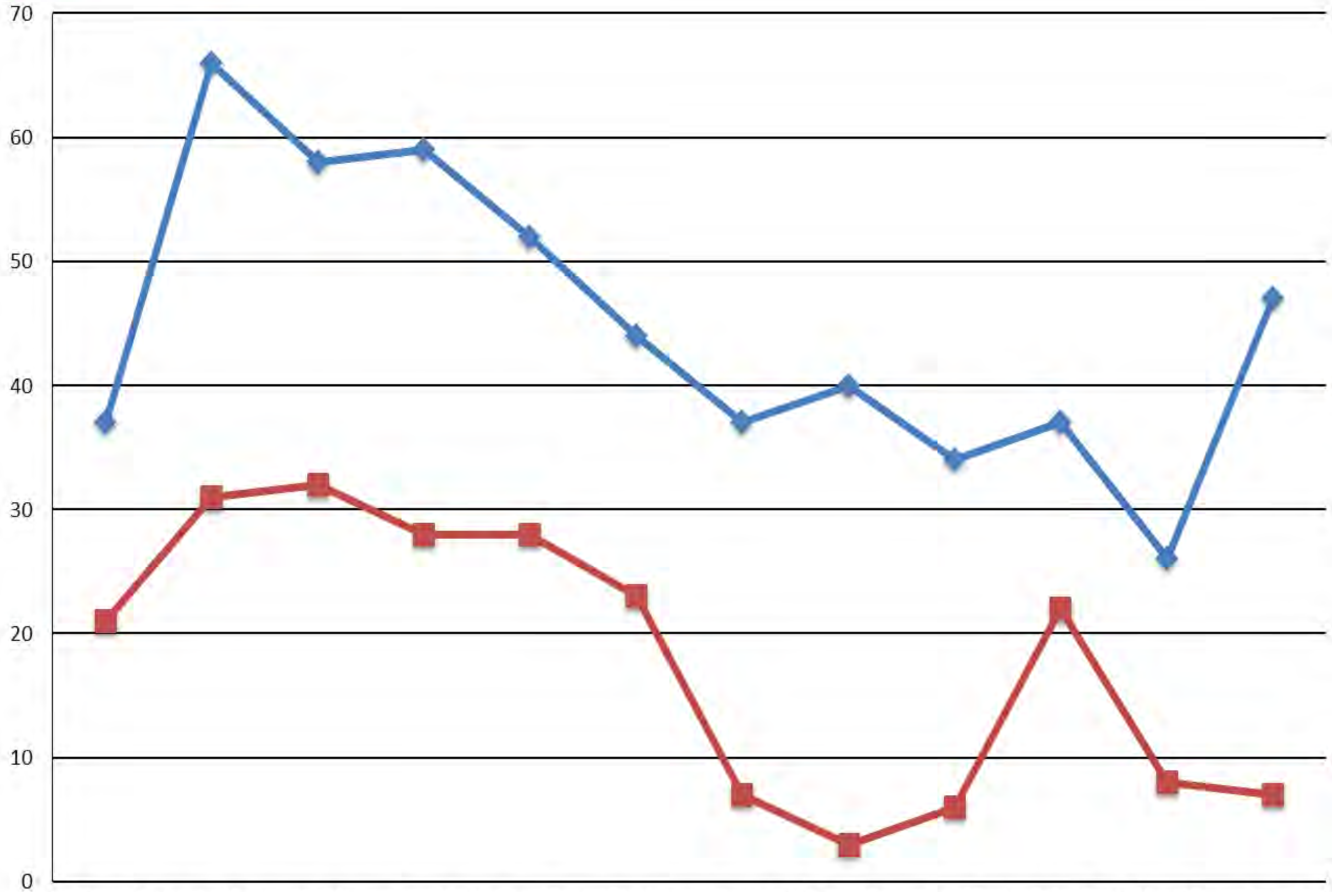


	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Jan-12	Feb-12	Mar-12	Apr-12
# Deficiencies	226	183	190	205	189	218	188	145	179	247	196	196
# Plans w/ Deficiencies	129	142	122	140	132	172	117	102	88	114	100	102
# Plans w/ Deficiencies	463	392	296	442	379	494	390	382	351	435	425	442
Avg Deficiency per Plan	0.49	0.47	0.64	0.46	0.50	0.44	0.48	0.38	0.51	0.57	0.46	0.44

- 4891 System security plans (SSPs) were accepted and reviewed during the 12 months
- 1460 of the SSPs (30%) required some level of correction prior to conducting the onsite validation
- 870 of the SSPs (18%) were granted IATO with corrections required
- 53 of the SSPs (1% of total ATOs) that went SATO required some level of correction
- 537 of the SSPs (11%) of the SSPs were denied IATO due to significant corrections needed (processed after corrections made)
- *Mar/Apr 196 is coincidental and double-checked*

Security Plan Denial & Rejection Rate

May 2011 - April 2012



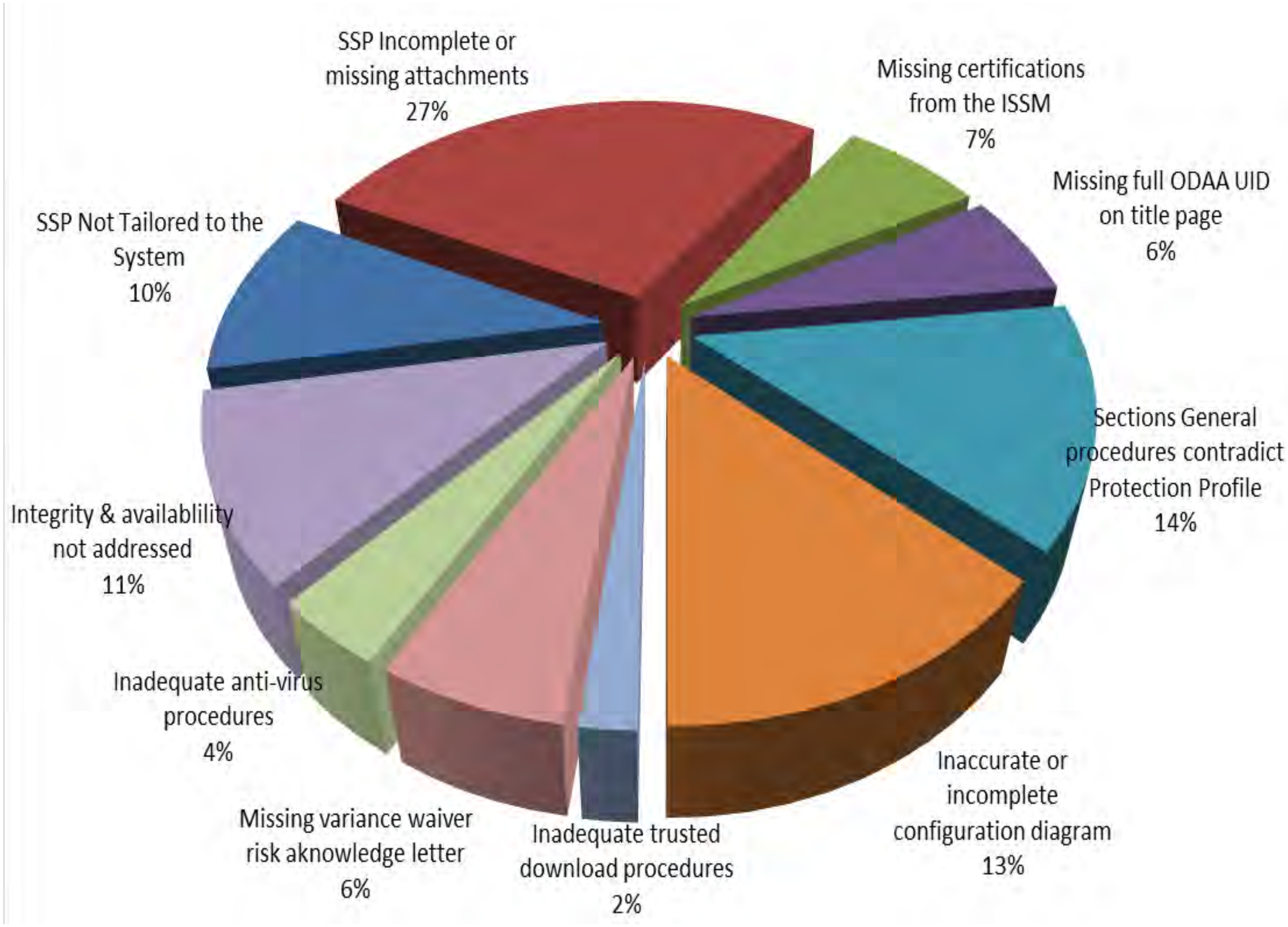
	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Jan-12	Feb-12	Mar-12	Apr-12
◆ Denials	37	66	58	59	52	44	37	40	34	37	26	47
■ Rejections	21	31	32	28	28	23	7	3	6	22	8	7

- Denials: 537 of the SSPs (11%) were received and reviewed, but denied IATO until corrections were made to the plan.

- "Rejections: 216 of the SSPs (4%) were not submitted in accordance with requirements and were not entered into the ODAA process. These SSPs were returned to the ISSM with guidance for submitting properly and processed upon resubmission. ."

Common Deficiencies in Security Plans

May 2011 - April 2012

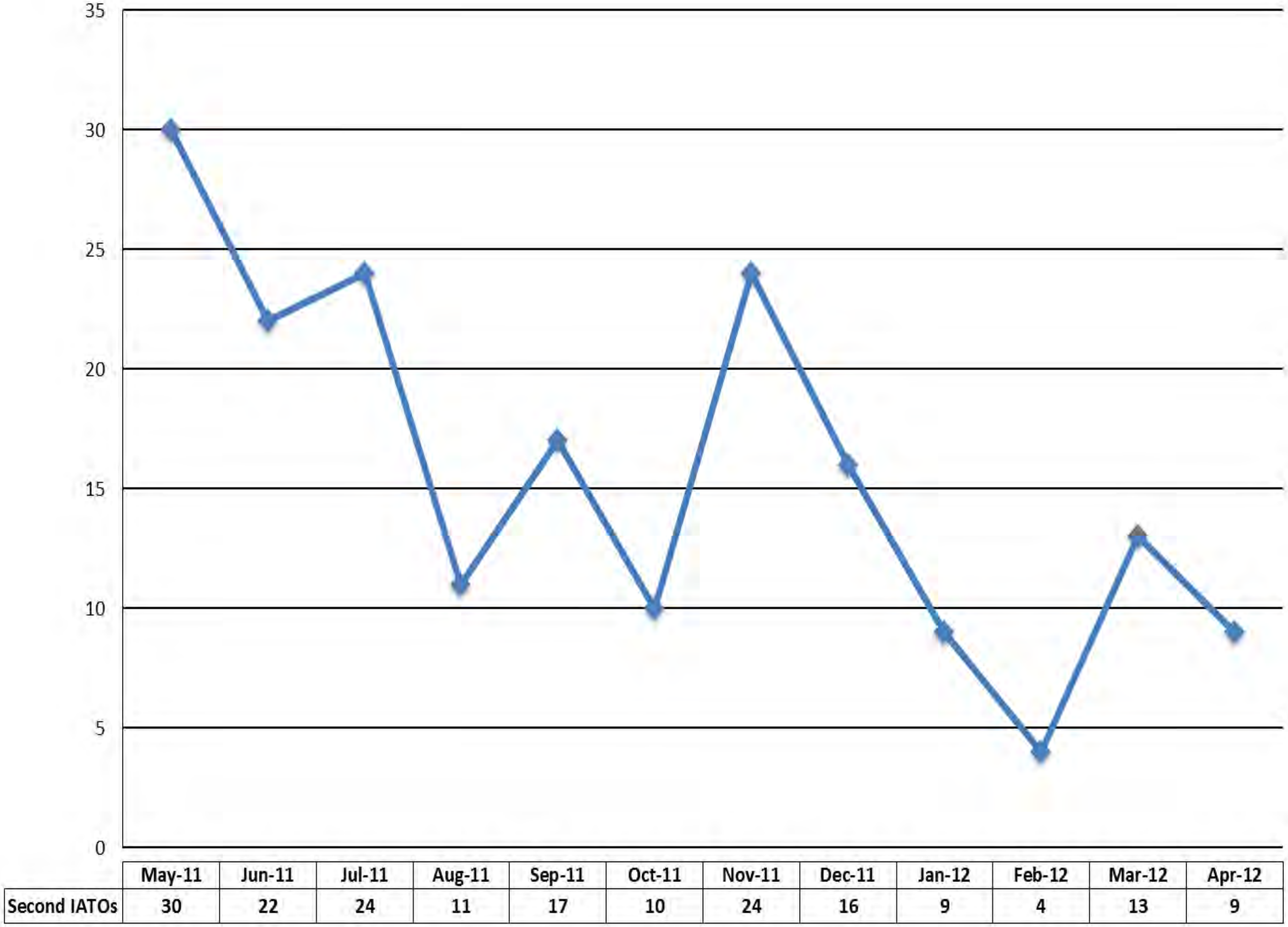


Top 10 Deficiencies

1. SSP was incomplete or missing attachments
2. Sections in general procedures contradict protection profile
3. Inaccurate or incomplete configuration diagram
4. Integrity & availability not properly addressed
5. SSP was not tailored to the system
6. Missing certification statements from the ISSM
7. Missing variance, waiver, or risk acknowledgement letter
8. Missing full ODAA UID
9. Inadequate anti-virus procedures
10. Inadequate trusted download procedures

Second IATOs

May 2011 - April 2012



	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Jan-12	Feb-12	Mar-12	Apr-12
Second IATOs	30	22	24	11	17	10	24	16	9	4	13	9

Common Reasons for second IATOs

- Host Based Security System (HBSS) not installed

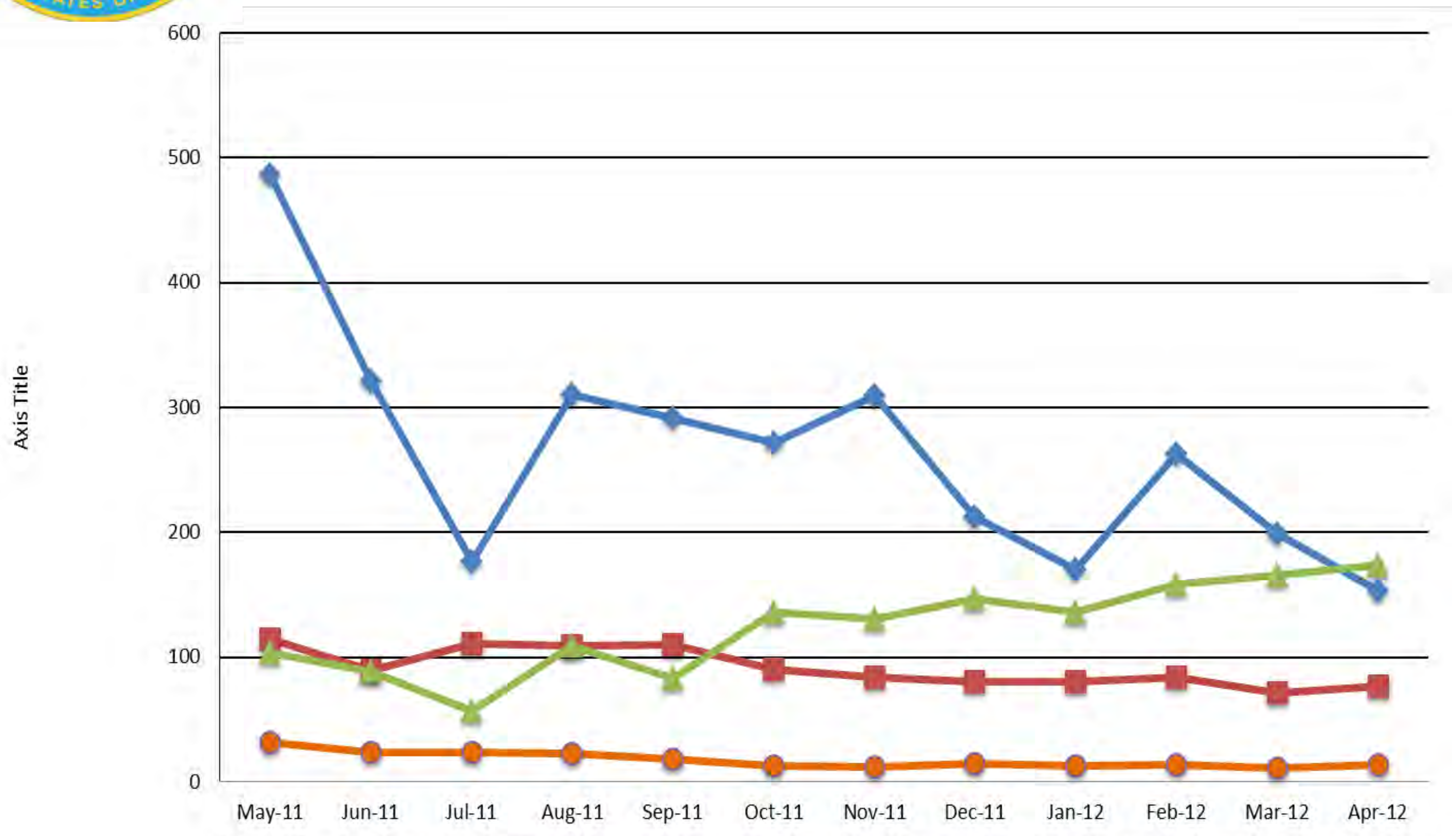
- Onsite validation rescheduled due to ISSP and/or ISSM availability

- Administrative reasons after the system is certified (MOUs, etc.)

The total number of 2nd IATOs for the past twelve months was 189

System Validations

May 2011 - April 2012



	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Jan-12	Feb-12	Mar-12	Apr-12
Total ATOs	486	321	176	310	291	272	309	212	170	263	199	153
Avg Days to ATO	114	89	111	109	110	90	84	80	80	84	71	77
Total SATOs	104	88	57	109	83	136	131	147	136	158	166	174
Avg Days to SATO	32	24	24	23	18	13	12	15	13	14	11	14

•3162 systems were processed from IATO to ATO status during the 12 months

•Across the 12 months, it took 94 days on average to process a system from IATO to ATO

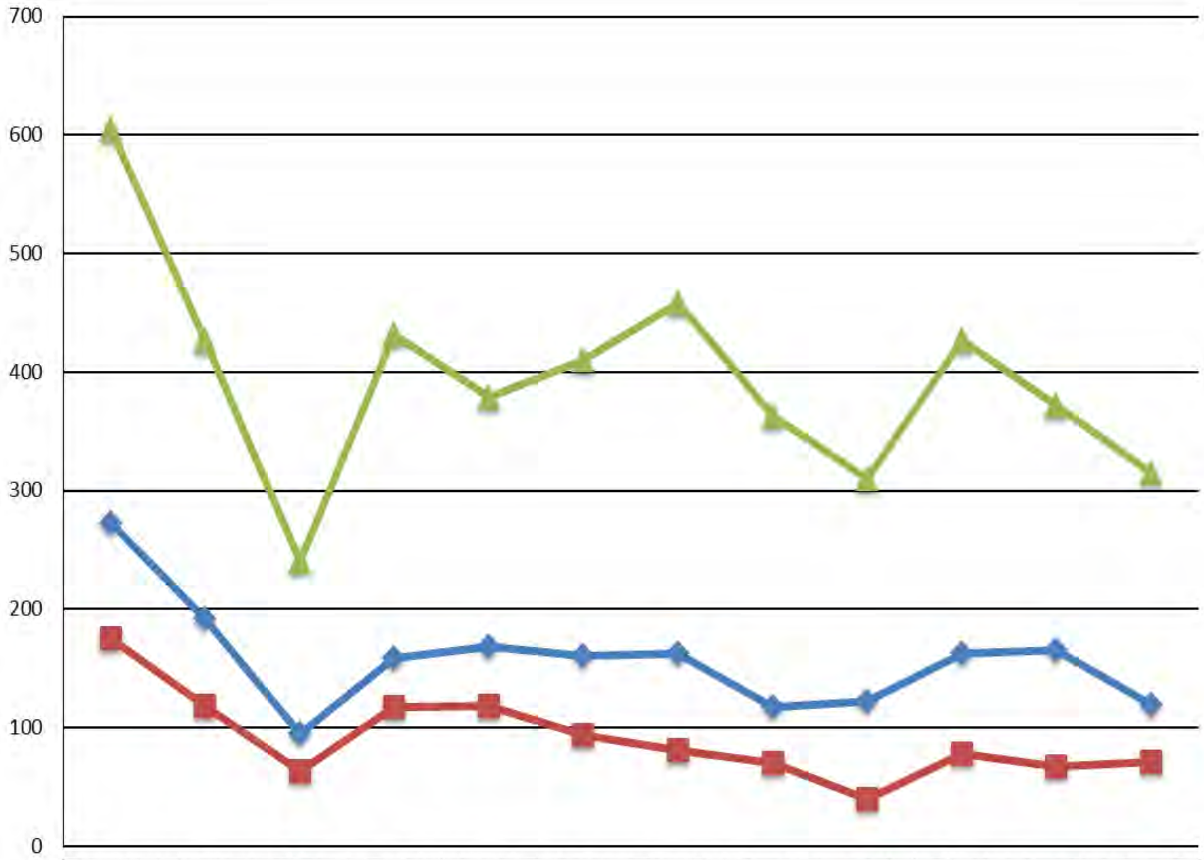
•1489 systems were processed Straight to ATO status during the 12 months

•Across the 12 months, it took 17 days on average to process a system Straight to ATO

•Across the 12 months, (32%) of ATOs were for systems processed Straight to ATO

System Validations

May 2011 – April 2012

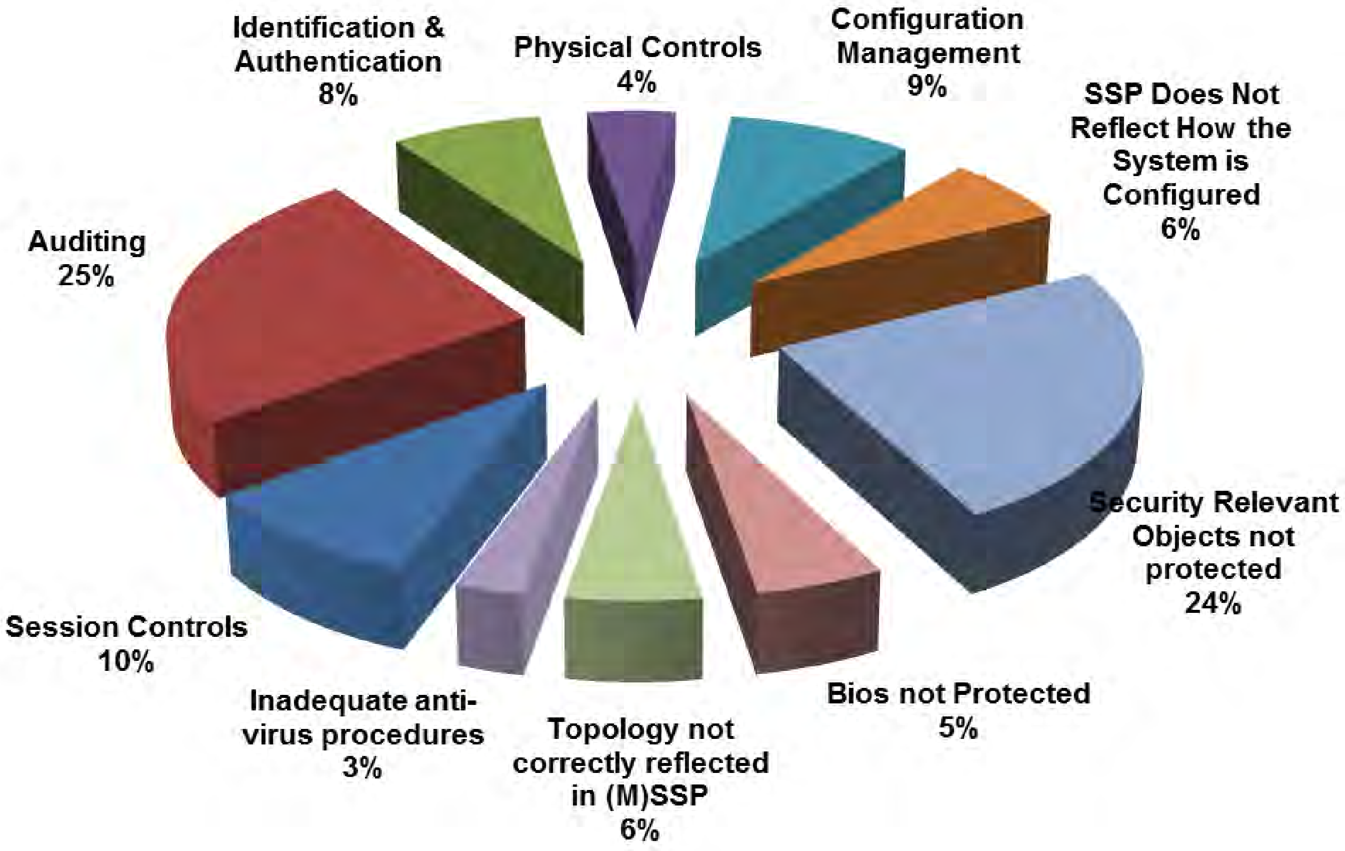


	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Jan-12	Feb-12	Mar-12	Apr-12
# Vulnerabilities	273	192	95	159	168	161	163	117	122	163	166	119
# Onsites w/ vulnerabilities	175	118	63	117	118	94	81	70	40	78	67	71
# Onsites	605	427	240	432	379	410	458	363	310	427	372	315
Avg Vulnerability per Onsite	0.45	0.45	0.40	0.37	0.44	0.39	0.36	0.32	0.39	0.38	0.45	0.38

- 4738 completed validation visits during the 12 months
- 3468 systems (73%) had no vulnerabilities identified
- 1163 systems (25%) had minor vulnerabilities identified that were corrected while onsite
- 107 systems (2%) had significant vulnerabilities identified, resulting in a second validation visit to the site after corrections were made

Common System Vulnerabilities

May 2011 - April 2012



Top 10 Vulnerabilities

1. Inadequate auditing controls
2. Security Relevant Objects not protected.
3. Improper session controls
4. Inadequate configuration management
5. Identification & authentication controls
6. SSP does not reflect how the system is configured
7. Topology not correctly reflected in (M)SSP
8. Bios not protected
9. Physical security controls
10. Inadequate Anti-virus procedures

Summary and Takeaways:

- Security Plans are Being Processed and Reviewed in a Timely Manner
  - Most Common Deficiencies in SSPs Include Missing Attachments, Documentation Errors, Integrity and Availability Requirements
  - Need More Emphasis on Reducing Deficiencies
- Onsite Validations are Being Completed in a Timely Manner
  - Most Common Vulnerabilities Identified During System Validation Include Auditing Controls, Configuration Management, Not Protecting Security Relevant Objects
- More Straight to ATO (Where Practical) to Reduce Risk and Increase Efficiency

Backup Slides

Security Plan Review Discrepancies by Facility Category

Number of Plans Submitted April 2012		55	102	67	78	140
	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
SSP Is incomplete or missing attachments	56	8.93%	**12.04%**	11.94%	**12.82%**	**14.08%**
Sections in General Procedures contradict Protection Profile	29	5.36%	0.00%	**8.96%**	**11.54%**	**7.75%**
Inaccurate or Incomplete Configuration diagram/system description	27	0.00%	1.85%	**7.46%**	**6.41%**	**10.56%**
Integrity & Availability not addressed completely	19	**3.57%**	0.00%	2.99%	**10.26%**	**4.93%**
Missing certifications from the ISSM	15	1.79%	**2.78%**	**5.97%**	1.28%	**4.23%**
Missing variance/waiver/risk acknowledgement letter	14	1.79%	**5.56%**	1.49%	**3.85%**	**2.11%**

Security Plan Review Discrepancies by Facility Category (cont'd)

April 2012	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
SSP Not Tailored to the System	14	1.79%	**2.78%**	1.49%	**3.85%**	**4.23%**
Inadequate anti-virus procedures	9	**1.79%**	0.00%	**1.49%**	**6.41%**	1.41%
Missing full ODAA UID on Title Page	8	**1.79%**	0.00%	1.49%	**2.56%**	**2.82%**
Inadequate trusted download procedures	3	0.00%	0.00%	**1.49%**	**2.56%**	0.00%
Inadequate recovery procedures	1	0.00%	0.00%	0.00%	0.00%	**0.70%**
Other	0	0.00%	0.00%	0.00%	0.00%	0.00%
Total Errors %	**195**	**7.69%**	**13.85%**	**15.38%**	**24.62%**	**38.46%**
Total Errors	**195**	**15**	**27**	**30**	**48**	**75**

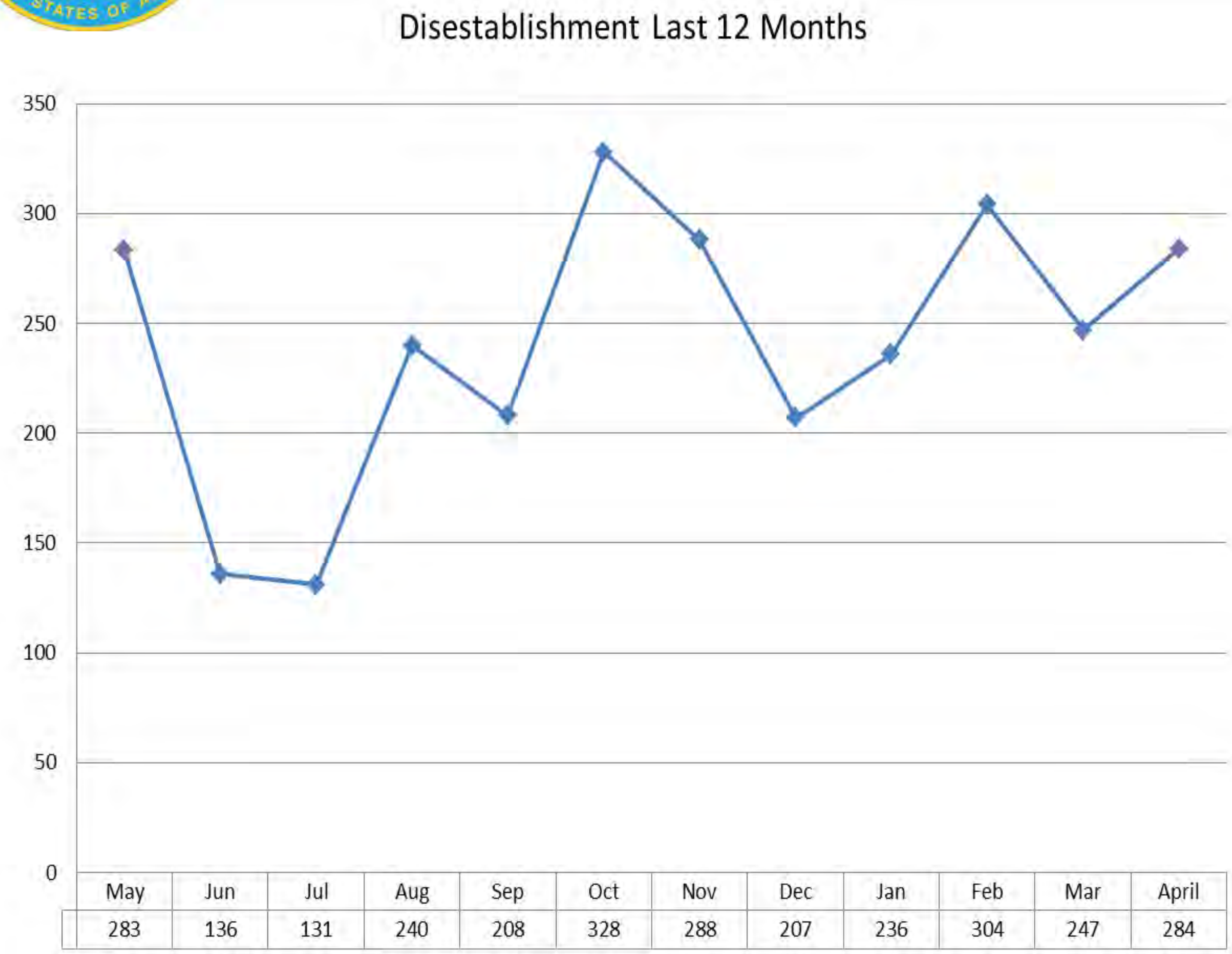
System Validation Vulnerabilities by Facility Category

Systems Validated by Facility Category April 2012		13	30	26	33	51
	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Auditing	33	**2.94%**	1.33%	**11.54%**	5.26%	**22.68%**
Security Relevant Objects not protected	28	2.94%	0.00%	**7.69%**	**8.77%**	**18.56%**
Session Controls	15	**5.88%**	0.00%	**5.77%**	5.26%	**7.22%**
Configuration Management	10	0.00%	**1.33%**	0.00%	**5.26%**	**6.19%**
I & A	6	**2.94%**	0.00%	**1.92%**	1.75%	**3.09%**
Physical Controls	6	0.00%	0.00%	**1.92%**	0.00%	**5.15%**
SSP Does Not Reflect How the System is Configured	5	0.00%	1.33%	**1.92%**	**1.75%**	**2.06%**
Bios not Protected	**5**	0.00%	0.00%	**1.92%**	**3.51%**	**2.06%**
Topology not correctly reflected in (M)SSP	**4**	0.00%	0.00%	**3.85%**	**1.75%**	**1.03%**
Root/Admin Account misconfigured	2	0.00%	0.00%	0.00%	0.00%	**2.06%**

System Validation Vulnerabilities by Facility Category (cont'd)

April 2012	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Inadequate anti-virus procedures	2	0.00%	0.00%	0.00%	0.00%	**2.06%**
Compilation	1	0.00%	0.00%	0.00%	**1.75%**	0.00%
All Users are Configured as Administrators	1	0.00%	0.00%	0.00%	0.00%	**1.03%**
PL Not Adequately Addressed	1	0.00%	0.00%	**1.92%**	0.00%	0.00%
RAL Not Provided	0	0.00%	0.00%	0.00%	0.00%	0.00%
Different System Type	0	0.00%	0.00%	0.00%	0.00%	0.00%
Trusted Download Review	0	0.00%	0.00%	0.00%	0.00%	0.00%
POA&M not Implemented	0	0.00%	0.00%	0.00%	0.00%	0.00%
Other	**0**	0.00%	0.00%	0.00%	0.00%	0.00%
NSP Not Provided/Referenced for a WAN Node	0	0.00%	0.00%	0.00%	0.00%	0.00%
Total Errors % Slide One and Two	**119**	**4.20%**	**2.52%**	**16.81%**	**16.81%**	**59.66%**
Total Errors # Slide One and Two	**119**	**5**	**3**	**20**	**20**	**71**

System Disestablishments



May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	April
283	136	131	240	208	328	288	207	236	304	247	284

Disestablishments for Month April 2012:

Total: 284

Capital: 22 (7.75%)

Northern: 115 (40.49%)

Southern: 29 (10.21%)

Western: 118 (41.55%)

Attachment # 7- Combined Industry Presentation

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

JULY 11, 2012

Outline

- Current NISPPAC/MOU Membership
- Charter
- Working Groups
- Policy Changes

National Industrial Security Program

Policy Advisory Committee Industry Members

Nominations will be accepted following this meeting to replace , Scott Conway & Marshall Sanders.

Members	Company	Term Expires
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
Rick Graham	Huntington Ingalls Industries	2015
Steve Kipp	L3 Communications	2015

Industry MOU Members

AIA	Vince Jarvie
ASIS	Marshall Sanders
CSSWG	Mark Rush
ISWG	Mitch Lawrence
NCMS	Rhonda Peyton
NDIA	Jim Hallo successor Ken White
Tech America	Kirk Poulsen

* Changes

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
  - Potential effects of Government Sequestration on clearance processing
  - EQUIP & JPAS change process/communication
  - Request to add a member of the Industry Team to this working group
  - USN's RapidGate Program challenges
- Automated Information System Certification and Accreditation
- Ad-Hoc
  - NISPOM Rewrite Working Group (12 meetings), Chapter 10 Comments provided back June 22nd
  - CI Working Group & Suspicious Contact reporting requirements continue to be fragmented

Working Groups continued

Industry requested an ISOO sponsored Ad-Hoc SAP Working Group

- **Industry provided White Paper on SAP issues/concerns**
- **25 January 2012 ISOO engaged Government agencies authorized to create SAPs to discuss:**
  - **Specific issues raised by Industry**
  - **Initial government response**
- **15 February 2012 Joint Government/Industry Session**
  - **Discuss results of Government session**
  - **Address Industry specific issues**
- **July 11th Collectively need to determine our next step with this working group**

Security Policy Changes

Executive Orders - Industry Implementation ?

EO # 13587

Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

7 October 2011

EO # 13556

Controlled Unclassified Information (CUI)

4 November 2010

THANK YOU

Attachment #8- DIB Presentation

Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Program

July 11, 2012

Victoria Morgan
Department of Defense

Contact Information

Ms. Victoria Morgan
Director, DIB CS/IA Program

E-mail: DIB.CS/IA.Reg@osd.mil

Phone: (703) 604-3167

Toll Free Number: 1-855-363-4227

FAX: (703) 604-4745

Interim Federal Rule:

http://www.gpo.gov/fdsys/pkg/FR-2012-05-11/pdf/2012-10651.pdf

Attachment 9- NISPPAC Action Items

Attachment 9.
Summary of Action Items
JULY 11, 2012 NISPPAC Meeting

1) The Chair requested the Personnel Security Clearance Working Group (PCLWG) to:

- Review the processes involving Reopens and Reimbursable Suitability Investigations (RSIs) with the goal of identifying ways to minimize their requirement and eliminate the percentage of pending investigations

- Review the impact of unsubmitted reinvestigations for industry, and the degree to which they impact the timeliness of the submission of clearances for industry and their reciprocity across other adjudicative agencies.

- To investigate and report on the processes to measure the crossover actions, including suitability, between the collateral and SCI communities

2) The ODNI, through the Performance Accountability Council (PAC) will provide the NISPPAC the results of its annual reporting under the Intelligence authorization Act of 2012, with emphasis on the impact to industry.

3) The DOE agreed to report on the reciprocity of its polygraph examinations across the Intelligence Community and other federal entities, as well as to provide ISOO with a copy of the Polygraph Memorandum adopted by numerous federal agencies.

4) Industry requested that ISOO:

-Add a member of the NCMS team working JPAS issues to the PCLWG so that these issues can be addressed in a more timely and effective manner.

- Assist in facilitating actions and distributing information regarding processes and procedures relating to the effective use of RAPIDGate by Industry.

-To continue to facilitate the Special Access Program Working Group (SAPWG), with *concentration on reciprocity issues, and the status of a new SAP manual.*

5) The DSS will provide the final industry status report regarding the 32 C.F.R. Part 2001, section 2001.43(b)(2) requirement for elimination of non-GSA security containers.

6) The DoD agreed to provide feedback on their discussions with ODNI regarding their National Interest Determinations (NIDs) process approval parameters.