NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

SUMMARY MINUTES OF THE MEETING

The NISPPAC held its 43rd meeting on Wednesday, November 14, 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. Minutes of this meeting were certified on January 14, 2013.

I. Welcome and Administrative Matters

Mr. Fitzpatrick welcomed the attendees, and reminded everyone that NISPPAC meetings are recorded public events. He recognized Tony Ingenito and J.C. Dodson as the new NISPPAC industry representatives, and Dan Cardenas as the new Nuclear Regulatory Commission (NRC) representative. He also recognized Karen Duprey as the new Chair of the Industrial Security Working Group, and Fred Riccardi as the NISPPAC's new Industry Spokesperson. A list of attendees is provided in Attachment 1.

II. Old Business

Greg Pannoni, Associate Director, ISOO and the NISPPAC Designated Federal Official reviewed the six action items from the last meeting. He noted that the first action item, which would be addressed in the Personnel Security Clearance Working Group (PCLWG) report, included: (1) the identification of ways to minimize reopened and reimbursable security investigations; (2) a review of the impact of unsubmitted reinvestigations, particularly with regard to reciprocity across other adjudicating agencies; and (3) a report on the process to measure crossover actions, including suitability factors between the collateral and Sensitive Compartmented Information (SCI) communities. Item two requested that the Office of the Director of National Intelligence (ODNI) present the results of their annual reporting under the Intelligence Reform and Terrorism Prevention Act (IRTPA). Item three requested that the Department of Energy, (DOE), provide a detailed report on the reciprocity of its polygraph examinations. Item four required ISOO to address several actions of specific concern to industry: (1) that an industry member of the National Classification Management Society (NCMS) Joint Personnel Adjudication System (JPAS) Issues Team be added as a permanent member of the PCLWG; This action was completed with the appointment of Quinton Wilkes to the PCLWG; (2) concerns involving access to installations using the RAPIDGate system which the Department of the Navy (NAVY) representative will update the Committee later in the meeting ; and (3) the ad-hoc Special Access Program (SAP) Working Group reconvened so Department of Defense (DoD) could update the group on the status of the revision of the SAP Manual as well as its changes in clearance reciprocity policy. The final two action items, which will be addressed during the DoD update, concern: (1) the final report regarding industry's elimination of non-Government Services Administration (GSA) approved security containers; and (2) a report on discussions with ODNI regarding the latter's National Interest Determinations (NID) process. Action items for this meeting are provided at Attachment 2.

III. Working Group Updates

A) The PCLWG Report

Lisa Loss, Office of Personnel Management (OPM), (see presentation at Attachment 3) reviewed industry timeliness metrics relating to security clearance initiations, investigations, and adjudications, which illustrate continuing trends toward meeting the requirements of the IRTPA. She noted that there were a few exceptions, such as in the timeliness of Top Secret investigations and periodic reinvestigations (PR), which she attributed to an influx in PRs during the spring of fiscal year (FY) 2012. She observed that this surge created both a positive and a negative impact in that while more investigations were adjudicated, overall timeliness suffered. Stan Sims, Director, Defense Security Service (DSS), opined that the underlying reasons for this surge was tied to recent budgetary constraints, and that many DoD organizations held their PRs until the last minute, and then submitted them to avoid rendering their personnel ineligible for access. The Chair asked if anyone had performed an analysis of this condition so as to forecast what period of time would be affected by these budgetary constraints. Mr. Sims responded there had been analysis done, but that it was hard to track exactly where these cases originate. Drew Winneberger, DSS, added that where industry typically submitted their requests six months in advance, the advance submittal time has now been compressed to 90 days which may negatively impact the process. He also noted that some intelligence community (IC) members are now using the National Industrial Security Program (NISP) program for submitting their PRs, which was a departure from past procedures. The Chair recommended that procedures be developed to track these processes, and make proactive use of JPAS and/or the Scattered Castles databases to estimate expected submissions, as well as track pending cases. Mr. Winneberger noted that such capability already existed, and that the research mechanism could be refined to include submission and timeliness conditions. The Chair responded that while we are seeing progress in this area, we need to be able to determine how far into the future we should expect this condition to continue. Mr. Sims agreed, stating that with the addition of some dedicated manpower to search the database, this procedure could be effectively implemented. Ms. Loss added that when there is an unexpected surge that impacts the normal workflow we encounter these unintended consequences, and although this condition requires only a short time to correct, even these few days can become critical when our objective is to achieve IRTPA goals. She noted that presently there is no backlog of investigations, , aside from these PRs, submissions are on target, and reiterated that having the ability to project the workload makes the case management function more efficient.

Ms. Loss continued the discussion by noting that the August 2012 adjudication timeliness trends for Top Secret PR determinations was up because of referrals by the Defense Industrial Security Clearance Office (DISCO) to the Central Adjudication Facilities (CAFs), as part of an effort to address delinquent investigations. She stated that increases may have resulted from the impact of adjudicating these older investigations in the system. Mr. Pannoni questioned if the huge drop in Secret/Confidential adjudications between June and July might be an error. Ms. Loss responded that, she suspected it was an error and would research the figures and report back to the committee.

Laura Hickman, DISCO, (see presentation at Attachment 4) reported on industry's pending adjudications, and the reasons for case rejections in FY 2012. Regarding initial cases pending

adjudications, she reported that the year ended with over 5,300 cases of which over 2400 were over 90 days old. She explained that once an interim Secret clearance is granted to a contractor who is overseas, OPM will send DISCO an investigation without a subject interview, which cannot be fully adjudicated. So 90-95% of the 90 plus days pending cases are awaiting subject interviews. She continued, stating that the inventory of initials and PRs is down by almost half from the beginning of the FY, and DISCO expects that number to remain steady for the foreseeable future. She further noted that the case inventory for FY 2012 was reduced from over 18,000 cases at the beginning year to 9,000 at year's end. Next, she discussed FY 2012 rejection rates for Electronic Questionnaires for Investigations Processing (e-QIP) for both OPM and DISCO, explaining that while they generally show a steady decline throughout the year, DISCO nevertheless shows a slight increase in the final two months as a result of the requirement to compress PR lead time from six months to 90 days. In addition, she observed that they could reduce DISCO's e-QIP rejections by as much as 42%, if the submitting organizations would ensure that the current employer information was correct. Further, she noted that the number one reason for DISCO rejections remains missing fingerprint cards. She explained that fingerprint cards are submitted directly to OPM, and that most of them either don't get to OPM or they arrive beyond the processing time limit set by OPM, so the e-QIP is returned to DISCO. She noted that if industry would submit their fingerprint cards within the 14-day timeline, fully 61% of the rejections would be eliminated. Mr. Ingenito, Industry, asked if there was anyone looking at revising the form to negate these rejections on the e-QIP. Ms Loss, OPM, responded that these fields are already required on e-QIP, and that submitters continue to inaccurately answer questions, and yet still meet the automated validation requirements. She noted that OPM works with ODNI and DoD continuously to refine the validation process, and reminded the committee that these e-QIP rejections tend to come from the smaller companies, whereas the larger companies use central submission sites that make fewer errors.

Christy Wilder, ODNI, (see presentation at Attachment 5) provided the IC's industry performance metrics. She reminded the committee that OPM provides the metrics for approximately 94% of the executive branch agencies, while the IC provides the metrics for the remaining six percent originating in the seven major IC agencies and the 14 agencies with delegated authorities. She noted a slight increase in FY 2012 investigative timeliness, from 69 days in the third quarter to 77 days in the fourth quarter, as well as a slight increase in adjudicative time from 32 days to 41 days during the same period. In addition, she noted that five of the seven IC agencies met their adjudication goals for PRs, and that all IC agencies met their end to end timeliness goals allowing them to make up for the longer investigative time lines through the adjudicative and/or initiation phases. She noted that for initial investigations, timeliness improved in FY2012, and that the investigative agencies have met their goals for three consecutive quarters. She mentioned that in October 2012 the ODNI issued guidance that established a new goal of 114 days for Top Secret investigations, with the Secret goal remaining at 74 days. The Chair asked if industry representatives were aware of these changes, and Charles Sowell, ODNI stated that the IC community had made announcements to appropriate industry associations, and through the NISPPAC.

Ms. Wilder briefed the results from the 2011 Intelligence Authorization Act report on security clearance determinations. She pointed out that Sections A and B of the report show that even as there have been only slight increases in numbers of both Confidential/Secret and Top Secret

clearances, from 4.7 million to 4.8 million, the IC community has nevertheless revised its methodology for all security determinations, to include both individuals with access to classified information and those eligible for access. She noted that the IC understands that people may need to be granted access to classified information at anytime, so these individuals are investigated and adjudicated, in case they require access. She explained that this methodology will form the basis for historical reporting from 2011 into the future because timeliness metrics are collected on all Single Scope Background Investigations that are conducted even if they do not result in access to classified information.

Ms. Wilder highlighted issues related to crossover/reciprocity initiatives, and noted that these issues are now in development and nearing informal coordination through the Security Executive Agent Advisory Committee and that its new Security Executive Agent Directive (SEAD) 600, is expected to be published in the spring FY 2013, which updates and consolidates existing national security reciprocity policy into one document. Next, she noted that the primary objective of the IC's reciprocity pilot project was to provide a venue for reporting non-compliance with reciprocity guidelines, and observed that a website will be launched under www.ncix.gov to provide the reporting format and critical information associated with the process. Finally, she noted that the IC community is in the process of validating the PR metrics they've received from 95% of the executive branch agencies in an effort to provide a more comprehensive picture of the requirements individual agencies can provide. The Chair thanked the IC for adding this information to their presentation, and asked if there was any congressional interest being expressed on this subject. Mr. Sowell responded that the most recent inquiries were focused on unauthorized disclosures and polygraph issues.

Carl Pietchowski, DOE (see presentation at Attachment 6) reminded the committee that DOE adjudicates both its federal and contractor staff, and that as of October 2012, it had a contractor staff of almost 62,000 with a Q clearance and almost 24,000 with an L clearance. He pointed out that the preponderance of clearance actions in DOE are associated with the contractor population, with a total clearance authorization of slightly over 100,000. Rosalind Baybutt, Industry, asked if OPM performed all of DOE's investigations, and if so how were they able to complete investigations in less time than required for other executive branch agencies. Ms. Loss responded that OPM performs all DOE investigations, and that they tend to require less time due to gains made in submissions and adjudication timeliness. Mr. Pietchowski described DOE's total federal and contractor adjudications case inventory (initial Top Secret/Q and L/Secret/Confidential clearances as well as all PRs) by month, and indicated that their goal of 74 days is almost always met. Shawn Daley, Industry, asked if there were any answers to his previously posed question regarding reciprocity of polygraph testing. Mr. Pietchowski reported that DOE follows the federal standards governing polygraphs and accepts results provided by other executive branch agencies. The Chair reminded the committee that an earlier polygraph reciprocity Memorandum of Agreement (MOA) was originally signed by the18 federal agencies who operated polygraph programs, and that he was aware of an ODNI initiative to update it, and inquired as to its status. Mr. Sowell responded that a national polygraph policy is now in coordination with the National Polygraph Working Group, and would be provided for agency comment soon. He added that it is expected to produce vastly improved consolidation and standardization of polygraph policy and practices. The Chair requested the ODNI representative

to provide an update on the status of this policy at both the next working group and public meetings.

Chuck Tench, DSS (see presentation at Attachment 7) reminded the committee that all DoD components must transition to the electronic fingerprint capture and submission program by December 31, 2013. He explained that electronic capture procedures includes either the full electronic processing of fingerprints or when the prints are taken on a hard card, scanned, and then submitted electronically. He noted that the advantages of electronic submission are fewer rejects by the Federal Bureau of Investigation (FBI) and because the process requires less mail time it yields faster processing time. Also, the process affords the user increased flexibility because OPM launches the electronic submissions to the FBI immediately upon receipt, invoking a 120-day completion window as opposed to the requirement to submit the hard copy prints within 14 days of the e-Qip submittal. He added that cost was the major constraint to electronic processing because small and medium size companies find it difficult to purchase the needed capture/scan devices. He reiterated that it was DoD's intent that everyone should use the electronic fingerprinting process, whether or not they own any processing equipment. He also reminded the committee that companies only need to set up a Secure Web Fingerprint Transmission (SWFT) account, either through the DSS or the Defense Manpower Data Center (DMDC) websites (see links on slide 1 of presentation 6), to meet the requirements of the DoD mandate. He noted that DSS can assist industry in locating vendors who provide contract services to capture their fingerprints electronically. Finally, he guided the committee through a step-by-step comparison and contrast between the manual and electronic fingerprinting processes, illustrating how many fewer personnel and how much less time is required to complete the SWFT process. Additionally, he informed the committee that to date only 15% of industry has established SWFT accounts, which includes their registering of electronic fingerprint equipment. Fred Riccardi, Industry Spokesperson, asked whether the equipment registration process might become a problem, and if so, what is being done to avoid a bottleneck at the end of 2013. Mr. Sims responded, noting that this issue had been discussed by DSS and DMDC and that they were looking at ways to reduce processing times. However, he reiterated that we are in the fifth year of a five year plan to get all these actions completed, and that everyone should have procured, or be in the process of acquiring the required equipment, or be implementing another acceptable compliance mechanism to meet this requirement. He stated that DSS will continue to monitor the registration process to determine if there are additional ways it can be streamlined, and that industry must move forward to purchase equipment and get their SWFT accounts established by the deadline.

Mr. Ingenito asked if companies submitting fingerprints manually will require a SWFT account, and Mr. Tench responded that all companies will need a SWFT account to submit fingerprints. Mr. Sims noted that owning equipment to capture the fingerprint file is not a requirement, but that everyone must have a SWFT account in order to transmit them as an electronic forms template file. Finally, Ms. Loss noted that industry represents their largest population that has not transitioned entirely to the electronic fingerprint capture and submission processes, and reiterated that these processes place fewer burdens on OPM and FBI resources. The Chair requested that the working group develop a graphic that depicts the process that needs to be understood regarding electronic fingerprint submissions, and what needs to be done by December 2013. Mr. Tench responded that DSS would upload the graphic to their website when

it is completed. Finally, it was reiterated that we must stop using manual processes to submit fingerprints if we want to significantly reduce case rejection statistics.

Ms. Hickman briefed (see presentation at Attachment 8) the committee that both DISCO and the Defense Office of Hearings and Appeals adjudication functions had migrated to the DoD CAF at Fort Meade, Maryland. She noted that this collocation completes the Office of the Secretary of Defense directed consolidation of DoD CAFs, which combined the Washington Headquarters Services, Joint Chiefs of Staff, DISCO, Department of the Air Force, Department of the Army, and Navy CAFs. She described changes that directly affected industry, and explained that most related to JPAS, such as new notations indicating "adjudicated by DoD CAF" as opposed to "adjudicated by DISCO". Additionally, she noted that the international visit requests and security assurance functions will remain with DSS and that the DoD CAF will migrate to the DoD enterprise e-mail system.

B) The C&AWG Report

Mr. Randy Riley, DSS, (see presentation at Attachment 9) reminded the committee that DSS is responsible for approving contractor information systems that process classified data, and that they work with industry partners to ensure that information system security controls are in place to limit the risk of compromising national security information, and to ensure adherence to NISP standards. He reviewed the security plan review results for FY 2012, and noted that there were 4,699 System Security Plans (SSP) reviewed, and that 2,479 Interim Authority to Operate (IATO) and 1,698 Straight to ATO (SATO) were issued. He reviewed the common SSP deficiencies for the same time period, noting that there were no significant changes in the top ten deficiencies list, and that SSPs with incomplete or missing attachments remain the largest single noted deficiency, and that on-site validation metrics haven't experienced significant changes. He also observed that DSS is in the process of assuming a Cyber Command Readiness Inspection (CCRI) mission which will enable approval of SIPRNET connections. Next, he explained that the top ten most common vulnerabilities remain essentially the same in terms of both magnitude and order, with unprotected security relevant objects being the most frequently encountered discrepancy. He further described the principle initiatives that the working group is addressing; such as vulnerabilities and deficiencies, the identification of potential future issues and problems, and how to implement new requirements. He noted that the working group actually does more than simply gathering and reporting metrics, and is now focusing more on new initiatives which confront industry systems and over which they must exercise control.

He cited several examples, such as the Windows 7 and 2008 server baseline standards document, the Office of Designated Approving Authority manual, the Industrial Security Field Operations process manual, and Chapter 8 of the updated National Industrial Security Program Operating Manual (NISPOM) as projects being worked by this group. He specifically described a system validation tool, the Security Content Automation Protocol (SCAP), as currently under consideration for use in assessing compliance on NISP information systems. SCAP will scan a system and provide a report that determines if that system is compliant with its predetermined settings. Finally, he reminded the committee that the timelines achieved by the C&A processes across industry are good with plans being submitted and accreditations completed.

IV. New Business

A) The Combined Industry Presentation

Mr. Riccardi began (see presentation at Attachment 10) with a review of changes in Memorandum Of Agreement Organizations leadership and security issues that impact industry. He requested that industry be kept abreast of any contemplated changes in JPAS, and explained that industry personnel working JPAS issues may have some ideas to contribute towards systemic improvements. He noted that ISOO, at industry's request, added Quinton Wilkes, a member of the NCMS/JPAS team to the PCLWG. He reported that industry had made some progress towards simplifying the RAPIDGate program, and added that Ms. Wendy Kay, Navy, was working with the Chief of the Navy Installation Command to make sure that those at the installation level understand the protocols for issuing a Common Access Card (CAC) to an industry partner, when they should either go through the RAPIDGate process, or when they should issue a 180-day non-Personal Identity of Verification (PIV) pass. Ms. Kay stressed that if any industry personnel need assistance, they should contact her office, if they need clarification and understanding of the fee structure. Next, Mr. Riccardi explained that industry is working to understand counterintelligence requirements, and to fully realize that there may indeed be different reporting requirements for reporting different types of activities, and that these reports continue to be fragmented. Industry would like to see these reports consolidated so that they don't need to consult several sources simultaneously. He expressed industry's desire to participate in the revision of the Department of Defense Form 254 (DD 254), Contract Security Classification Specification. Mr. Sims responded that DoD is in the process of updating and automating this form, and are now in the requirements generations process, and noted that even though this is a DoD product, it functions as a federal form, and that the NISPPAC, through its working group process, captured the consolidated requirements from both federal agencies and industry regarding form substance, development, and design. The Chair concurred with the suggestion, and stated that ISOO would continue to facilitate an ad hoc working group to develop changes to the DD 254. Next, Mr. Riccardi challenged the NISPPAC to avoid any gap in governance regarding SAP issues and concerns. Further, industry vigorously supports retention of the NISPOM supplement and the delivery of a SAP manual in FY 2013. He reiterated industry's concerns over changes to the Federal Acquisition Regulation (FAR) clause. The Chair responded that ISOO added both NISP and CUI representatives to its working groups so that various points of view can be represented once the comments on the FAR clause have been adjudicated. Mr. Riccardi thanked DSS personnel for their continued efforts on industry's behalf to achieve better efficiency and a sound common sense approach, especially in an environment of increased budgetary constraints. Mr. Sims added that the methodology they have adopted, that of holding both government and industry stakeholder meetings prior to bringing issues to the NISPPAC continues to effectively support finding solutions for otherwise complex issues.

B) The DoD Update

Steven Lewis, Office of the Undersecretary of Defense for Intelligence, (OUSD(I)), reminded the committee that conforming change number one which makes the NISPOM compliant with existing national policy, is awaiting final signature. This change covers the industry

implementation of Executive Order 13526, as well as a change in Chapter 10 on International Security Requirements, and specifically the implementation of the United States/United Kingdom Defense Trade Cooperation Treaty. He noted that the NISPOM rewrite has completed all pre-coordination requirements within DoD, to include migration to the current DoD format and is now entering the formal DoD coordination process. He explained that conforming change number two, which implements national standards for insider threat is progressing, with the Cognizant Security Authorities- NRC, ODNI, DoD, and DOE, along with ISOO, and the National Insider Threat Task Force determining how to apply the insider threat standards to industry. This conforming change to the NISPOM will build upon existing procedures, many of which already address the issue of insider threat from the standpoint of adverse information. He added that DoD believes it has a sound mechanism to leverage these insider threat requirements on industry, and that once the national standards are issued they will engage with the industry NISPPAC members to get feedback on implementation. Next, he updated progress on the DoD SAP manual, reminding the committee that it will be published in four volumes. The first three volumes which describe general procedures, personnel security, and physical security requirements are in the formal coordination process, and volume four, on markings, is in the pre-signature review process. He explained that once it has progressed far enough, DoD will distill the information into a NISPOM SAP manual so that there will be one NISP standard for the protection of SAP information in industry, which we will in turn share with other government SAP program participants, so that they can get a sense of what DoD is putting into its SAP manual. Next, he described DoD's streamlining of the tier review process, noting that OUSD(I) has received some excellent inputs from other DoD components and expects the end result will be the issuance of guidance on how the tier review process can leverage existing eligibility determinations, particularly in the SCI environment, and to apply those processes in granting access to SAPs. Next, he updated the Committee that industry has eliminated the use of its non-GSA approved security containers, and noted that the DSS survey, completed at the end of September 2012, validated that there were no substandard security containers in use by industry. Finally, he updated the NISPPAC on progress relating to ODNI guidance on NIDs. He reported that OUSD(I), DSS, and ODNI representatives met and developed a consensus on improved NID procedures, to include a commitment on the part of ODNI to a more formal SCI promulgation process.

V. Closing Remarks and Adjournment

The Chair reminded those assembled that the meeting was open to the public, and asked if any guests or other members wanted to pose additional comments, questions, or concerns. Recognizing none, he reviewed the action items, (see attachment # 2) to be addressed either by the formal working groups or by the full committee at the next NISPPAC meeting. He also encouraged that attendees having a special interest in any item of concern to the NISPPAC join in a working group's dialogue. Finally, he thanked all the presenters for the time and energy they had dedicated to achieving our meeting's goals. The Chair adjourned the meeting at 12:05.

Attachment #1- NISPPAC Attendees

Attachment 1
NISPPAC MEETING ATTENDEES/ABSENTEES

The following individuals were present at the November 14, 2012, NISPPAC meeting:

• John Fitzpatrick,	Information Security Oversight Office	Chairman
• Greg Pannoni,	Information Security Oversight Office	Designated Federal Officer
• Charles Sowell	Office of the Director of National Intelligence	Member
• Carl Pietchowski	Department of Energy	Member
• Stan Sims	Defense Security Service	Member
• Kimberly Baugher	Department of State	Member
• Wendy Kay	Department of the Navy	Member
• Patricia Stokes	Department of the Army	Member
• Ryan McCausland	Department of the Air Force	Member
• Anna Harrison	Department of Justice	Member
• Anthony Lougee	National Security Agency	Member
• Daniel Cardenas	Nuclear Regulatory Commission	Member
• Anthony Ingenito	Industry	Member
• Shawn Daley	Industry	Member
• Richard Graham	Industry	Member
• Frederick Riccardi	Industry	Member
• Michael Witt	Industry	Member
• Rosalind Baybutt	Industry	Member
• Steven Kipp	Industry	Member
• J.C. Dodson	Industry	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
• Kishla Braxton	Department of Commerce	Alternate
• Richard Hohman	Office of the Director of National Intelligence	Alternate
• Derrick Broussard	Department of the Navy	Alternate
• Drew Winneberger	Defense Security Service	Alternate
• Lisa Loss	Office of Personnel Management	Presenter
• Christy Wilder,	Office of the Director of National Intelligence	Presenter
• Laura Hickman	Defense Security Service	Presenter
• Charles Tench	Defense Security Service	Presenter
• Randy Riley	Defense Security Service	Presenter
• Jeff Jones	Department of the Navy	Attendee
• Karen Duprey	MOU Representative	Attendee
• Mark Rush	MOU Representative	Attendee
• Mitch Lawrence	MOU Representative	Attendee
• Vincent Jarvie	MOU Representative	Attendee
• Rhonda Peyton,	MOU Representative	Attendee

• Lisa Gearhart	Department of Defense	Attendee
• Valerie Heil	Department of Defense	Attendee
• Tracy Kindle	Defense Security Service	Attendee
• Christine Beauregard	Defense Security Service	Attendee
• Andy Kesavanathan	Defense Security Service	Attendee
• Kathy Branch	Defense Security Service	Attendee
• John Haberkern	Defense Security Service	Attendee
• Robert Harney	Industry	Attendee
• Marta Thompson	Industry	Attendee
• Dorothy Rader	Industry	Attendee
• Mary Edington,	Industry	Attendee
• Doug Hudson	Industry	Attendee
• Dan Jacobson,	Industry	Attendee
• Linda Dei	Industry	Attendee
• David Best	Information Security Oversight Office	Staff
• Robert Tringali	Information Security Oversight Office	Staff
• Joseph Taylor	Information Security Oversight Office	Staff
• Alegra Woodard	Information Security Oversight Office	Staff

The following members/alternates were not present at the November 14, 2012, NISPPAC meeting:

• Kathy Healey	National Aeronautics & Space Administration	Alternate

Attachment 2- NISPPAC Action Items

Attachment 2 - NISPPAC Action items

The following were action items identified during the meeting:

(1) The PCLWG group will assess the impact of the increased volumes of PRs on overall performance standards and timeliness, while ensuring that a backlog of PRs doesn't occur.

(2) The PCLWG will ensure a graphic is developed and disseminated that depicts what industry needs to understand in terms of electronic fingerprint submissions, and what needs to be done by December 2013.

(3) ODNI will present an overview of the security executive agent policies that are under development and how they may impact industry.

(4) ODNI will provide an overview of the updated polygraph policy and the impact of its reciprocity requirements.

(5) OUSD(I) will provide an update on the status of the conforming change to the NISPOM relating to National Insider Threat Policy, to include what the policy and guidance means and how it will impact industry.

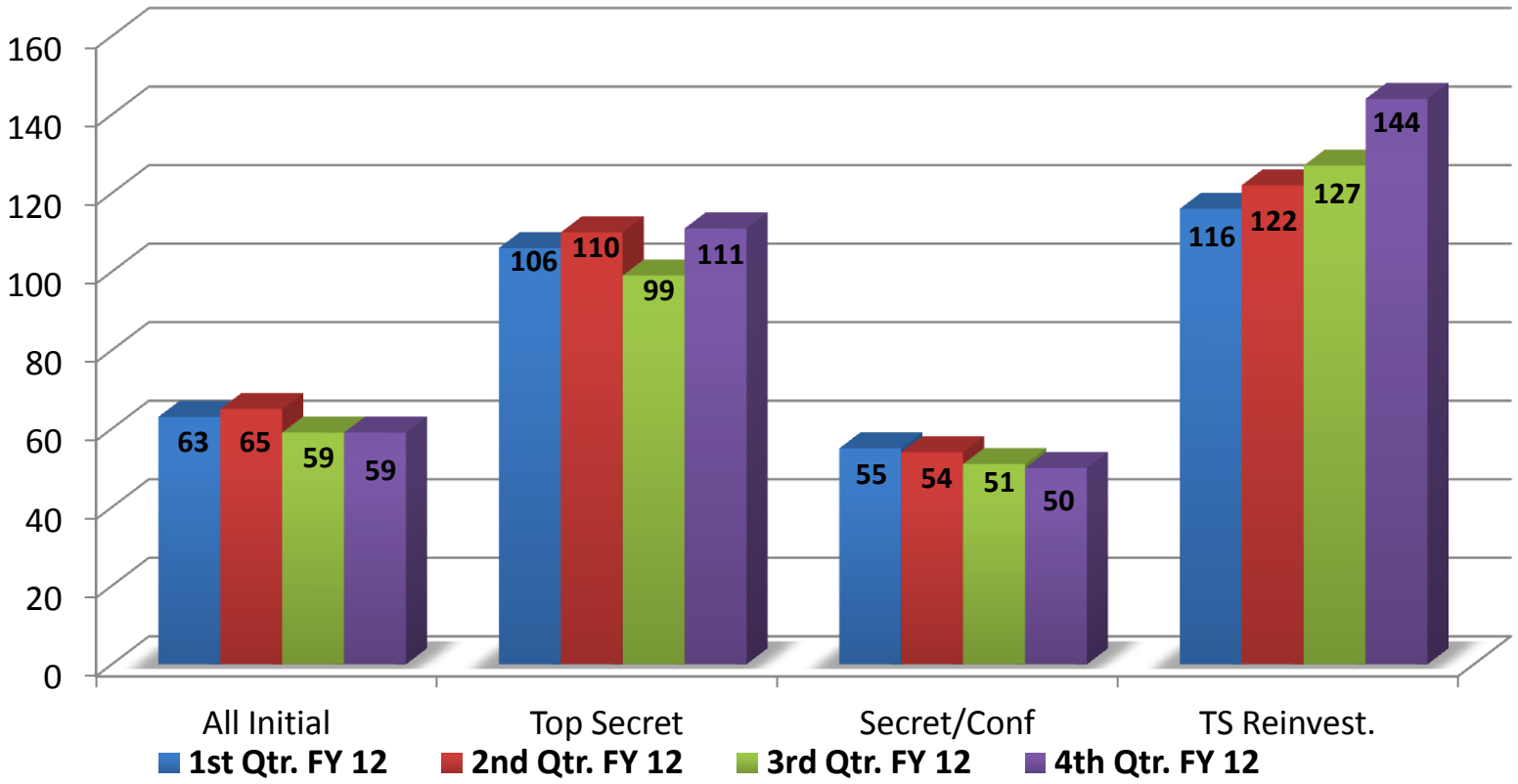
(6) ISOO will continue to facilitate an ad hoc working group to develop changes to the DD-254.

Attachment #3- OPM Presentation

a New Day for Federal Service

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

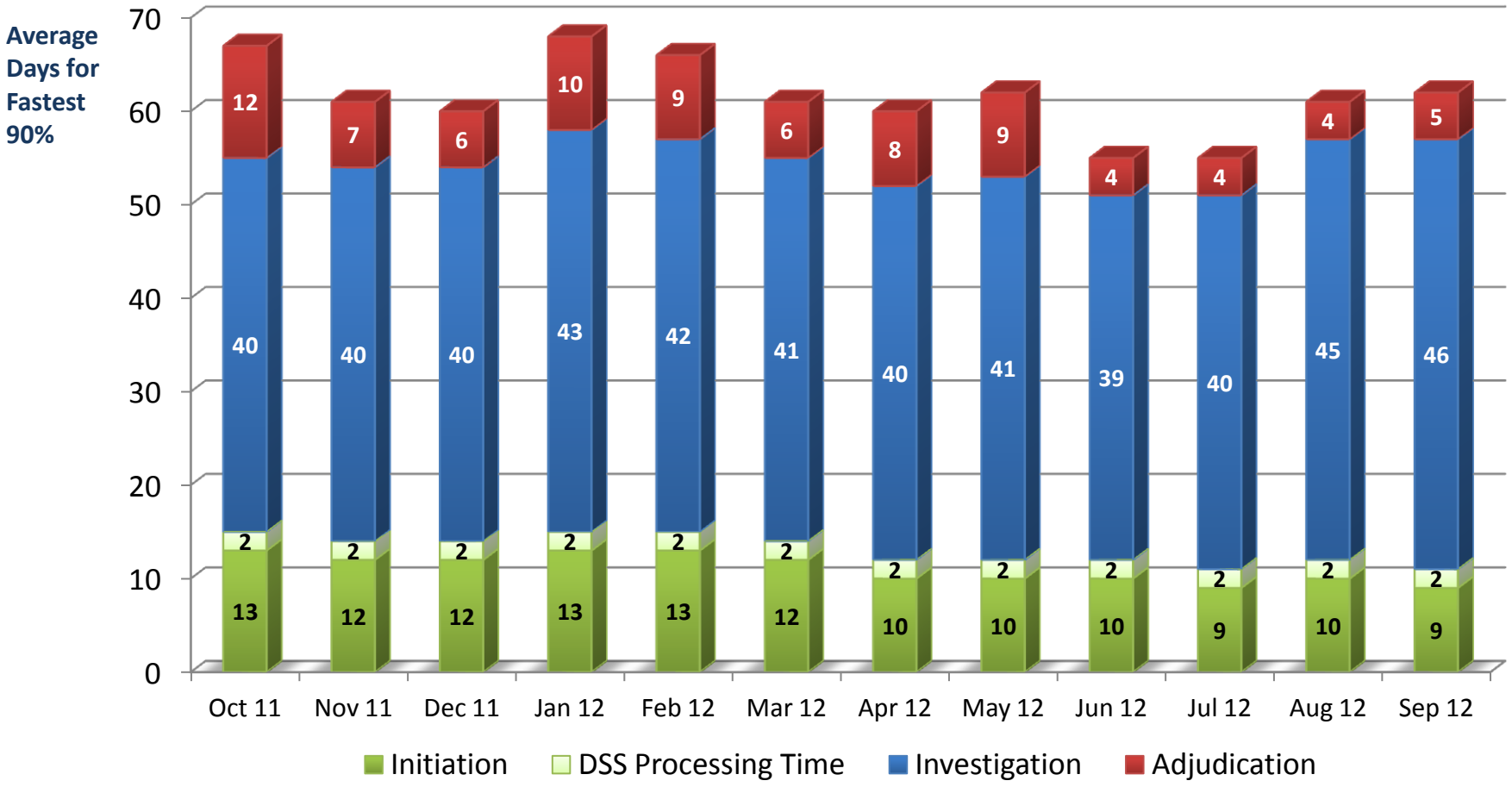
Average Days of Fastest 90% of Reported Clearance Decisions Made*



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 1st Q FY12	32,020	5,383	26,637	8,279
Adjudication actions taken – 2nd Q FY12	30,985	5,975	25,010	11,487
Adjudication actions taken – 3rd Q FY12	30,349	5,161	25,188	10,634
Adjudication actions taken – 4th Q FY12	26,996	4,312	22,675	12,492

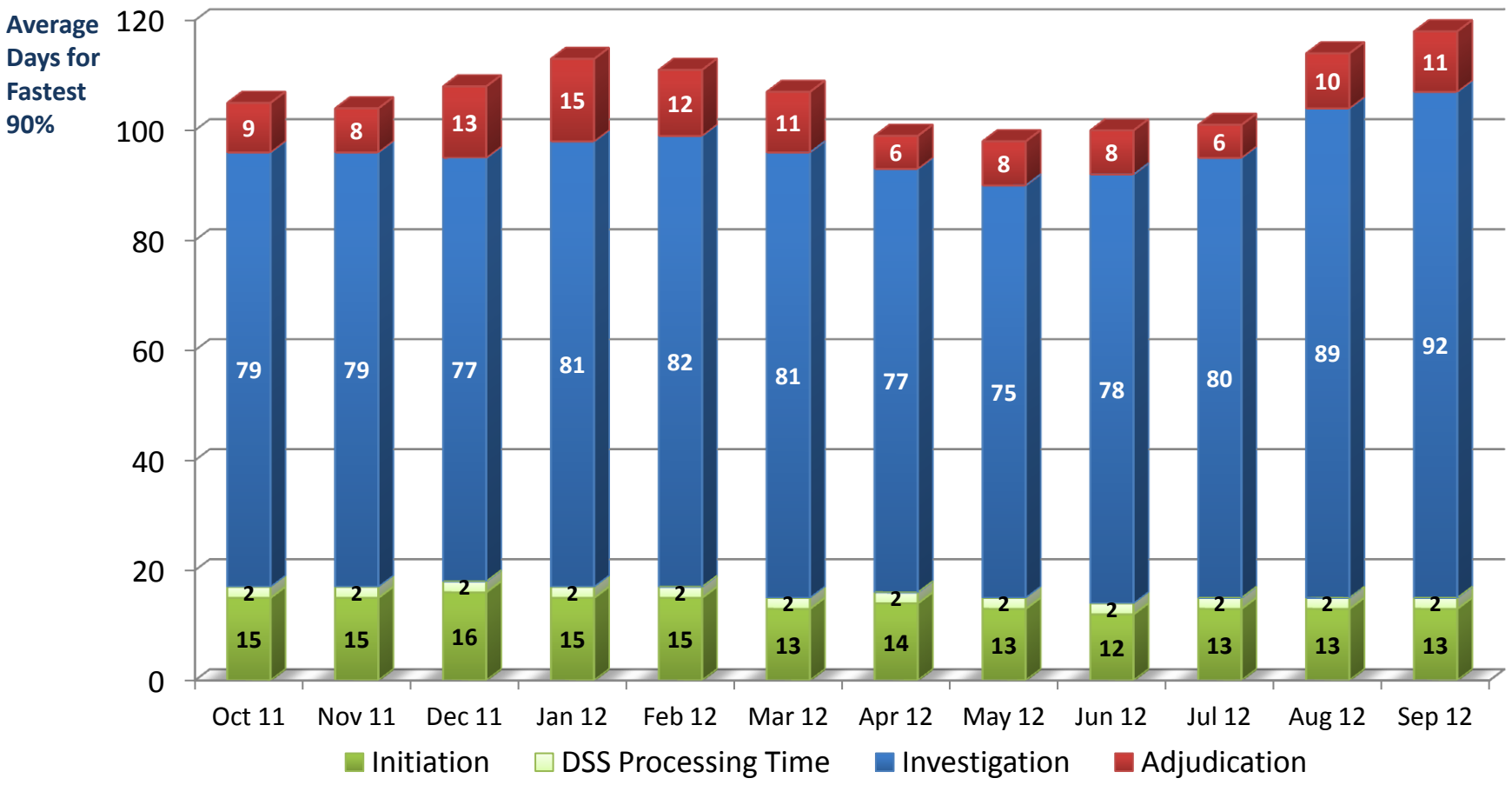
*The adjudication timeliness include collateral adjudication by DISCO and SCI adjudication by other DoD adjudication facilities

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



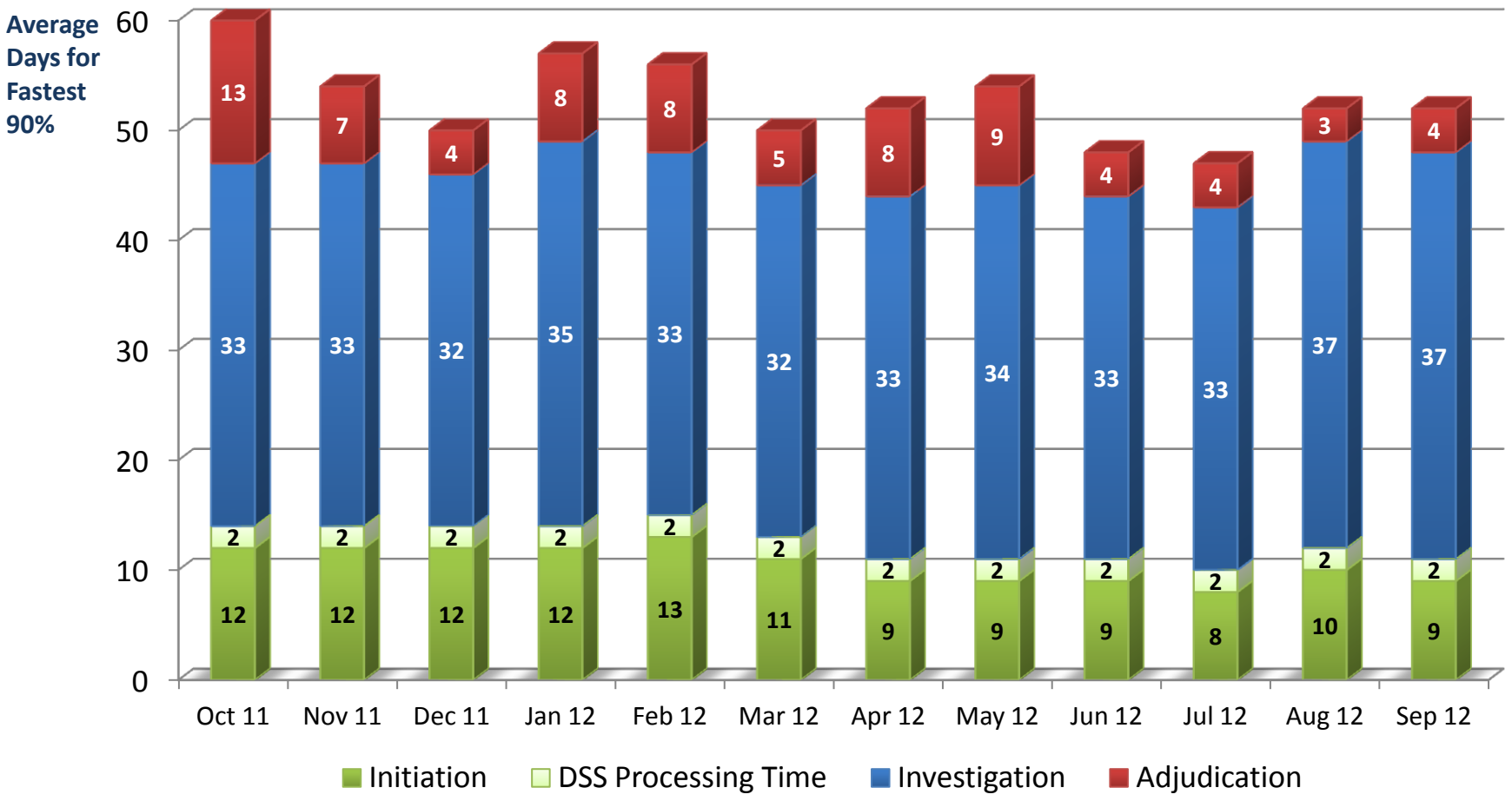
	Oct 11	Nov 11	Dec 11	Jan 12	Feb 12	Mar 12	Apr 12	May 12	Jun 12	Jul 12	Aug 12	Sep 12
100% of Reported Adjudications	12,158	9,776	10,106	10,768	8,940	10,769	8,755	10,633	10,980	4,013	10,333	8,054
Average Days for fastest 90%	67 days	61 days	60 days	68 days	66 days	61 days	60 days	62 days	55 days	55 days	61 days	62 days

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



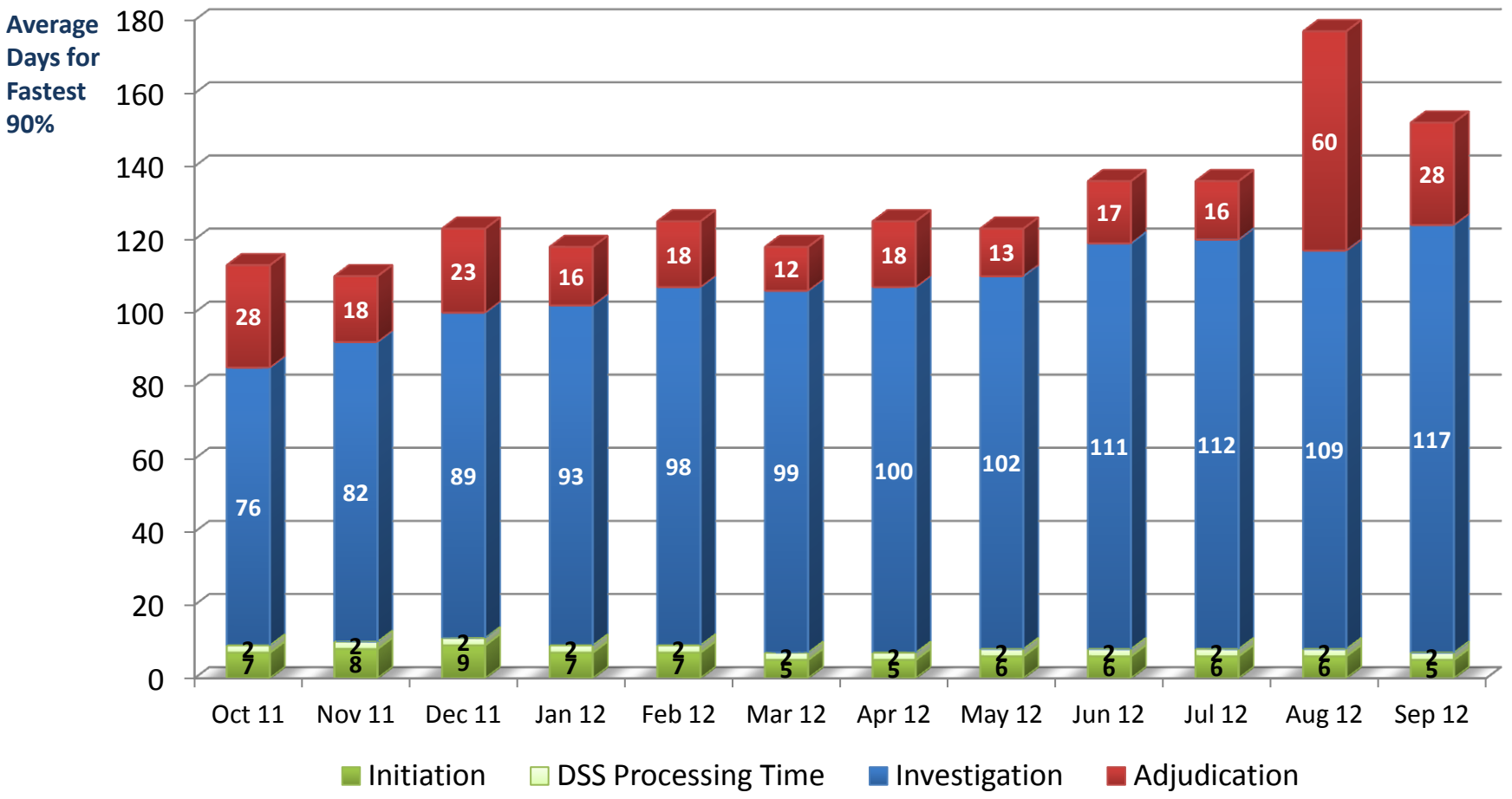
	Oct 11	Nov 11	Dec 11	Jan 12	Feb 12	Mar 12	Apr 12	May 12	Jun 12	Jul 12	Aug 12	Sep 12
100% of Reported Adjudications	2,035	1,514	1,837	2,077	1,688	2,099	1,519	2,023	1,625	595	1,573	1,420
Average Days for fastest 90%	105 days	104 days	108 days	113 days	111 days	107 days	99 days	98 days	100 days	101 days	114 days	118 days

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



	Oct 11	Nov 11	Dec 11	Jan 12	Feb 12	Mar 12	Apr 12	May 12	Jun 12	Jul 12	Aug 12	Sep 12
100% of Reported Adjudications	10,123	8,262	8,269	8,691	7,252	8,670	7,236	8,610	9,355	3,418	8,760	6,634
Average Days for fastest 90%	60 days	54 days	50 days	57 days	56 days	50 days	52 days	54 days	48 days	47 days	52 days	52 days

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



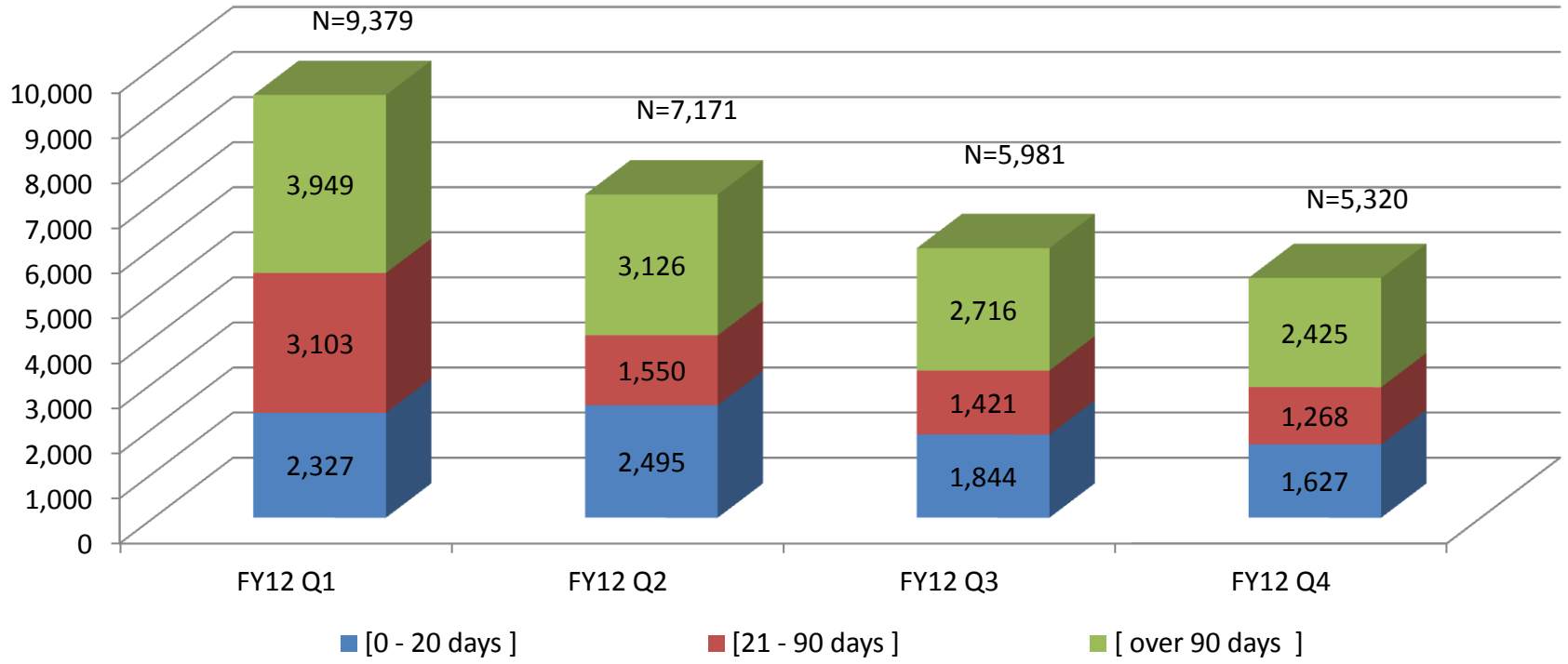
	Oct 11	Nov 11	Dec 11	Jan 12	Feb 12	Mar 12	Apr 12	May 12	Jun 12	Jul 12	Aug 12	Sep 12
100% of Reported Adjudications	3,278	2,046	2,958	4,276	2,726	4,087	2,813	3,841	3,988	3,053	4,678	3,024
Average Days for fastest 90%	113 days	110 days	123 days	118 days	125 days	118 days	125 days	123 days	136 days	136 days	177 days	152 days

Attachment #4- DISCO PCL Presentation

Defense Industrial Security Clearance Office

FY12 Initial Pending Adjudications

Initial (SSBI and NACLC)

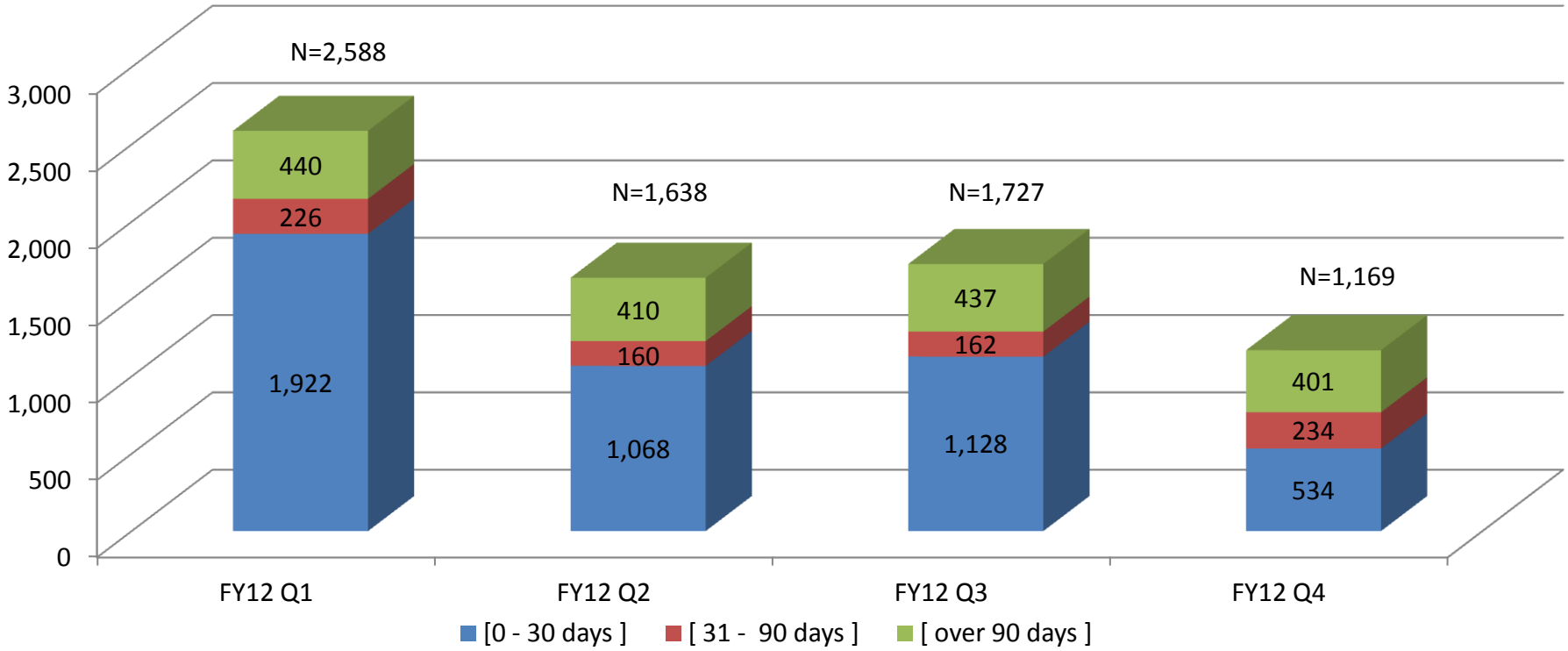


Case Type	Day Category	FY12 Q1	FY12 Q2	FY12 Q3	FY12 Q4
Initial (SSBI and NACLC)	[0 - 20 days]	2,327	2,495	1,844	1,627
	[21 - 90 days]	3,103	1,550	1,421	1,268
	[over 90 days]	3,949	3,126	2,716	2,425
Initial Total		**9,379**	**7,171**	**5,981**	**5,320**

Does not include cases with no investigation closed date

FY12 Renewal Pending Adjudications

Renewal (PPR and SBPR)

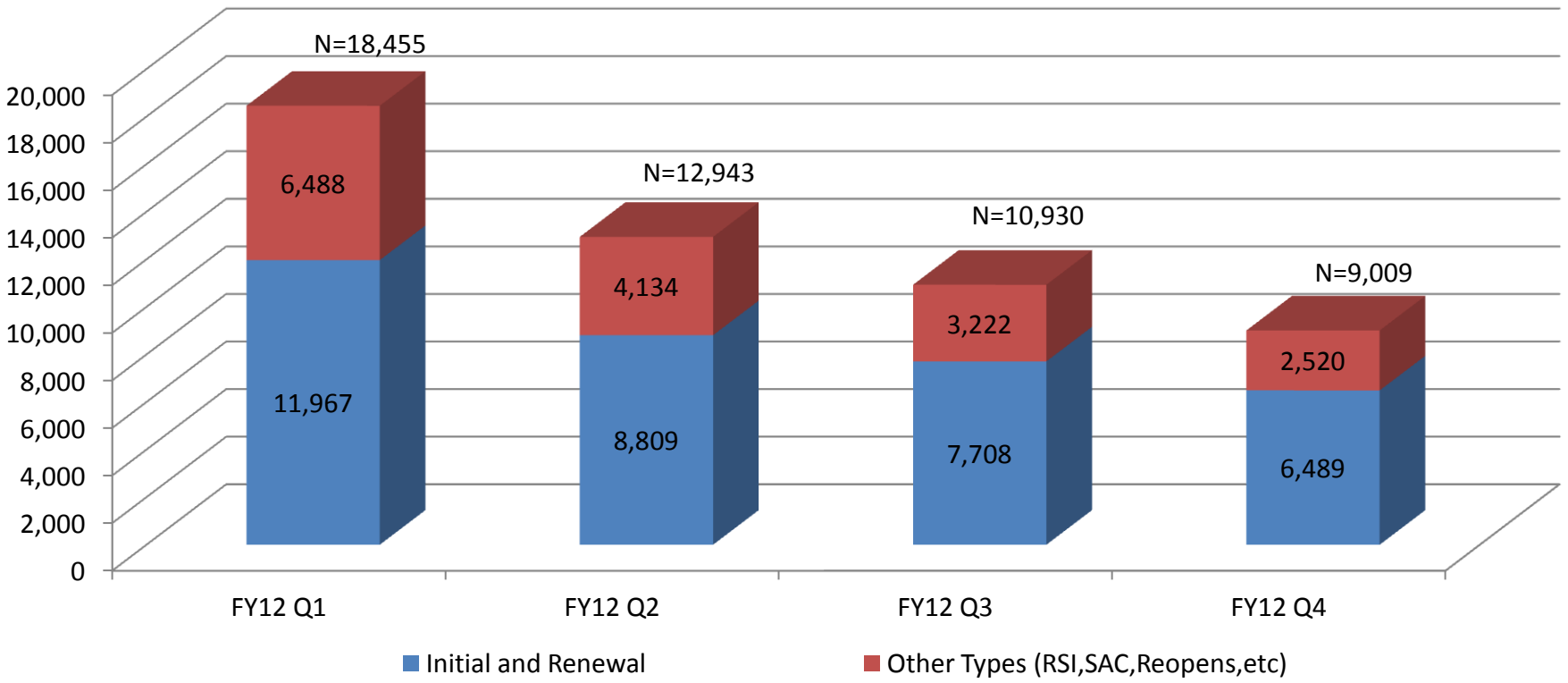


Case Type	Day Category	FY12 Q1	FY12 Q2	FY12 Q3	FY12 Q4
Renewal (SBPR and PPR)	[0 - 30 days]	1,922	1,068	1,128	534
	[31 - 90 days]	226	160	162	234
	[over 90 days]	440	410	437	401
Renewal Total		**2,588**	**1,638**	**1,727**	**1,169**

Does not include cases with no investigation closed date

FY12 Overall Pending Adjudications

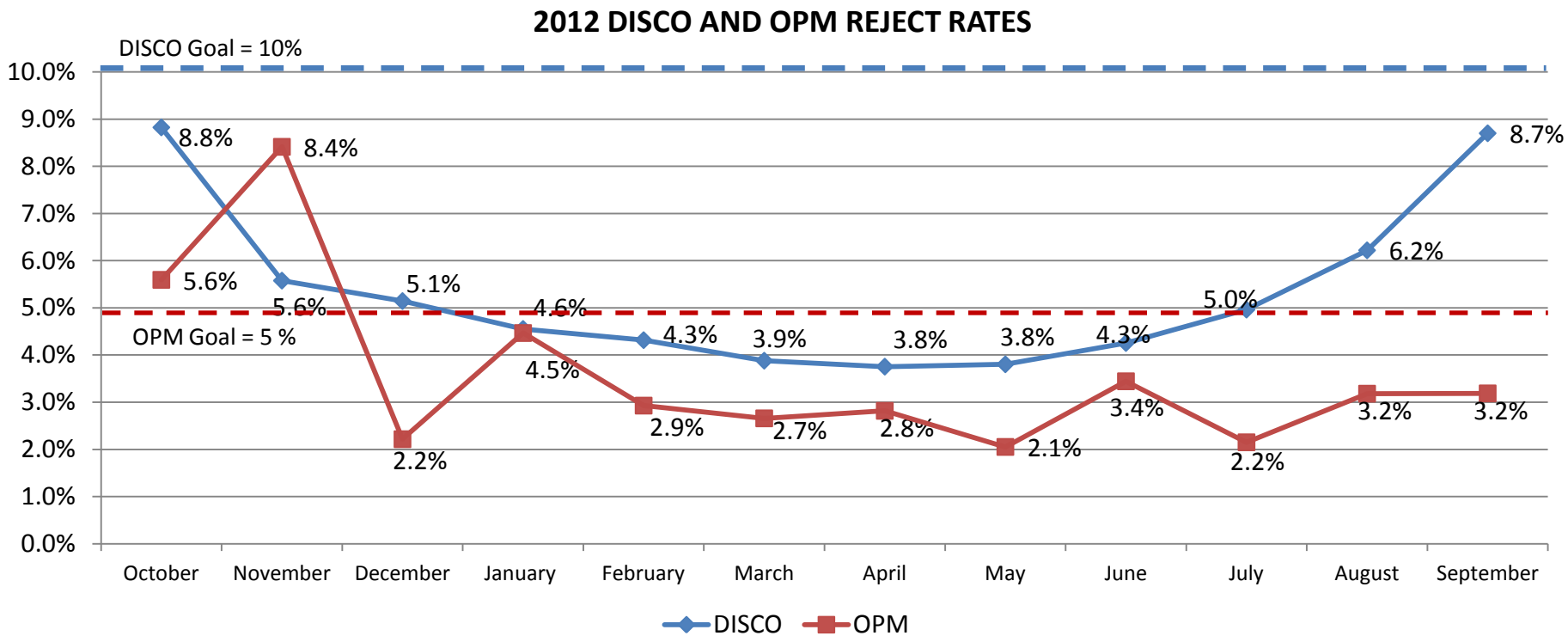
SSBI / NACLC / TSPR / Other (Suspended Cases)



Case Type	FY12 Q1	FY12 Q2	FY12 Q3	FY12 Q4
Initial and Renewal	11,967	8,809	7,708	6,489
Other (RSI, SAC, Positions of Trust, etc)	6,488	4,134	3,222	2,520
Total	**18,455**	**12,943**	**10,930**	**9,009**

Does not include cases with no investigation closed date

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 184,913 investigation requests
  - Rejects – DISCO rejected 10,068 (5.2% on average) investigation requests for FSO re-submittal

- FY12 - OPM Received 196,733 investigation requests
  - Rejects – OPM rejected 7,060 (3.5% on average) investigation requests to DISCO (then FSO) for re-submittal
  - 51% of rejections - Unacceptable fingerprint cards and fingerprint cards not submitted within timeframe

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

TOP 10 REASONS FOR DISCO REJECTION OF INVESTIGATION REQUESTS		
REASONS	**COUNT**	**PERCENT**
Missing employment information (submitting organization)	1,126	42%
Missing social security number of spouse or co-habitant	373	14%
Missing relative information	320	12%
Missing Selective Service registration information	231	9%
Incomplete information concerning debts or bankruptcy	208	8%
Missing education reference information	191	6%
Missing employment reference information	93	3%
Incomplete explanation of employment record	70	2%
ID Number Discrepancy	51	1%
Missing personal references	35	1%
Total	**2,698**	**98%**

- 68% are attributable to missing current employment activity and family member or co-habitant information
- Top 10 reasons account for 98% of DISCO's case rejections

Source: JPAS/e-QIP

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

TOP 10 REASONS FOR OPM REJECTION OF INVESTIGATION REQUESTS		
REASONS	**COUNT**	**PERCENT**
Fingerprint card not submitted within required timeframe (14 days)	862	61%
Certification / Release forms illegible	243	17%
Certification / Release forms not meeting date requirements	96	7%
Discrepancy with applicant's place of birth and date of birth	88	6%
Missing Initials on Signature Page	23	2%
Missing personal references	21	1%
Discrepancy of e-QIP Request ID Number on certificate/release forms	10	1%
Missing Certificate/Release forms	10	1%
Missing employment information	9	1%
Missing social security number of spouse or co-habitant	8	1%
Total	**1,370**	**98%**

- Top 10 reasons account for 98% of OPM's case rejections

Source: JPAS/e-QIP

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

Month	Facility Category						
	A	AA	B	C	D	E	Others
October	0.8%	0.4%	0.5%	1.7%	4.4%	8.2%	0.0%
November	0.5%	0.2%	0.2%	0.8%	2.4%	4.4%	0.0%
December	0.5%	0.2%	0.3%	0.8%	2.4%	4.5%	0.1%
January	0.3%	0.2%	0.3%	0.5%	2.3%	4.5%	0.0%
February	0.4%	0.3%	0.2%	0.8%	2.4%	4.3%	0.0%
March	0.3%	0.3%	0.2%	0.7%	2.3%	4.2%	0.0%
April	0.3%	0.2%	0.3%	0.7%	2.1%	3.6%	0.0%
May	0.3%	0.3%	0.4%	0.6%	1.8%	4.0%	0.1%
June	0.2%	0.2%	0.2%	0.6%	1.9%	3.7%	0.1%
July	0.2%	0.2%	0.4%	0.5%	2.3%	3.9%	0.0%
August	0.2%	0.2%	0.4%	0.6%	2.1%	4.5%	0.0%
September	0.1%	0.1%	0.1%	0.5%	1.4%	2.9%	0.0%
Grand Total	**4.0%**	**2.6%**	**3.7%**	**8.9%**	**27.7%**	**52.7%**	**0.4%**

DISCO Case Rejections

80.4% of cases rejected by DISCO originate from smaller Category D and E facilities

Source: JPAS/e-QIP

Defense Security Service

Summary and Takeaways:

- IRTPA
  - DISCO continues to exceed IRTPA timelines (avg 8 days)
  - DISCO case inventory is at a very healthy level (~10K)
- e-QIP Rejects Decrease
  - Significant reduction since 2010 version of SF86 implemented
    - Slight increase in Sep 12 due to PR 90 day change.
  - Missing employment information still #1 DISCO reject: submitting company needs to be listed as current employer
  - Fingerprints not submitted w/in 14 days still #1 OPM reject: submit fingerprints immediately; go electronic as soon as possible

Attachment #5- ODNI PCL Presentation

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

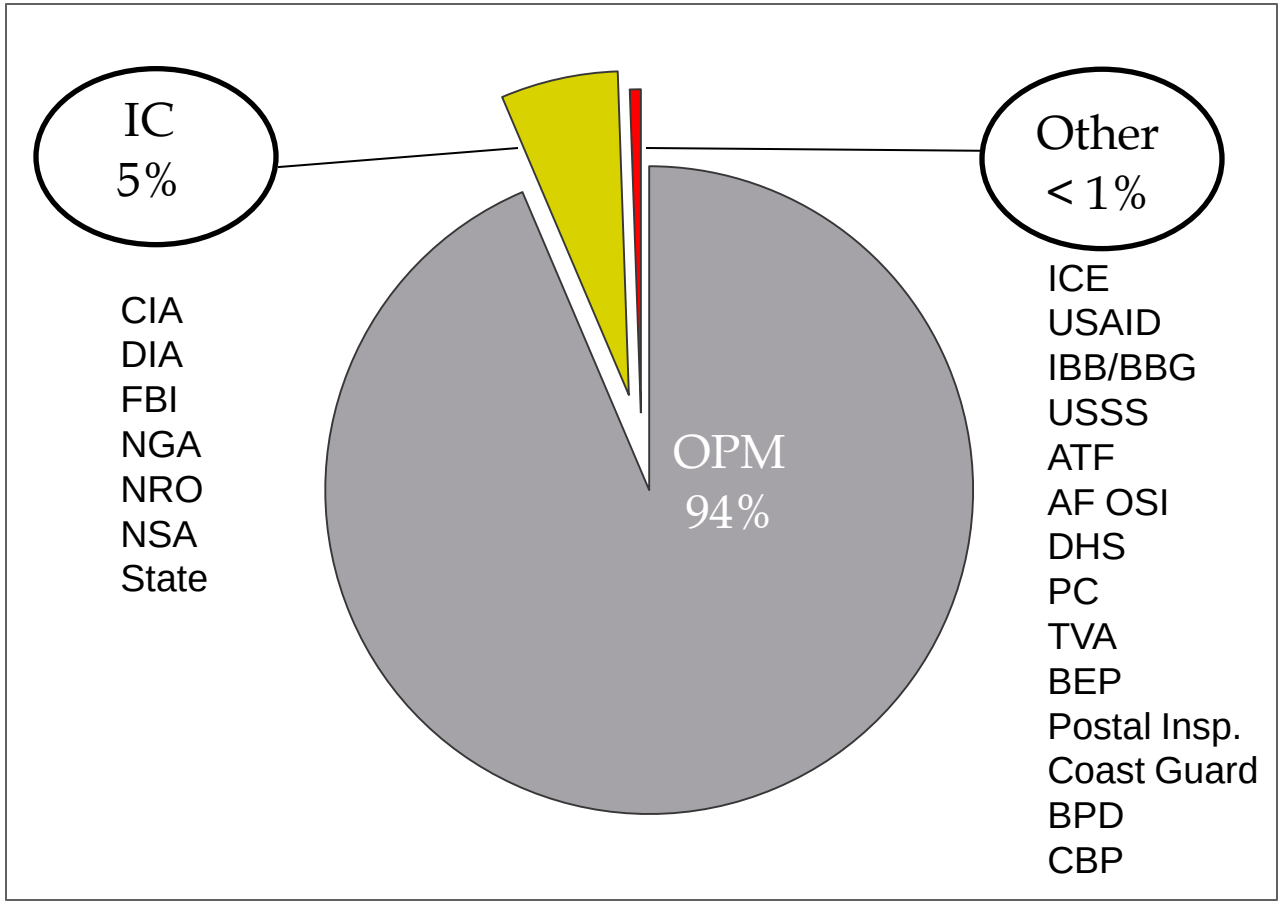
Industry Performance Metrics

ONCIX/Special Security Directorate

LEADING INTELLIGENCE INTEGRATION

NISPPAC/PCL Working Group
7 November 2012

Overall Volume by ISP



Intelligence Community Timeliness for Industry

7 IC agencies report metrics as delegated ISPs (5% of USG workload)

- Initials
  - Slight increase in investigative time from 69 days in FY12 Q3 to 77 days in FY12 Q4
  - Slight increase in adjudicative time from 32 days in FY12 Q3 to 41 days in FY12 Q4
- Periodic Reinvestigations
  - Adjudication Phase: 5 IC agencies met the 30-day goal
  - End to end: All agencies met the goal of 150 days

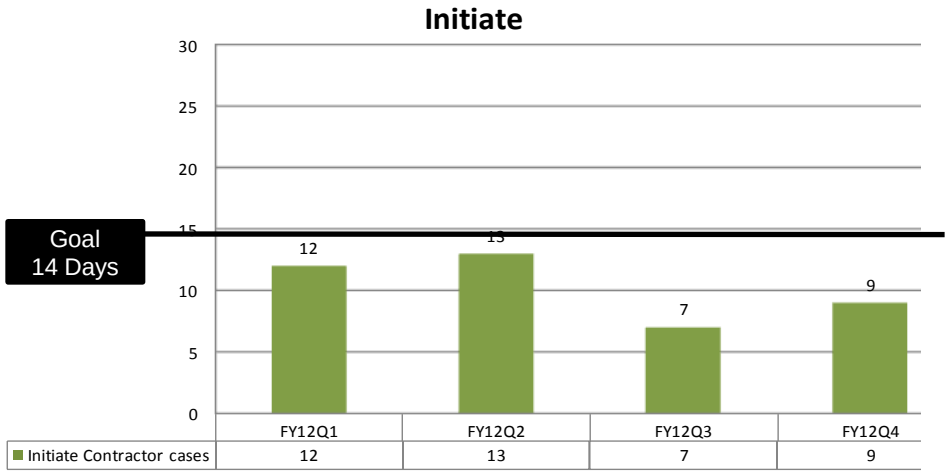
Revised TS Goal metrics will provide additional insight to agency performance

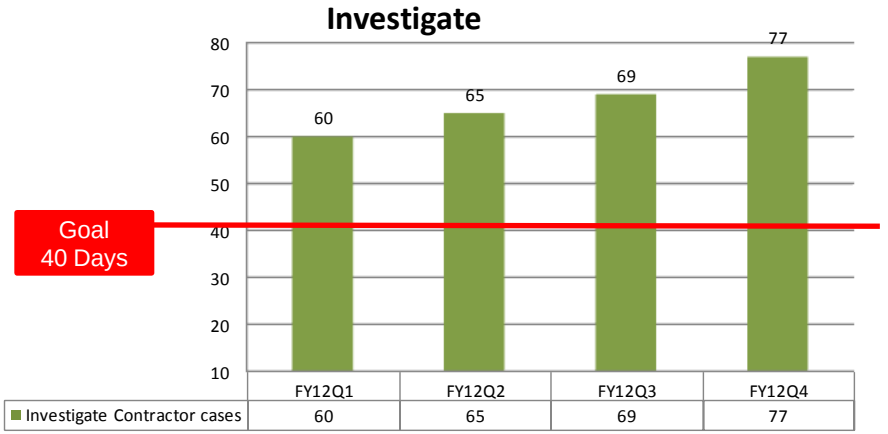
Other Delegated Investigative Service Provider's (ISP) Timeliness for Industry

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 – Timeliness has steadily improved from FY12 Q1 to Q4. Investigative timeliness goal was met in FY12 Q4
- Periodic Reinvestigations –Agencies have met goal three quarters in a row

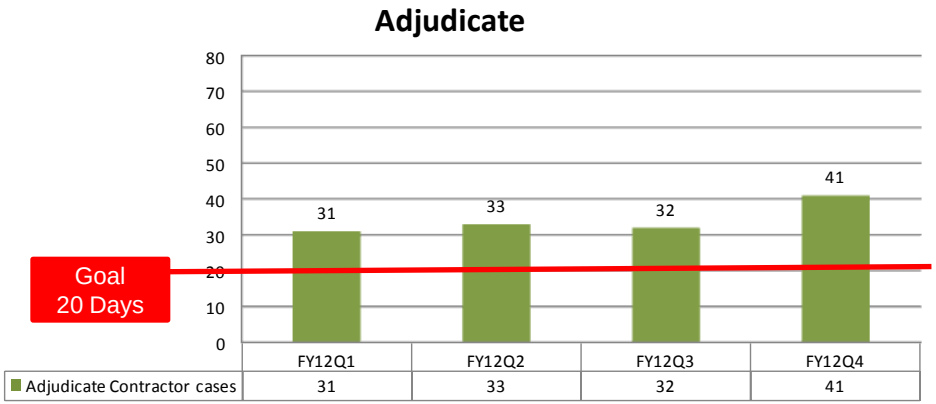
Intelligence Community
Combined Top Secret and Secret Initials
(5% of USG Workload)





Timeliness:

for Contractors



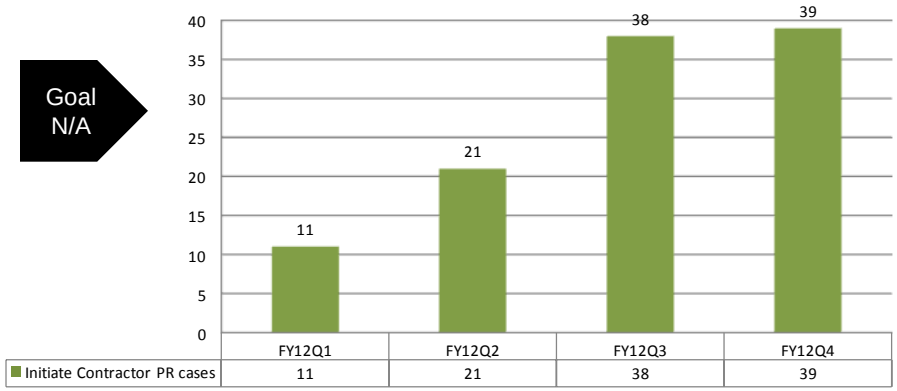
Intelligence Community

Combined Top Secret and Secret Periodic Reinvestigations

(5% of USG Workload)

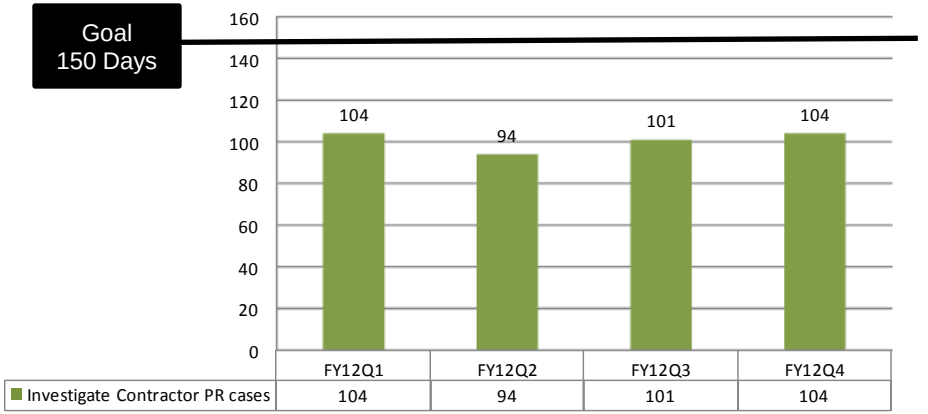
Initiate

Goal N/A



Investigate

Goal 150 Days

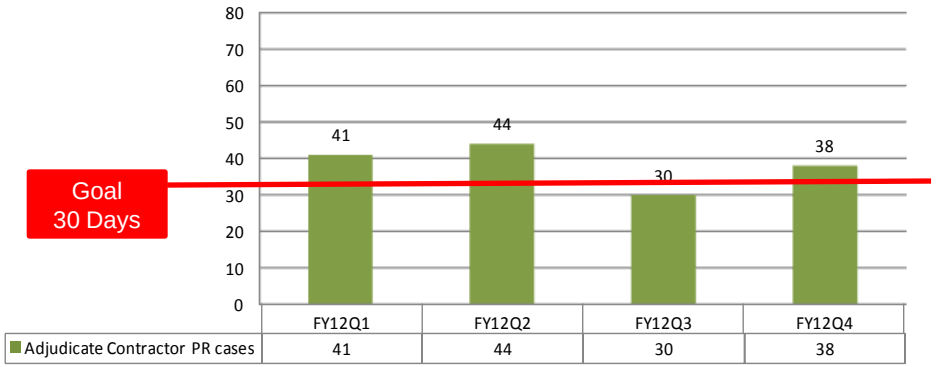


Timeliness:

for Contractors

Adjudicate

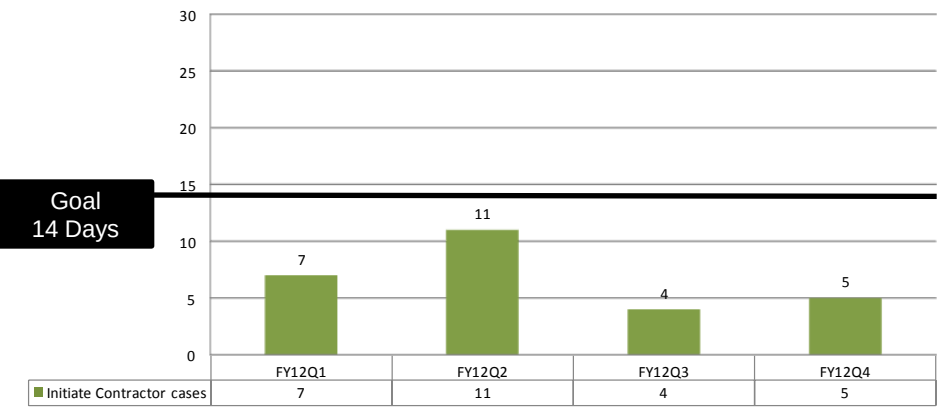
Goal 30 Days



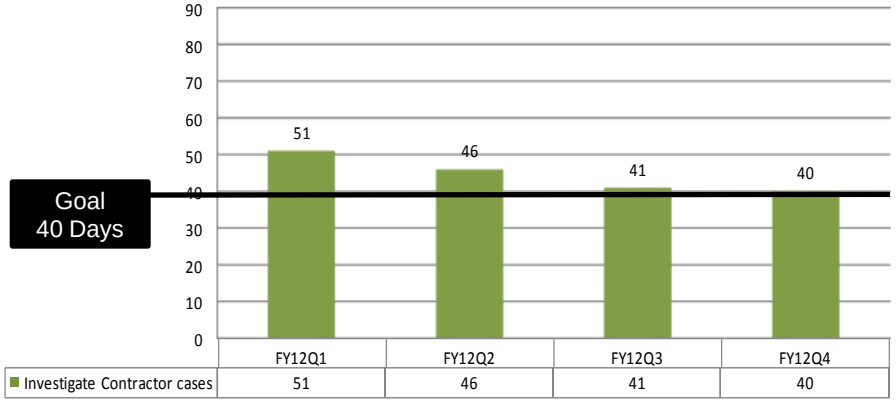
Other Delegated

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

Initiate



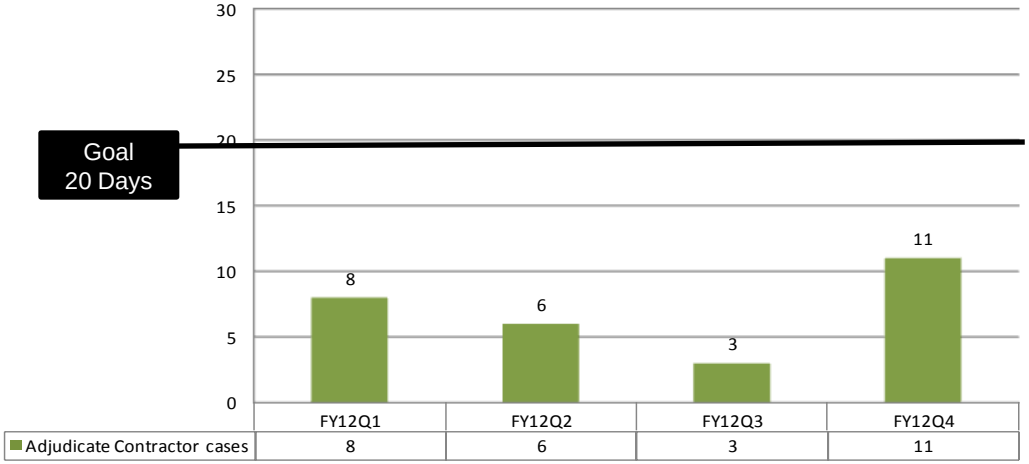
Investigate



Timeliness:

for Contractors

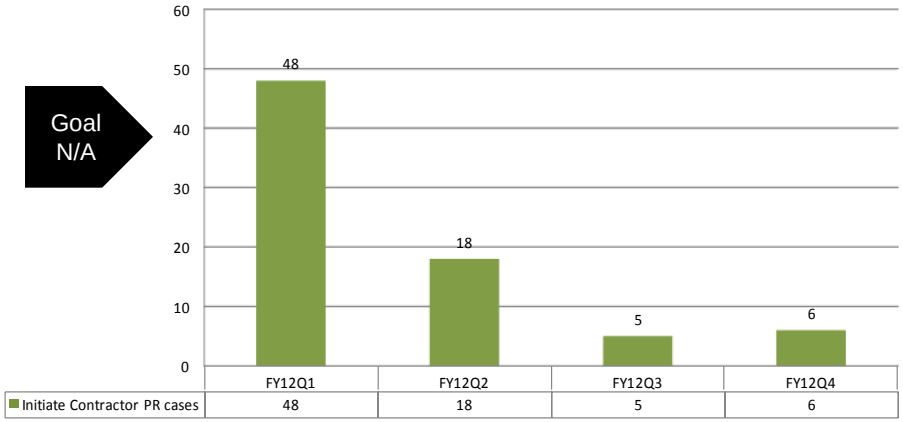
Adjudicate



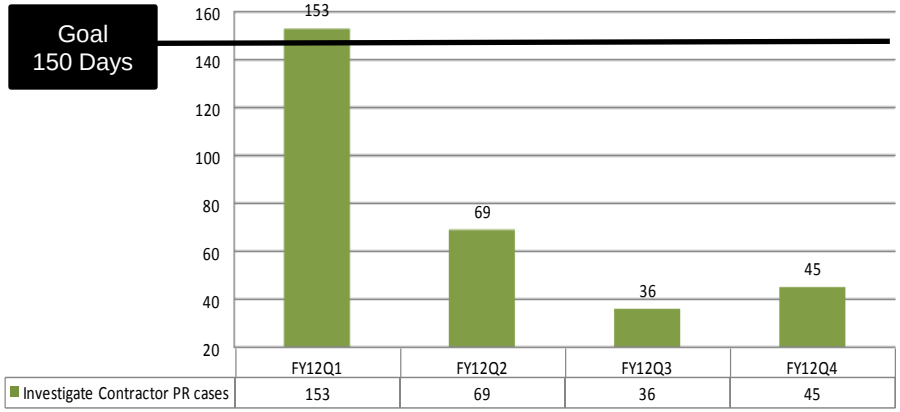
Other Delegated

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

Initiate



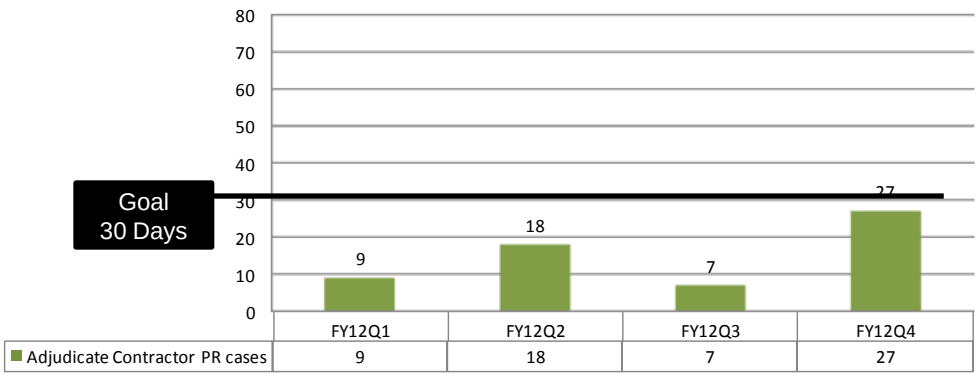
Investigate



Timeliness:

for Contractors

Adjudicate



2011 Intelligence Authorization Act Report on Security Clearance Determinations

Held a security clearance at such level as of 10/1/2011

Held a security clearance at such level:

Employee Type	As of 10/1/10: Conf/Secret	As of 10/1/10: Top Secret	As of 10/1/11: Conf/Secret	As of 10/1/11: Top Secret
Government	2,559,014	756,672	2,693,402	766,245
Contractor	620,783	550,642	598,006	478,835
Other	91,468	129,662	161,606	165,458
Sub-Total:	3,271,265	1,436,976	3,453,014	1,410,538
Total:	4,708,241		4,863,552	

Key: New methodology

- Modified methodology
- Includes all individuals in access, in addition to those deemed eligible to hold a clearance
- Refreshed FY 2010 data based on new methodology
- More consistent with ODNI's methodology to assess timeliness metrics
- More accurate depiction of impact to resources

Approved for security clearance from 10/1/2010 to 9/30/2011

Approved for a security clearance at such level:

Employee Type	As of 10/1/10: Conf/Secret	As of 10/1/10: Top Secret	As of 10/1/11: Conf/Secret	As of 10/1/11: Top Secret
Government	512,076	130,755	400,490	178,926
Contractor			97,453	102,277
Other			42,546	29,702
Sub-Total:	512,076	130,755	540,489	310,905
Total:	642,831		851,394	

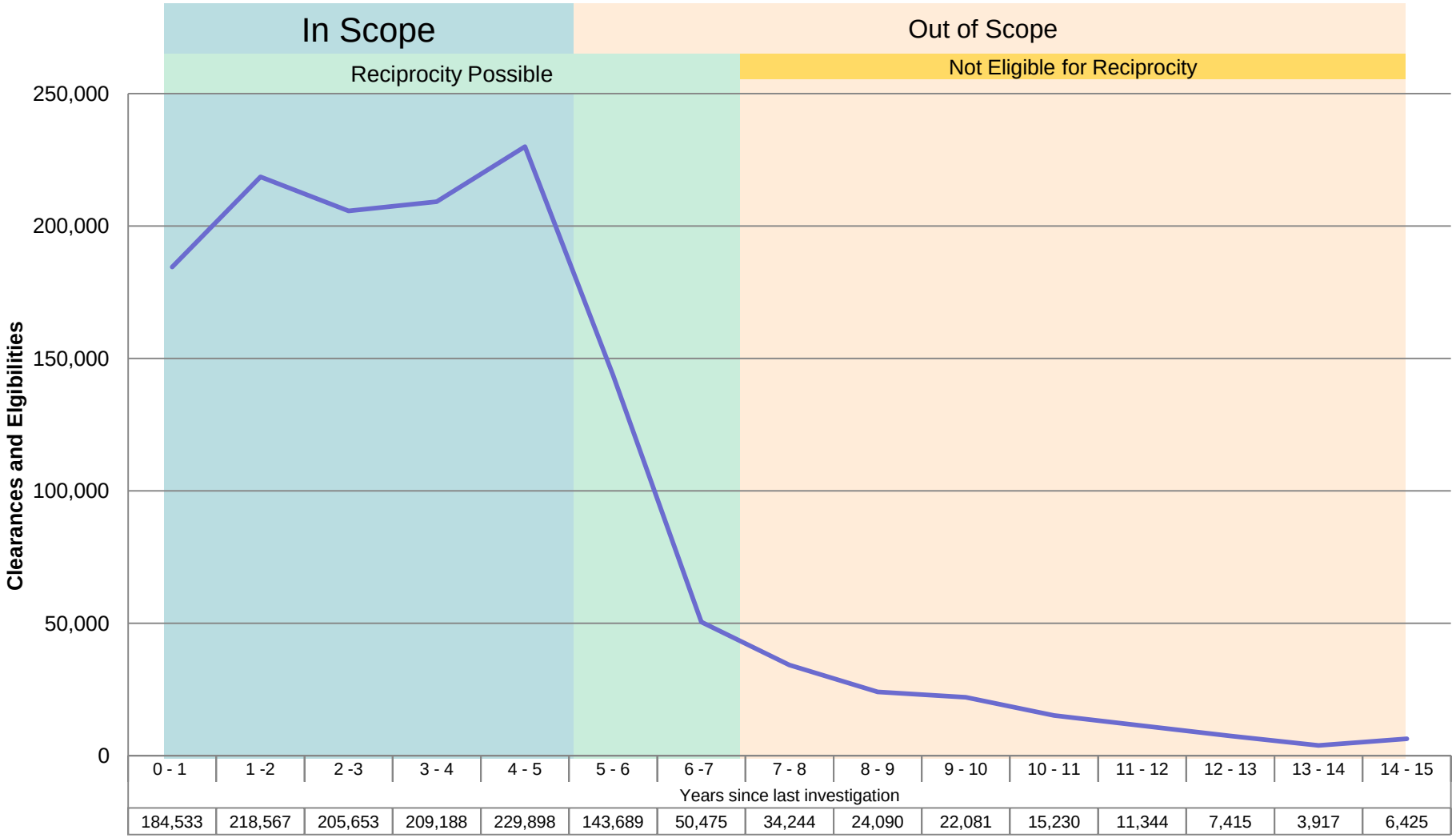
Key: Data could not be refreshed using new methodology
New methodology

- Modified methodology to include eligibility determinations
- Could not refresh FY 2010 data
- Could not distinguish between initial and PR determinations in Scattered Castles
- Does not take into account individuals that are debriefed or removed from access

Industry Crossover/Reciprocity Initiatives

- Draft SEAD 600 - National Reciprocity Policy
  - In development by SSD/PSG and preparing for informal coordination with the SecEA Advisory Committee;
  - SEAD 600 updates and consolidates existing national security reciprocity policy into one document;
  - Projected Implementation -- Spring 2013
- Reciprocity Pilot:
  - Draft Reciprocity Pilot CONOPS undergoing final internal ONCIX/SSD review and approval
  - Pilot will involve four (4) each of small, medium and large ISWG member companies
  - Pilot duration will be 90 days to test the draft ODNI web form for reporting reciprocity issues in 2013, to include:
    - Volume and frequency of reciprocity non-compliance examples
    - Accuracy of data provided via the web form
    - Usefulness of the web form data in identifying non-compliance examples
    - Usefulness of web form data in informing development of reliable metrics
    - Compilation of the most frequent reasons for reciprocity non-compliance
- ODNI Website for Reporting Reciprocity Non-Compliance:
  - ODNI server support for reporting via the web form being developed and tested
  - Upon completion of the Reciprocity Pilot, lessons learned will be incorporated into final web site design
  - Implementation of ODNI Website for reporting reciprocity non-compliance is projected for late Spring 2013
- Periodic Reinvestigation Data
  - Pulled from record repositories
  - Currently being verified by agencies

Periodic Reinvestigations – TS & SCI in IC/DoD



Attachment #6- DOE PCL Presentation

U.S. Department of Energy

Personnel Security Brief

October 2012

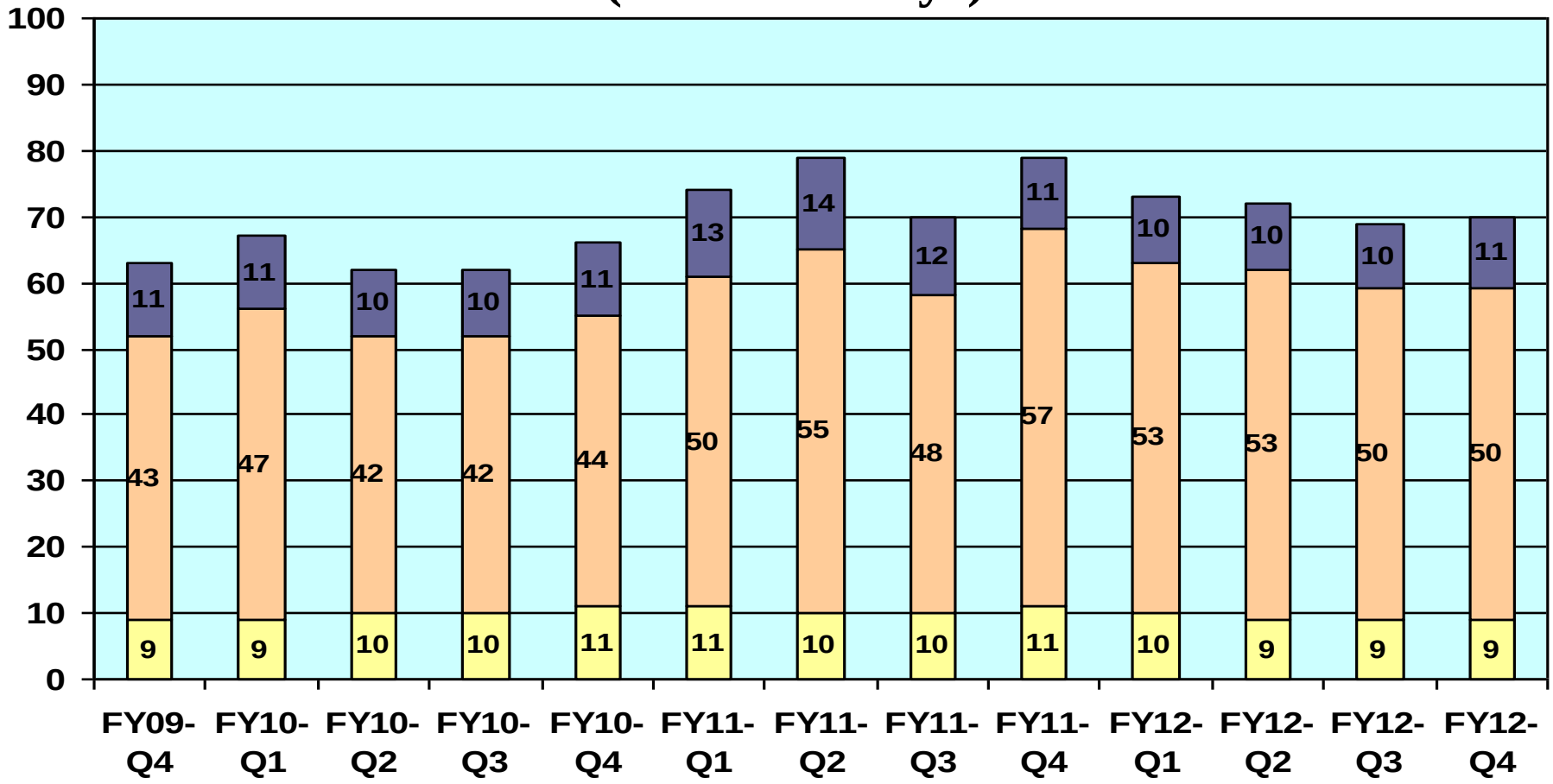
Personnel Security Overview

- DOE adjudicates both Federal and contractor staff
- Eight adjudicative facilities
- Policy, administrative review, and appeal functions centralized at Headquarters
- Cleared contractors, as of October 22, 2012:

  -61,718 Q access authorizations

  -23,543 L access authorizations
- Have met IRTPA initial security clearance adjudicative goals since April 2009

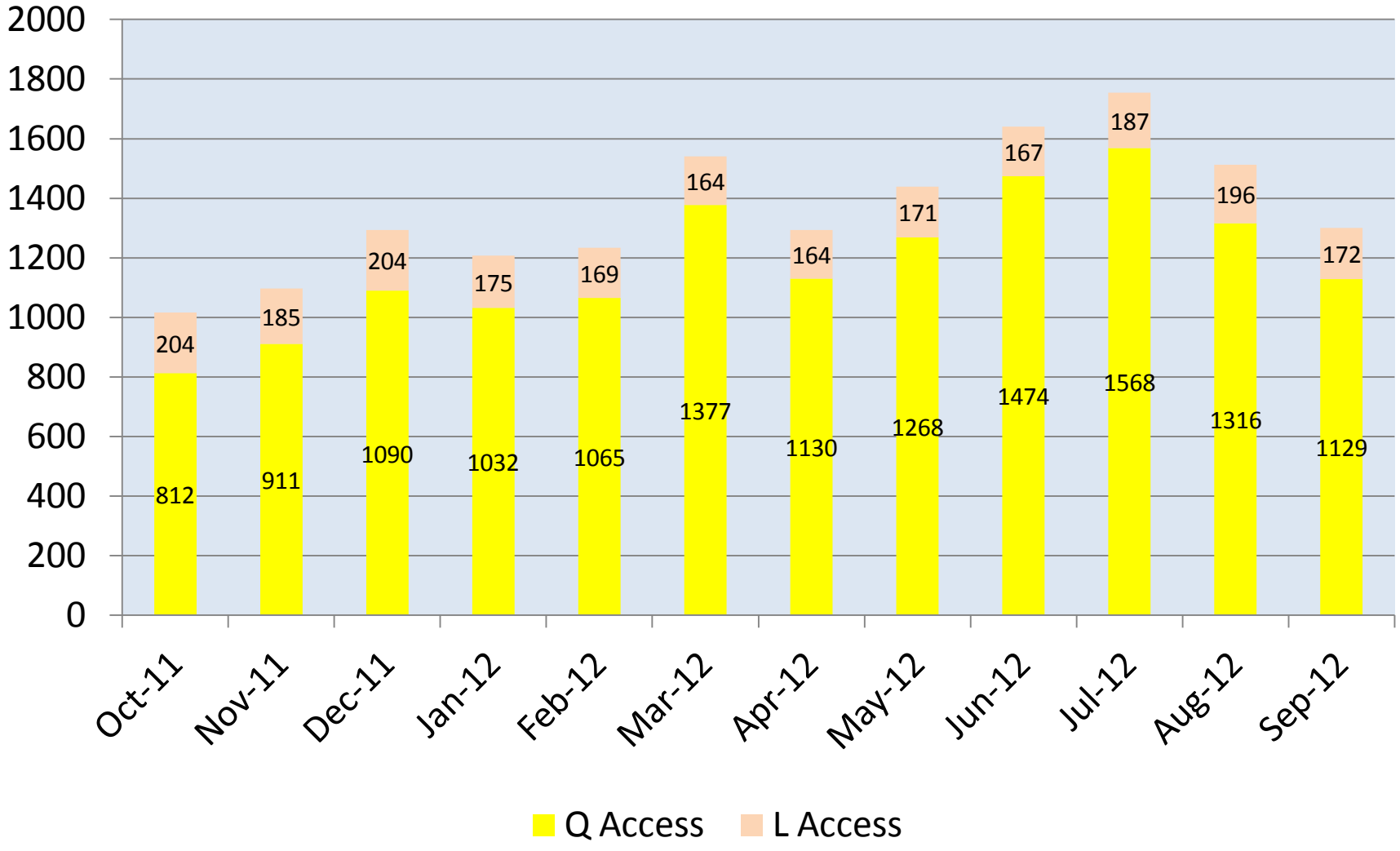
DOE's Average End-to-End Timeliness Trends for 90% Initial Q/TS and All L/S/C Security Clearances (Goal: 74 Days)



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 #7- eFP Briefing

Electronic Fingerprint Submission & Process Changes

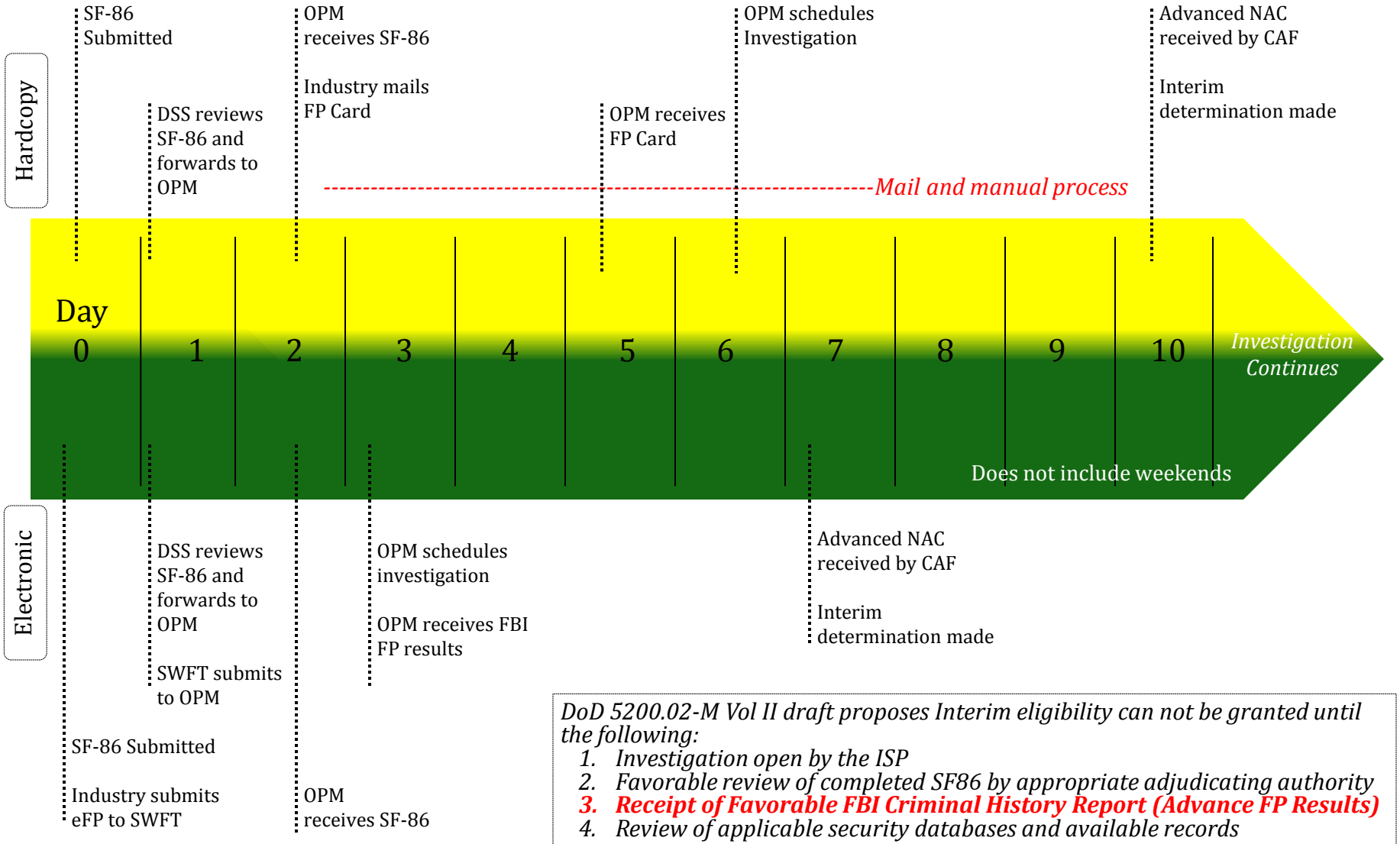
Presented By:
Chuck Tench
DSS, Planning Office
November 14, 2012

Electronic Fingerprint Submissions

- **Requirement**: All DoD components transition to electronic capture and submission of fingerprints by December 31, 2013.
- **Advantages**:
  - Less unclassifiable
  - Less mail time and faster processing
  - OPM processes e-FP upon receipt and results are valid for 120 days
    - e-QIP submission can be received within 120 days.
    - Hardcopy fingerprints must arrive at OPM within 14 days of e-QIP submission - #1 OPM reject reason for Industry
- **Constraints**: Small to Medium Companies - not feasible to purchase capture/scan devices and software ($$)
- **Solutions**:
  - DMDC – Secure Web Fingerprint Transmission (SWFT) – https://www.dmdc.osd.mil/psawebdocs
  - Military services, DoD Agencies and other (NISP) government agencies
  - Multiple OPTIONS: Companies need to start planning NOW!

NISP	Hard copy			Electronic		
FY	Total	Unclassified	%	Total	Unclassified	%
FY10	99,399	5,567	6%	9,229	456	5%
FY11	89,452	5,532	6%	10,685	392	4%
FY12	77,663	6,744	9%	14,574	446	3%

e-FP to Support Interim Clearance Process Change



DoD 5200.02-M Vol II draft proposes Interim eligibility can not be granted until the following:

1. *Investigation open by the ISP*
2. *Favorable review of completed SF86 by appropriate adjudicating authority*
3. ***Receipt of Favorable FBI Criminal History Report (Advance FP Results)***
4. *Review of applicable security databases and available records*

Attachment #8- CAF Consolidation Briefing

DoD CAF Consolidation

Defense Adjudication Activities Facility

WHS CAF	Joint Staff CAF	DISCO	DOHA Adj	Air Force CAF	Army CCF	Navy CAF

Note: DoD CAF Consolidation does not include: DIA, NGA, NRO, NSA, or DOHA- Due Process

DoD CAF Timeline

- Completed
  - 3 May: DepSecDef Directs DoD CAF Consolidation
  - 26 Aug: WHS and JCS officially became the DoD CAF
  - 26 Aug: Dan Purtill (WHS CAF Director) named acting DoD CAF Director
  - 22 Sep: DoD CAF established in JPAS
  - **21 Oct: DISCO and DOHA migrated to the DoD CAF**
  - **27 Oct: Industry migrated to DOD CAF version of JPAS**
- Estimated (subject to change)
  - 18 Nov: AF migrate to the DoD CAF
  - **8 Dec: DoD CAF teams created in JPAS. Ex: DOD CAF – Industry; DOD CAF - AF**
  - 16 Dec: Army migrate to the DoD CAF
  - 27 Jan: Navy migrate to the DoD CAF
  - 30 Sep 13: Full Operating Capability (to include HSPD-12 and Suitability determinations)

Changes?

Change :

- JPAS Industry Users – effective 27 Oct 2012
  - Adjudications will show as adjudicated by the DOD CAF
  - DISCO will no longer be a selection in any of the drop-down fields
  - For RRU or Incident Report submissions select DOD CAF
    - **After 8 Dec, select DOD CAF – Industry Division A for DISCO; Industry Division B for DOHA**
  - JPAS and DSS announcements will be posted as changes occur

- International Visit Request and Security Assurance
  - Functions will move to International Branch located at DSS HQ
  - DISCO will continue to perform function until transfer: est. 15 Mar 2013

- DISCO/DoD CAF migration to DISA Enterprise email (*@mail.mil vs. dss.mil*)
  - **Date TBD**

No Change:

- No change to SON/SOI
- DoD Security Services Call Center remains the same
- Adjudication operations will continue to be performed as they are today
- DSS/Industry Working Group will continue to meet monthly
- Goal to be transparent to Industry

Attachment 9- ODAA C&A Presentation

NISPPAC C&A Working Group Update for the Committee

October 2012

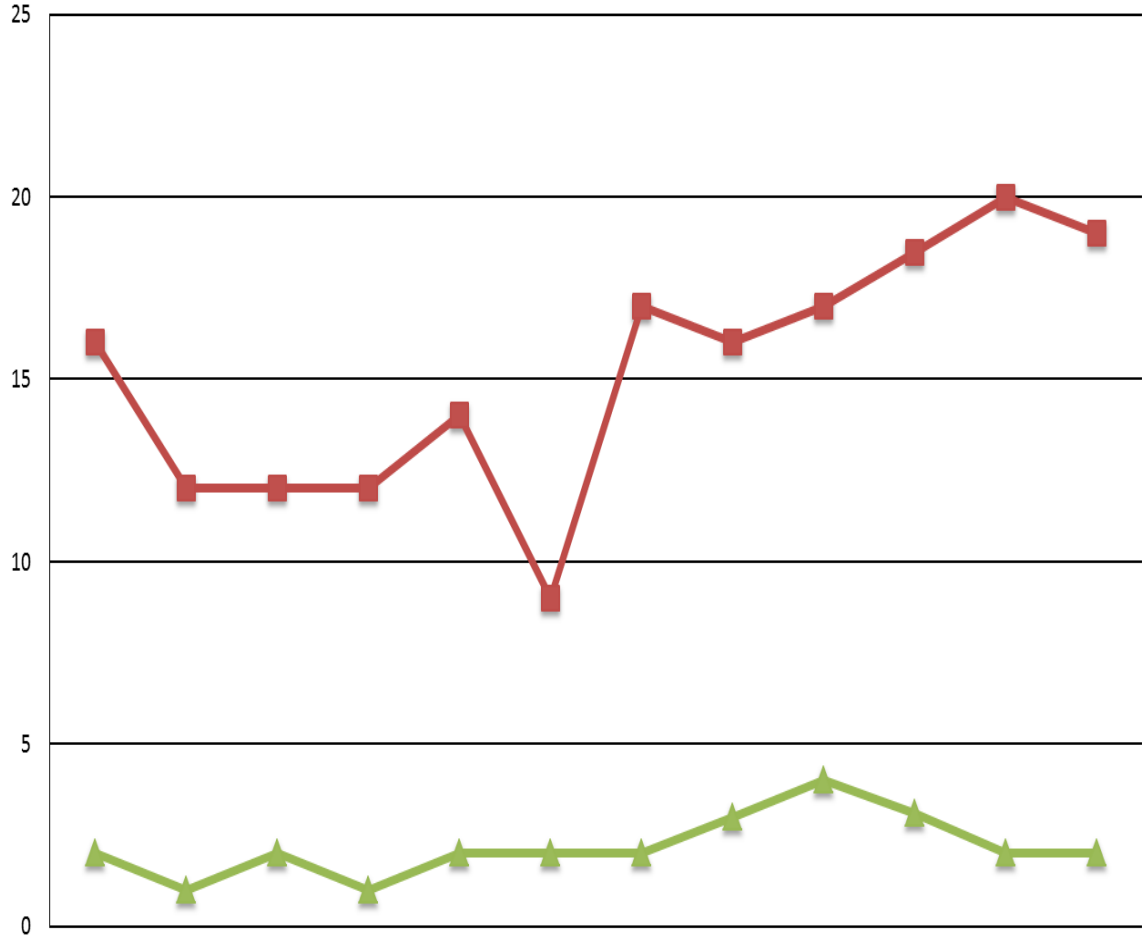
Overview:

- C&A Program Metrics
  - Security Plan Processing (IATO) Timeliness
  - Top Ten Security Plan Deficiencies
  - Security Plan Denial and Rejection Rates
  - Second IATOs Issued
  - Onsite Validation (ATO) Timeliness
  - Top Ten Vulnerabilities
- Working group initiatives

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 Results from Oct 2011- Sept 2012



	Oct-11	Nov-11	Dec-11	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12
Total IATOs	314	222	195	181	240	233	221	140	183	179	178	193
Time from DSS Receipt of plans to Granting of IATOs	16	12	12	12	14	9	17	16	17	18	20	19
Industry Response Time to DSS Questions, Comments	2	1	2	1	2	2	2	3	4	3	2	2
# Second IATOs	10	24	16	9	4	13	9	5	10	5	11	11

4699 SSPs Reviewed

2479 IATOs Issued

Avg 15 Days to Issue IATOs

1698 SATOs Processed

14 Days to Issue SATO

1220 of the SSPs (26%) required some level of correction

- 785 of the SSPs (17%) were granted IATO with corrections required

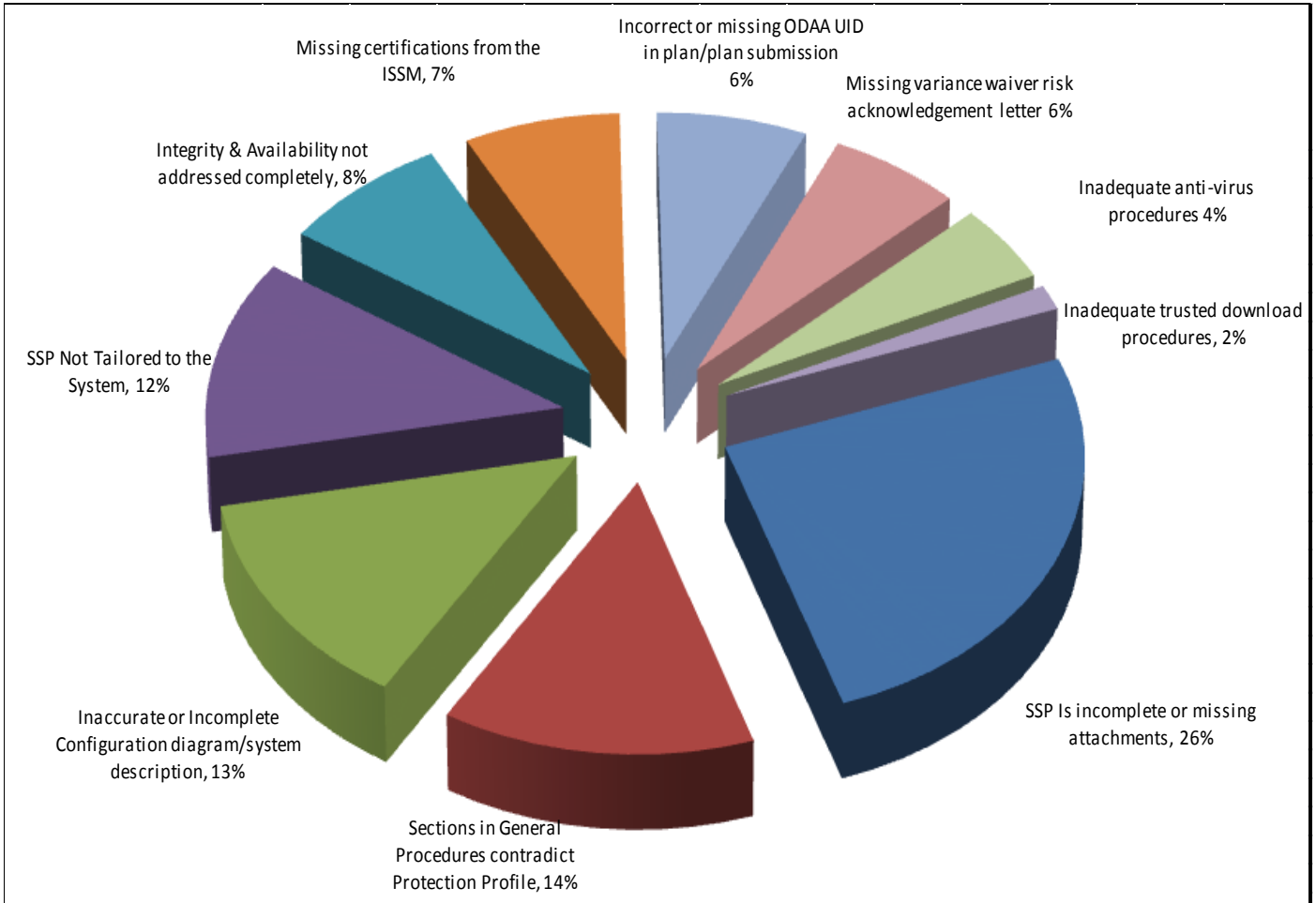
- 28 of the SSPs (1%) that went SATO required some level of correction prior to ATO

- 407 of the SSPs (9%) were reviewed and denied IATO (resubmitted after corrections)

- 115 of the SSPs (2%) were not submitted in accordance with requirements and were rejected. (resubmitted after corrections)

-

Common Deficiencies in Security Plans from Oct 2011- Sept 2012

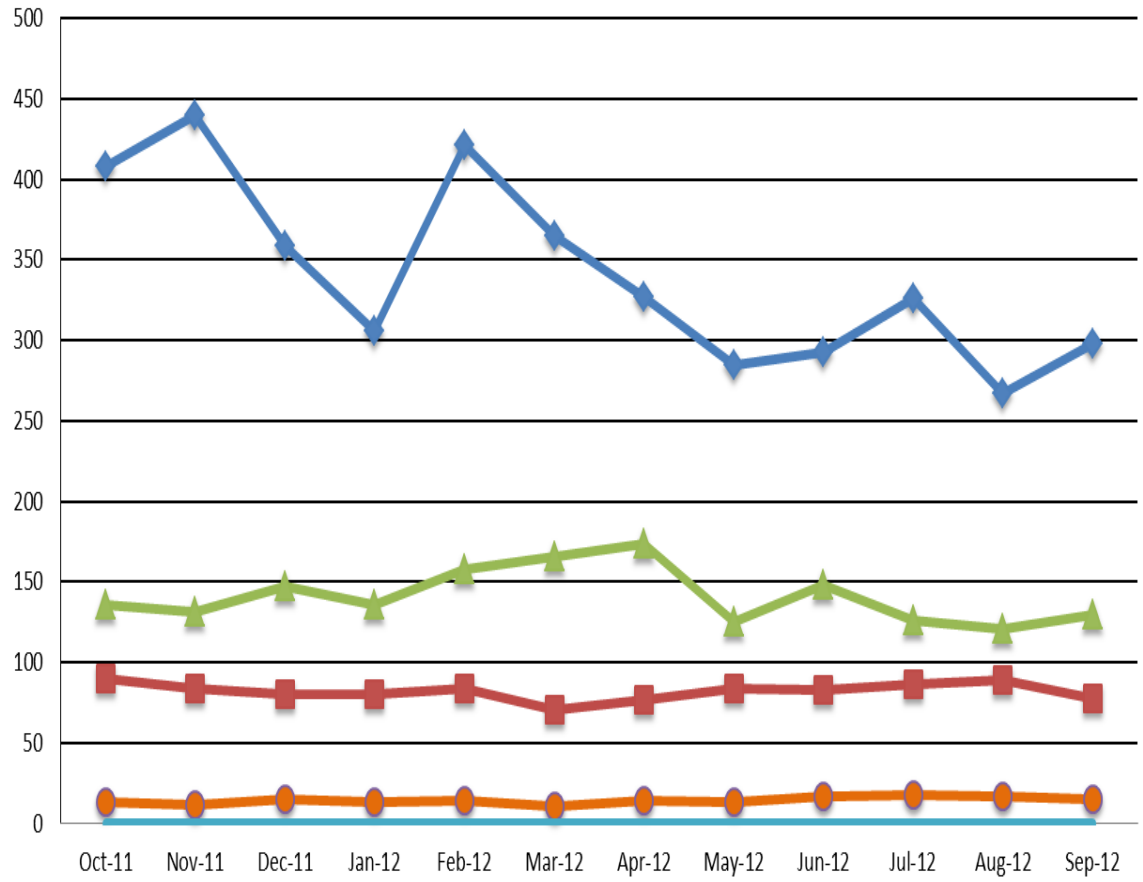


	Oct-11	Nov-11	Dec-11	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12
# Deficiencies	218	188	145	179	247	196	196	192	175	194	162	194
# Plans w/ Deficiencies	172	117	102	88	114	100	102	96	83	102	79	102
# Plans Reviewed	494	390	382	351	435	425	442	300	360	339	330	339
Avg Deficiency per Plan	0.44	0.48	0.38	0.51	0.57	0.46	0.44	0.64	0.49	0.57	0.49	0.57
Denials	44	37	40	34	37	26	47	34	24	25	25	34
Rejections	23	7	3	6	22	8	7	11	5	9	6	8

Top 10 Deficiencies

1. SSP Is incomplete or missing attachments
2. Sections in General Procedures contradict Protection Profile
3. Inaccurate or Incomplete Configuration diagram/system description
4. SSP Not Tailored to the System
5. Integrity & Availability not addressed completely
6. Missing certifications from the ISSM
7. Missing variance waiver risk acknowledgement letter
8. Incorrect or missing ODAA UID in plan/plan submission
9. Inadequate anti-virus procedures
10. Inadequate trusted download procedures

On Site Review Results from Sept 2011- Aug 2012



	Oct-11	Nov-11	Dec-11	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12
Total ATOs	408	440	359	306	421	365	327	285	293	326	267	298
Avg Days to Reg ATO	90	84	80	80	84	71	77	84	83	86	89	78
Total SATOs	136	131	147	136	158	166	174	125	148	126	121	130
Avg Days to SATO	13	12	15	13	14	11	14	13	17	18	17	15
% SATO's	33%	30%	41%	44%	38%	45%	53%	44%	51%	39%	45%	44%

During the Past 12 Months:

4095 Total ATOs (ATO+SATO)

2397 Standard ATOs

Avg 83 Days from IATO to ATO

1698 SATOs

Avg 14 days for SATOs

41% of all ATOs were SATO

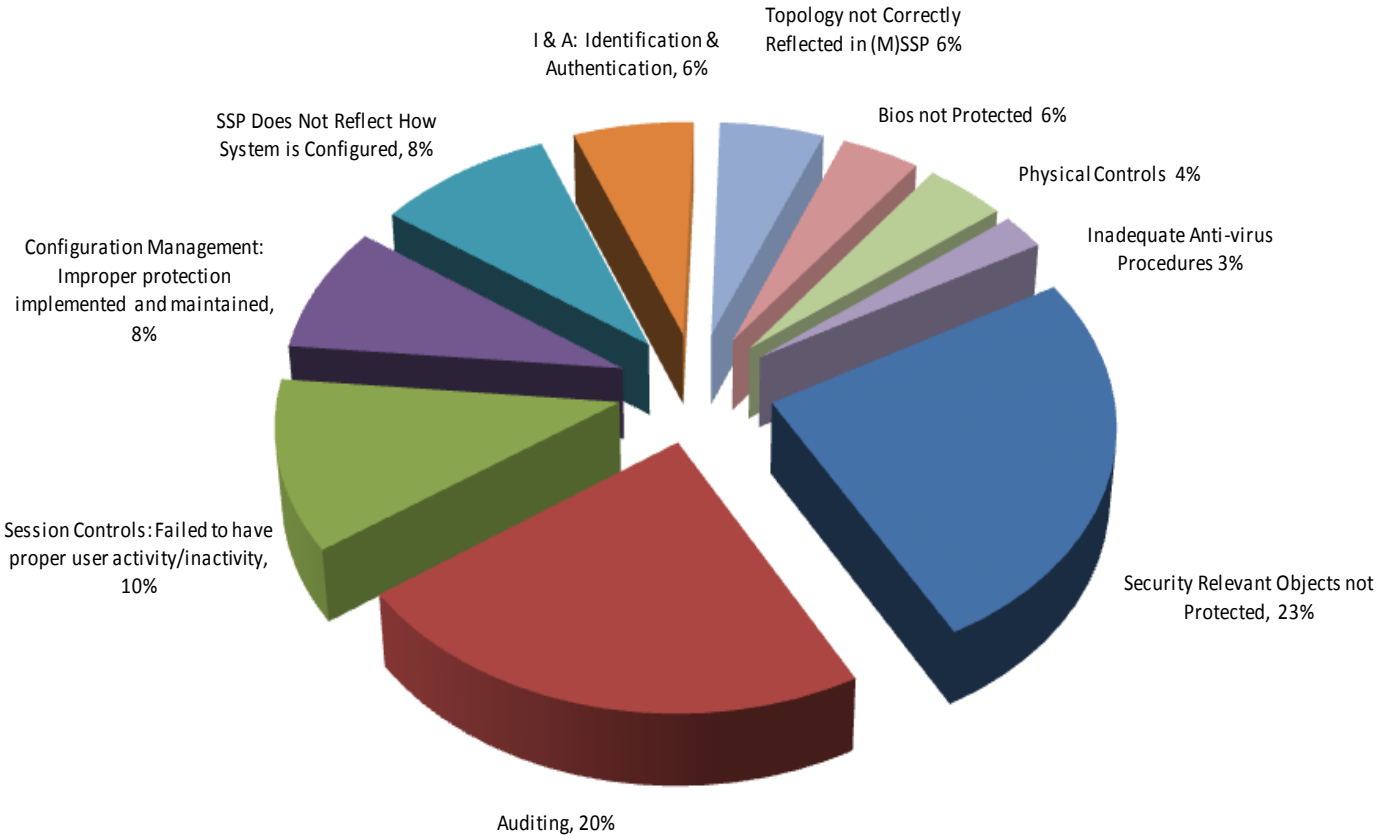
4064 ATO System Validations

- 3121 systems (77%) had no vulnerabilities identified.

- 876 systems (22%) had minor vulnerabilities identified that were corrected while onsite.

- 67 systems (2%) had significant vulnerabilities identified, resulting in a second validation visit to the site after corrections were made

Common Vulnerabilities found during System Validations from Oct 2011- Sept 2012



	Oct-11	Nov-11	Dec-11	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12
# Vulnerabilities	161	163	117	122	163	166	119	94	124	94	96	95
# Onsites w/ vulnerabilities	94	81	70	40	78	67	71	62	73	68	51	63
# Onsites	410	458	363	310	427	372	315	278	284	305	256	286
Avg Vulnerability per Onsite	0.39	0.36	0.32	0.39	0.38	0.45	0.38	0.34	0.44	0.31	0.38	0.33

Top 10 Vulnerabilities

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

Working Group Initiatives

- Windows 7 & 2008 Server Baseline Stds
  - Adding instructions/clarifying information to final draft prior to formal coordination
- Reviewing continuous monitoring to define applicability to NISP systems
  - Planning for adjustments to NISP C&A process as government moves toward NIST and DIARMF
- Preparing final draft of updated ODAA manual for coordination and comments
- Reviewing DoD security content automation protocol (SCAP) for possible use in assessing compliance on NISP information systems

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
- The working group is planning for pending changes to the program due to higher level policy and operating environment influences

Backup Slides

Security Plan Review Discrepancies by Facility Category

Number of Plans Submitted Sept 2012		46	60	62	68	140
	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Inaccurate or Incomplete Configuration diagram/system description	46	0.00%	6.67%	12.90%	11.76%	18.57%
SSP Is incomplete or missing attachments	44	10.87%	6.67%	12.90%	8.82%	15.00%
Sections in General Procedures contradict Protection Profile	28	4.35%	0.00%	1.61%	5.88%	15.00%
Missing certifications from the ISSM	26	2.17%	5.00%	1.61%	13.24%	8.57%
Inadequate anti-virus procedures	26	4.35%	0.00%	4.84%	7.35%	11.43%
SSP Not Tailored to the System	18	0.00%	1.67%	3.23%	1.47%	10.00%

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

September 2012	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Missing variance/waiver/risk acknowledgement letter	17	0.00%	5.00%	1.61%	5.88%	6.43%
Inadequate recovery procedures	8	0.00%	1.67%	0.00%	0.00%	5.00%
Integrity & Availability not addressed completely	7	0.00%	0.00%	1.61%	0.00%	4.29%
Inadequate trusted download procedures	4	0.00%	0.00%	0.00%	1.47%	2.14%
Missing full ODAA UID on Title Page	0	0.00%	0.00%	0.00%	0.00%	0.00%
Other	0	0.00%	0.00%	0.00%	0.00%	0.00%
Total Errors %	**224**	**0.00%**	**7.14%**	**11.16%**	**16.96%**	**60.27%**
Total Errors	**224**	**0**	**16**	**25**	**38**	**135**

System Validation Vulnerabilities by Facility Category

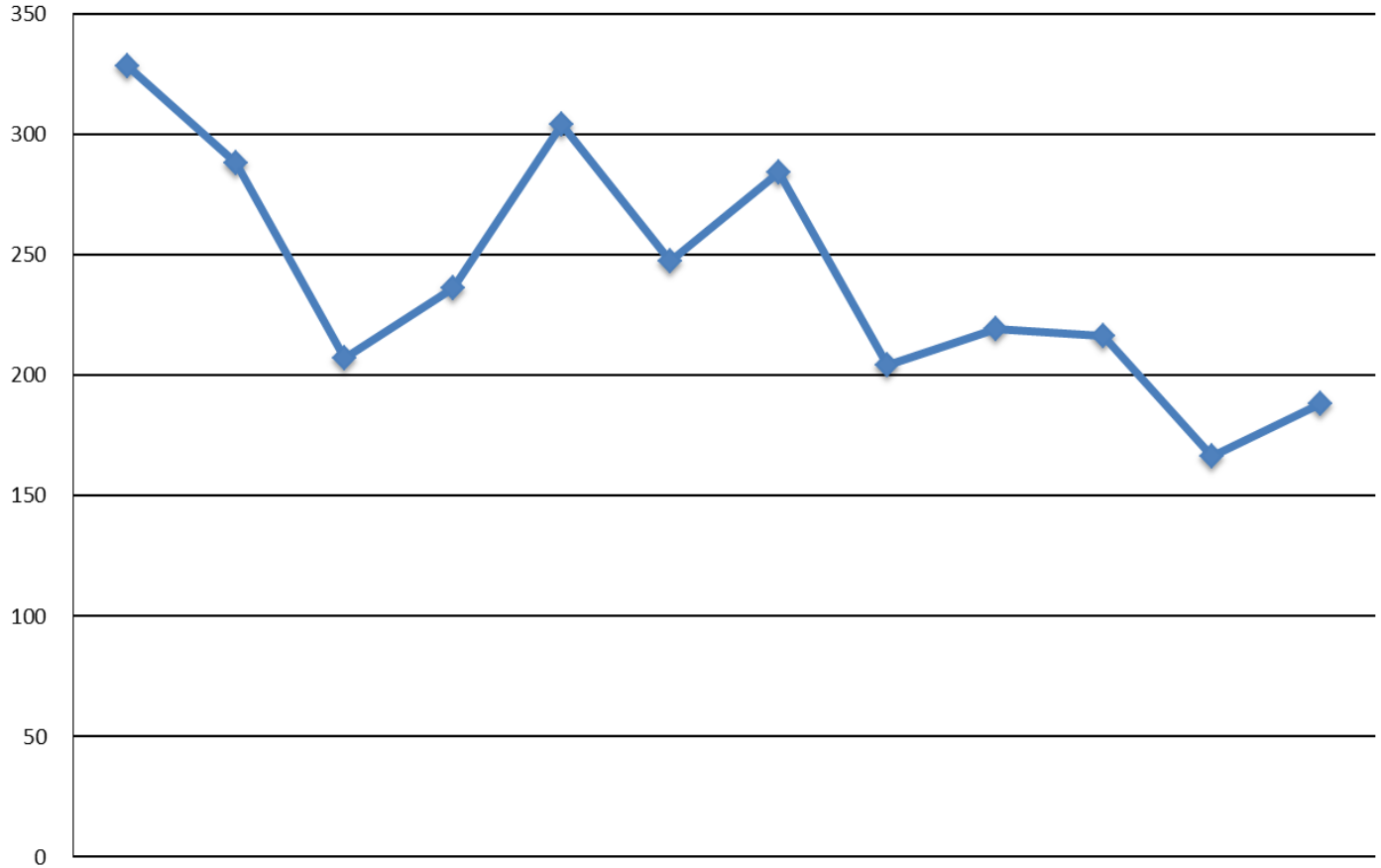
Systems Validated by Facility Category Sept 2012		36	30	24	23	55
	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Security Relevant Objects not protected	27	5.88%	0.00%	3.64%	16.28%	16.67%
Auditing	18	0.00%	6.25%	5.45%	2.33%	12.22%
Configuration Management	15	5.88%	0.00%	10.91%	4.65%	4.44%
SSP Does Not Reflect How the System is Configured	8	0.00%	0.00%	0.00%	0.00%	8.89%
Physical Controls	6	0.00%	0.00%	1.82%	0.00%	5.56%
I & A	6	0.00%	0.00%	5.45%	0.00%	3.33%
Session Controls	3	0.00%	2.08%	0.00%	0.00%	2.22%
Topology not correctly reflected in (M)SSP	3	0.00%	0.00%	0.00%	0.00%	3.33%
Bios not Protected	3	0.00%	0.00%	0.00%	2.33%	2.22%
Inadequate anti-virus procedures	2	0.00%	2.08%	0.00%	0.00%	1.11%

System Validation Vulnerabilities by Facility Category (cont'd)

September 2012	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Root/Admin Account misconfigured	2	1.96%	0.00%	0.00%	2.33%	0.00%
PL Not Adequately Addressed	1	0.00%	0.00%	0.00%	0.00%	1.11%
Trusted Download Review	1	1.96%	0.00%	0.00%	0.00%	0.00%
Compilation	0	0.00%	0.00%	0.00%	0.00%	0.00%
All Users are Configured as Administrators	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%
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%
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	**95**	**8.42%**	**5.26%**	**15.79%**	**12.63%**	**57.89%**
Total Errors # Slide One and Two	**95**	**8**	**5**	**15**	**12**	**55**

System Disestablishments

Oct 2011 - Sept 2012



Oct-11	Nov-11	Dec-11	Jan-12	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12
328	288	207	236	304	247	284	204	219	216	166	188

Disestablishments for Month Sept 2012:

Total: 188

Capital: 39 (20.74%)

Northern: 52 (27.66%)

Southern: 28 (14.89%)

Western: 69 (36.70%)

Attachment #10- Combined Industry Presentation

NATIONAL INDUSTRIAL SECURITY PROGRAM

POLICY ADVISORY COMMITTEE

(NISPPAC)

NOVEMBER 14, 2012

Outline

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

National Industrial Security Program

Policy Advisory Committee Industry Members

Members	Company	Term Expires
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
J.C. Dodson	BAE Systems	2016
Tony Ingenito	Northrop Grumman Corp	2016

Industry MOU Members

AIA	**Vince Jarvie**
ASIS	**Tom Langer**
CSSWG	**Mark Rush**
ISWG	**Mitch Lawrence**
NCMS	**Rhonda Peyton**
NDIA	**Ken White**
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**
  - **Potential effects of Government Sequestration on clearance processing**
  - **JPAS change process/communication**
  - **Request to add a member of the Industry Team to this working group - status**
  - **USN's RapidGate Program challenges**
- **Automated Information System Certification and Accreditation**
  - ***Metrics good. Focus - strategic requirements and implementation***
- **Ad-Hoc**
  - **NISPOM Rewrite Working Group (13 meetings), on-going progress**
  - **CI Working Group & Suspicious Contact reporting requirements continue to be fragmented**
  - **Current Threat information sharing is still lagging**
  - **Potential revision to DD 254 – Industry invited to comment**

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**
- **15 February 2012 Joint Government/Industry Session**
  - **Discuss results of Government session**
  - **Address Industry specific issues**
- **10 October 2012 Retain NISPOM Sup - changed NISPOM App D**
  - **DOD to issue NISPOM SAP Manual in late FY 13**
  - **DOD to share draft SAP volumes with other NISP signatories**

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

DOD Manual – 5200.01

Draft FAR Clause

THANK YOU