NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

SUMMARY MINUTES OF THE MEETING

The NISPPAC held its 41st meeting on Wednesday, March 21, 2012, at 10:00 a.m. in the Archivist's Reception Room 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. The following minutes were finalized and certified on June 15, 2012.

The following individuals were present:

- John Fitzpatrick (ISOO, Chair)
- Greg Pannoni (ISOO, Designated Federal Officer (DFO))
- Daniel McGarvey (Department of the Air Force (USAF), Member)
- Ryan McCausland (USAF, Alternate)
- Booker Bland (Department of the Army, Observer)
- George Ladner (Central Intelligence Agency (CIA), Alternate))
- Jim Glukas (CIA, Observer)
- Eric Dorsey (Department of Commerce, Member)
- Timothy Davis (Department of Defense (DoD), Member)
- Stephen Lewis (DoD, Alternate)
- Richard Hohman (Office of the Director of National Intelligence (ODNI), Member)
- Carrie Wibben (ODNI, Presenter)
- Christy Wilder, (ODNI, Presenter)
- Charles Sowell (ODNI, Presenter)
- Drew Winneberger (Defense Security Service (DSS), Member)
- Kathleen Branch (DSS, Alternate)
- Stan Sims (DSS, Presenter)
- Charles Tench (DSS, Presenter)
- Helmut Hawkins (DSS, Presenter)
- Randy Riley (DSS, Presenter)
- Mike Buckley (DSS, Presenter)
- Helencia Hines (DSS, Observer)
- Tracey Kindle (DSS, Observer)
- Carl Piechowski (Department of Energy (DOE, Observer)
- Geralyn Praskiewicz (DOE, Observer)
- Christal Fulton (Department of Homeland Security, Alternate)
- Anna Harrison (Department of Justice, Member)
- Kathy Healey (National Aeronautics and Space Administration, Observer)
- Jeffrey Moon (National Security Agency, Observer)
- Derrick Broussard (Department of the Navy, Member)
- Darlene Fenton (Nuclear Regulatory Commission (NRC), Member)
- Krista Juris (NRC, Observer)
- Daniel Cardenas (NRC, Observer)
- Kimberly Baugher (Department of State, Member)
- Lynn Gebrowsky (Office of Personnel Management, OPM), Presenter)
- Priscilla Matos (Office of the Undersecretary of Defense for Intelligence, Observer)
- Judy Baron (Defense Advanced Research Projects Agency (DARPA), Observer)

- Pamela Spilner (DARPA, Observer)
- Steven Welch (Missile Defense Agency, Observer)
- Patrice Murray (National Archives and Records Administration, Observer)
- Scott Conway (Industry, Member)
- Shawn Daley (Industry, Member)
- Richard Graham (Industry, Member)
- Frederick Riccardi (Industry, Member)
- Michael Witt (Industry, Member)
- Steven Kipp (Industry, Member)
- Michelle Sutphin (Industry, Observer)
- J. Paul Veronie (Industry, Observer)
- Marshall Sanders (Memorandum of Understanding (MOU) Representative, Member
- James Hallo (MOU Representative)
- Mark Rush (MOU Representative)
- Mitch Lawrence (MOU Representative)
- Kirk Poulsen (MOU Representative)
- Tony Ingenito (MOU Representative)
- Vincent Jarvie (MOU Representative)
- Patrick Viscuso (ISOO)
- David Best (ISOO)
- Robert Tringali (ISOO)
- Daniel Livingstone (ISOO)
- Joseph Taylor (ISOO)

I. Welcome and Administrative Matters

John Fitzpatrick, welcomed the attendees, and reminded everyone that a NISPPAC meeting is a recorded public event. He then asked Greg Pannoni, ISOO and NISPPAC DFO, to review old business.

II. Old Business

Mr. Pannoni stated that the first open item from the last meeting was for ISOO to coordinate with ODNI and the Defense Office of Hearings and Appeals (DOHA) to provide all investigative and adjudicative information and statistics that enable a holistic picture of the security clearance processes impacting industry. He noted that the NISPPAC Personnel Security Clearance Working Group (PCLWG) update will include intelligence community data for industrial clearances, and that discussions are underway for determining the appropriate way forward for presentation of DOHA data. The second item was for the PCLWG to determine the impact, and develop a plan to meet the OPM mandated 14 day standard for fingerprint submittal. Also, the Working Group was to evaluate how to close the gap between the number of completed investigations and the number of reported adjudications to ensure confidence in the comprehensive nature of these data. He noted that these items would also be addressed during the PCLWG update. The third open item was a request for a briefing on the ongoing efforts of the Controlled Unclassified Information (CUI) Office, which was on the meeting's agenda. Next, there would be an update from DoD on the status of changes to the Defense Federal Acquisition Regulation Supplement (DFARS), and the National Industrial Security Program Operating Manual (NISPOM). Next, the request for a briefing by the Insider Threat Task Force (ITTF) on their plans to implement applicable portions of E.O. 13587, "Structural Reforms to Improve Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," has been postponed. He reminded everyone that an e-mail had been sent, along with today's agenda, wherein the Chair requested that the membership come prepared

to discuss any issues stemming from the implementation of E.O. 13587 that impact NISP contractors. Next, was an industry request for ISOO to host an ad-hoc working group meeting on Special Access Programs (SAP). Mr. Pannoni noted that this working group was convened, and the Committee would receive an update during today's meeting. Next, was a request for DSS to inquire into the Defense Manpower Data Center's (DMDC) policy for reinstating JPAS accounts that have been disabled due to account inactivity, as well as efforts to encourage DMDC to post their policy account usage on their website, so account holders can avoid having accounts disabled. He informed the Committee that DSS now reports that DMDC has posted its account usage policy on the Joint Personnel Adjudication System (JPAS) website and has added a reminder on the JPAS logon page that 90 days of account inactivity will result in the account being disabled. The final action item was for the Certification and Accreditation Working Group (CAWG) to consider the aggregation of system security errors so that such data may be provided at the corporate level. He advised this item would be discussed by the CAWG during today's update. The Chair then asked for Committee working group updates.

III. Working Group Updates

A) The PCLWG Report

Helmut Hawkins, DSS, presented the Defense Industrial Security Clearance Office (DISCO) portion of the update (Attachment 1). He reported that pending adjudications at DISCO, in the first quarter of FY 2012, reflected a 19 percent reduction in initial cases awaiting adjudication. Further, there has been a 61 percent reduction in pending Periodic Reinvestigations (PR). Also, the average PR monthly cost for FY 2011 was approximately $7.3 million. Whereas, for the first five months in FY 2012 that cost has risen to approximately $10.2 million. Mr. Hawkins suggested that there were perhaps several factors that may contribute to the increase: (1) efforts to encourage industry to submit long overdue PRs; (2) some agencies that had been completing their own PRs are now sending them to DISCO; and (3) there may be changes in OPM criteria that cause a case to rise to issue level. He proffered that by the next NISPPAC meeting, DISCO should be able to confirm the reason(s) for the increased costs. He continued by noting that the number of DISCO adjudications are significantly lower. Thus the overall adjudication time has fallen 17 percent over the first five months of FY 2012. In addition, investigations pending at OPM have increased by five percent.

He then described decreased reject rates, and pointed to initiatives by both OPM and DISCO to provide additional instructions to smaller companies as factors contributing to these reductions. As regards DISCO Rejections, 49 percent are due to missing employment and/or family member information. He noted that attachment 1 lists all ten rejection reasons, accounting for 99 percent of the cases. The Chair interjected with a suggestion that the Working Group should begin to collect all these observations in one chart in order to capture a more complete and informative picture. By so doing, one might more easily be capable of drawing several helpful conclusions, such as the identification of concern areas, the onset of negative trends, or even the observation of well-deserved kudos. In addition, the Chair recommended that all who prepare metrics-type briefings should consider this type of all-inclusive chart, as it offers the opportunity to identify both positive and negative conditions and may explain why some results are achieved while

others fail, as well as pinpointing systemic risk factors. He envisions this kind of analysis becoming a significant factor in determining insider threat policy, and he suggests that these factors, such as the currency of PRs and the number of cases that have not been submitted, represent relevant metrics information that we will want to study.

Next, Charles Tench, DISCO, provided an update on the continuing problems associated with unacceptable fingerprint cards. He reported that DISCO has altered the Secure Web Fingerprint Transmission (SWFT) system to permit the submission of fingerprint cards prior to submission of the Standard Form (SF) 86, "Questionnaire for National Security Positions." In addition, SWFT has been modified to permit, upon securing an account, an organization to service multiple case codes. This allows companies to share services, such as one company collecting fingerprint information for another company, thus assisting those having not yet acquired electronic fingerprint capability. Tony Ingenito, National Classification Management Society (NCMS), added his enthusiastic support for these process changes, and encouraged everyone in industry to quickly establish a SWFT account, as that process in itself takes a long time to complete.

Next, Lynn Gebrowsky, OPM, continued the PCLWG's report by presenting the OPM performance metric updates on the security clearance timelines of investigations and adjudications. She summarized a statistical comparison of first quarter FY 2012 with the previous three quarters (Attachment 2). She informed that the analysis showed a clear increase in overall timelines, and that this appears to be linked to increases in case volumes. The Chair asked if these timeliness numbers were captured in the Federal Information Processing Standard (FIPS), and if so, was this data reported by the adjudicating agency. Ms. Gebrowsky affirmed both conditions. In addition, she added that there is a slight time increase for Top Secret PR investigations and attributed this to the fact that initial investigations receive a higher priority than PRs. The Chair interjected that this was yet another area which would likely receive more attention as insider threat policy matures.

Next, Christy Wilder, ODNI, completed the PCLWG's report update. Ms. Wilder presented statistical updates from those investigations and adjudications that are conducted by other Investigative Service Providers (ISP) (Attachment 3). She mentioned that approximately 5.9 percent of the government's investigations and adjudications for industry are conducted by the Intelligence Community (IC). She noted that less than one percent of these investigations are conducted by other agencies, and the owning agency invariably performs the adjudications. She then explained that the future of charting PRs would include how often they are being scheduled. Also, for those not scheduled they will concentrate on an analysis of the difference between those that are out of scope and those not yet scheduled. She informed that this additional process was not yet refined, but it will likely be ready for inclusion in future reports. The Chair applauded the Working Group's inclusion of this initiative. Ms. Wilder added that such analysis will provide an excellent opportunity for agencies to perform some much-needed database cleanup. She further commented that PR timelines are largely on target, as most everyone is within the 195 day goal: the proper mix of 150 investigative and 30 adjudicative days, leaving 15 days applied to the initial phase. The Chair then thanked the PCLWG for its efforts, and since the Committee was already energized on security clearance concerns, moved directly to the

update on Joint Reform and the Security Executive Agent (SEA), and introduced Charles Sowell, ODNI.

B) The Joint Reform and SEA Update

Mr. Sowell began by addressing the Chair's earlier comments on the PR backlog. He explained that the ODNI has begun to examine this issue and is gathering more data for additional analysis. Further, the ODNI has already concluded that this issue is having a significant, negative impact throughout the government, and plans to highlight agencies' un-submitted PR numbers in next year's performance letters. Therefore the ODNI is energized to work with agencies to address this problem, describing it as one perpetuated by extremely limited resources, and this joint effort will help identify the resources that could be applied toward solutions.

Next, Mr. Sowell noted (Attachment 4) that recently the ODNI held the first Security Clearance and Suitability Performance Accountability Council (SCSPAC) meeting since December 2010. He described the Council's agenda as providing updates across the largest security and suitability stakeholders group in government on automated record check pilots, the performance metrics previously described by Ms. Wilder, and the federal investigative standards. He noted that the intent of the Council's principals is to hold their meetings monthly, a significant change from previous policy, thus indicating their commitment to the reform effort. He further noted that the federal investigative standards are undergoing legal review, and estimates project completion and signing implementation by April 2012. He added that signing would prompt the beginning of the implementation process, which is in the form of a strategic framework document, expected by December 2013. Also, he informed that the training standards for both suitability and security adjudicators have been under review for a long time but was hopeful that they would be issued shortly.

Next, Mr. Sowell noted the ongoing concerns with the item on the SF 86 pertinent to mental and emotional health. He described this as a government-wide, critically important issue that is trying to balance security needs with compassionate concerns, such as encouraging individuals to seek counseling versus the desire to maintain privacy. The ODNI decided to have the item revised, and an SEA Advisory Committee working group has been charged with the item's revision. He then yielded to Carrie Wibben, Chief of Personnel Security, ODNI, who discussed the recent in-depth focus on implementing the authority and responsibilities in E.O. 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information."

Ms. Wibben explained that her staff has focused on joint reform efforts but is now moving toward implementation. That effort has led to the development of a capstone directive, "Security Executive Agent Directive 1," wherein all the disparate authorities of the SEA have been codified, from such sources as the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as well as other executive orders, law, and policy, into a single document. She noted that the Directive was signed in March, 2012, and represents an important milestone in that it establishes the framework from which we will generate all other forthcoming SEA directives. In

addition, she announced the recently launched SEA website, which is linked on the unclassified side to the National Counterintelligence Executive (NCIX) homepage at http://www.ncix.gov.

Next, she described several other pages of interest to the community that are also linked to the website. The first, which is in its initial and educational stage, is the page on reciprocity. The reader can view current policies on reciprocity, complete with applicable OMB memoranda. The next phase will focus on the development of a web-based form, essentially a restart of the original reciprocity hotline initiative through which we can collect electronic data to be subsequently populated into a database from which trend analysis and follow-on actions can be performed. She stated that the initial target audience would be industry, as there are many concerns to be generated there. She mentioned other reciprocity initiatives, such as the ongoing development of a national reciprocity policy. Mr. Pannoni, DFO, suggested that in light of the website's educational awareness objectives with regard to reciprocity, perhaps the SEA should consider providing an enhanced pictorial representation of the security and suitability tier levels, and how they intersect with each other. That, in fact, in some cases there is not so much a reciprocity issue as simply an issue of differing investigative requirements based on suitability or national security. Ms. Wibben accepted the suggestion, and agreed to consult with OPM to make certain that there was no obstruction to ODNI's posting crosswalk information on the website. The Chair then returned to the regular agenda and asked Randy Riley, DSS to present the CAWG update.

C) The Certification & Accreditation Working Group (CAWG) Report

Mr. Riley explained that today's report would be centered on two items: the feasibility of consolidating all system security plan (SSP) errors for a particular corporation, to include all Commercial and Government Entity (CAGE) codes under a specific corporate umbrella, and the standard certification and accreditation metrics. With regard to the first item, he noted that the Group had determined that there was indeed feasibility in such a plan, and has already begun work on designing a presentation format, complete with component specificity and depth. He explained that there is presently six months of data that can be rolled out to one year, and then the Working Group can provide, probably on a quarterly basis, a 12-month picture of the SSP errors at the various CAGE code levels. He noted that the system validation errors were already described at the CAGE code level, and that in the future the Working Group would include recurring on-site vulnerability assessments. This would provide the corporate point of contact (POC) with specific facility vulnerabilities at the CAGE Code level and a roll up at the corporate level of the three components involved in certification and accreditation. These components include the SSP documentation deficiencies, any system vulnerabilities identified on-site as not in accordance with the SSP, and the vulnerability assessment results determined during recurring visits. The Working Group's ultimate goal is the identification of these specific problem areas, so that it can focus on what requires correction, thus making across the board program improvements. Industry will need to provide the POC for each corporation, who in turn will provide the Office of Designated Approving Authority (ODAA) a list of the CAGE codes for facilities under their purview. DSS will then provide the roll up in either a .pdf file or as an Excel spreadsheet, depending upon the client's desires. He then turned to the certification and accreditation metrics.

Mr. Riley noted that the certification and accreditation metrics format was slightly modified to achieve better focus on vulnerabilities, errors, and attributes that require immediate correction (Attachment 5). He noted that DSS is the designated government authority for certification and accreditation, and the ODAA's primary goals are to work with our industry partners to ensure the accomplishment of information security requirements, to limit the risks for compromising information, and to ensure adherence to standards. He then presented the latest metrics for timeliness of SSP reviews, describing the continued achievement of stable turnaround times of approximately 14 days. He mentioned that the ODAA continues to focus on a Straight to Authority to Operate (SATO) process as opposed to the issue of an Interim Authority to Operate (IATO), as this minimizes/eliminates systemic risk because it enables DSS to conduct an onsite visit within a couple of weeks to validate the implementation of system requirements prior to authorizing use.

Mr. Riley continued with a discussion of the types of deficiencies identified during SSP reviews. He noted that over the previous 12 month tracking, roughly 1/3 of the plans required corrections, and thus about 950 SSPs were issued IATOs until those deficiencies could be eliminated. Further, roughly 13 percent of plans had significant deficiencies that precluded issuance of an IATO. He next presented the most recent metrics affecting SSP denial and rejection rates, and noted that the trend continues to be markedly downward. Next, he presented a chart that captured the types and frequencies of deficiencies found in the SSPs over the most recent 12 months. In addition, the ODAA will further segment the categories, so that the quarterly report to the corporate POCs will be capable of tracing each error back to a specific item, thus increasing the opportunity for enhanced training. Mr. Ingenito interjected to offer industry's appreciation for the ODAA's increasing the granularity in this process.

Mr. Riley then discussed system validation metrics resulting from on-site reviews. The metrics reveal that in the most recent 12 month period there were roughly 3,400 systems issued ATOs, requiring an average of 99 days for processing each system from IATO to ATO. He noted that when systems were granted an immediate ATO during that same 12 month period, the average processing time was 19 days. Therefore, the much reduced processing time, similar to the case of vulnerabilities described above, is equally worth eliminating the risk. He further noted that the ODAA was currently averaging 13 days on straight to ATO cases. Further, the system validation metrics describe that 12 month period's vulnerabilities on the systems in which a visit was made. He stated that the ODAA is not yet capturing the specific vulnerabilities, but rather the number of vulnerabilities. Also, he noted that even as these systems are processing classified information, the 12 month period demonstrated that 71 percent had no vulnerabilities and 23 percent had minor vulnerabilities that were corrected on the spot. Nevertheless, two percent of the systems are plagued by significant vulnerabilities that could not be corrected immediately, thus prohibiting the issuance of an ATO and prompting a return visit. Both of these conditions are problematic, as they describe systems that have already been certified as properly configured, and which was the basis for issuance of the original IATO. Finally, he closed with a chart representing these same system vulnerabilities, and noted that in the future, the ODAA would refine some of the categories, especially those that require more specificity. The Chair commended the Working Group on an excellent program, and encouraged DSS to intensify its systems relationship building with the IC community, as it is leading the way with regards to

information systems. In addition, the Chair pointed out that the Senior Information Sharing and Safeguarding Steering Committee, on which he serves, is now developing policy in this arena which will be directly linked to the NISPOM, and will require action from the industrial community. Next, the Chair called for Mr. Pannoni to give a report on the initial efforts of the SAP Working Group (SAPWG).

D) The Special Access Program Working Group (SAPWG) Report

Mr. Pannoni explained that industry had requested that the NISPPAC establish a SAPWG (Attachment 6). Industry cited three overarching concerns that drive the need for a SAPWG: personnel security clearance concerns, information systems issues, and physical security concerns, the commonality of which is reciprocity. He explained that industry's goal was the achievement of standardization throughout all security requirements, and he further described their concerns as a security framework based on risk management, as opposed risk avoidance. He then explained that an initial forum was held that was composed of government representatives whose agencies were authorized to establish SAPs. He noted that what was discovered in this forum was that the methodology for providing policy guidance from one agency to another is often different, as some agencies have detailed instructions while others have minimal guidance. Also, there is no centralized policy that directs the conduct of SAPs for the government, and thus implementation within industry is inconsistent. The second meeting brought both government and industry representatives together, and led to the conclusion that both would need to work together to design policies based on minimum baseline standards that were acceptable by all. He posited that perhaps such a model could adapt the tier-formula concept presently used by the personnel security clearance process. He characterized the central objective directing the efforts of the combined government/industry forum as, being driven by NISPOM program objective guidance, to adopt a single, integrated, cohesive program that reduces or avoids overlapping and redundant processes. At the same time, all parties recognized that until such a methodology is developed, they must continue to operate in accordance with the present NISPOM supplement.

In response to an inquiry from the floor from Shawn Daley, Industry, Mr. Pannoni stated that the Joint Air Force, Army, Navy (JAFAN) document was discussed during the forum, but that the NISPOM supplement should serve as the overarching, baseline document for SAPs. Steve Lewis, DoD, added that as a result of the 1985 development of the NISPOM supplement, the military services took the opportunity to update their internal policies in an attempt to align wherever possible with IC issuances, and he noted that the resulting JAFAN did indeed mirror the IC guidance in many respects. Therefore, he suggested that, at least in the interim, the JAFAN remains a necessary expedience. He also reminded the Committee that DoD is working diligently on a DoD SAP manual, and it is hoped that upon its completion and approval it will become the basis for an updated NISPOM supplement. Mr. Pannoni then yielded to the Chair who directed that the meeting move to new business, and asked Scott Conway, Industry Spokesman, to provide the Combined Industry report.

IV. New Business

A) The Combined Industry Presentation

Mr. Conway advised that two industry members, Marshall Sanders and he are due for replacement this summer, and that soon he will be soliciting nominations for replacements from the NISPPAC industry membership. In addition, a new industry spokesperson will be selected from within the current membership. He then recognized that all MOU members were at today's meeting, and Mark Rush, Chair of the Contractor Special Security Working Group had recently replaced the retiring Randy Foster. Next, he mentioned that the basic tenant of industry's charter (Attachment 7) was to provide advice to the Director, ISOO, in his capacity as Chair of the NISPPAC on all matters concerning NISP policies.

Mr. Conway then applauded the efforts of the PCLWG in expanding the metrics collection procedures to capture all personnel security clearance processes, and the initiative to include the SEA in future deliberations. He mentioned that industry had also held a separate and extensive discussion to determine what else should be included in this area. They remain concerned that there is yet no visibility into metrics on SAP accesses, but they welcome the initiative to institute a working group on this subject so that this issue can ultimately be resolved. Next he reminded the Committee of some of the challenges endured when JPAS was being formulated, and wants to be certain now that JPAS is to be replaced, that industry performs an active role in the development of its replacement. He then asked for Mr. Ingenito to add industry's thoughts on the subject of JPAS replacement.

Mr. Ingenito posited that the real value of including industry in the JPAS replacement process comes with the synergies of all stakeholders working together, as then all issues would be discovered and discussed by the various organizational representatives. In addition, all parties then get the opportunity to define the concerns, permitting industry to join in discussions and decision–making with regard to potentially systemic issues involving everyone's interests. Vincent Jarvie, Aerospace Industries Association (AIA) echoed the comments of both Mr. Conway and Mr. Ingenito with a call for active participation in this replacement process. He also thanked Mr. Sims for his aggressive efforts to include industry in the process. He expressed assurance that industry would engage the right people and resources to achieve a dynamic and workable product.

Mr. Conway then mentioned a concern pertinent to the lack of government personnel security clearance investigators overseas; explaining that industrial personnel overseas are impacted because they cannot get subject interviews required for the granting of a final clearance. He explained that industry urges that the interim clearance process be retained, as it enables industry to put people to work on at least a baseline level, which is a position of critical importance to some industry partners.

Next, Mr. Conway applauded the efforts of the CAWG in enhancing their metrics, but inquired whether the Working Group could expand its efforts to include classified information systems that are carved out of the DSS certification and accreditation process.

He then commented briefly on other industry interest items. He applauded the NISPOM rewrite initiative, complementing the participants on the process' openness, and suggesting that the project was nearing maturity. He addressed the insider threat information sharing program, and expressed industry's appreciation for the education, but recommended that we move forward as industry understands the threat but the effort must focus on how to receive the intelligence in a timely manner. He mentioned that as there is now an industry forum within NCMS, we have a working group that can concentrate on improving conditions and issues affecting medium and small-sized facilities, as well as smaller sites of larger corporations. He applauded the initial meetings of the SAPWG but cautions that not all companies have POCs within the customer community on these issues and we very much need to evolve to the point where we have consistency among everyone who operates in a SAP environment. He posited that we might consider a DoD ombudsman through whom we could send and receive information policy and documentation. One of industry's concerns is that when the new NISPOM is complete and we are still without a DoD SAP manual, we may suddenly lack the necessary cohesiveness and relapse into an unproductive situation. Therefore, industry believes that there remains a lot of work to be done in this area.

Mr. Pannoni asked a question relative to the overseas interim clearance process about which Mr. Conway had spoken earlier. Namely, in view of the sophisticated technology available in today's environment, might it be possible that, notwithstanding any legal issues, and in the case of the non-issue subject interviews, video teleconferencing could be employed? Mr. Sims advised that DoD has such a program, and some industrial cases have been accomplished that way. But the problem has been that such interviews have been conducted poorly. Also, he noted that industry has been consulted as to the possibility of notifying DISCO on any occasion in which applicants are returning to the states, so that they could coordinate with OPM personnel to perform the interviews, such as during the mid-cycle leave period. Finally, he advised that they have even tried sending teams to the forward locations to perform the interviews but with mixed results, as getting the people away from the work areas and securing a safe zone to conduct the interviews has proven problematic.

Mr. Sims also mentioned that DSS has begun routinely holding stakeholder meetings, with both government and industry, in which many issues surfaced at the NISPPAC are discussed in greater detail. In the case of the government stakeholders, he explained that a lot of time had been spent in discussing ways of improving the partnership with industry. He noted that this forum has continued discussing the National Interest Determination (NID) process, and that its membership was recently informed that there is a new policy that has resulted in a significant reduction in overdue NIDs. Furthermore, they have discussed how to reduce or eliminate breakdowns in communication and effectiveness, and also agreed that on the government side, there remains a lack of education in matters concerning industry and the NISPOM when it comes to acquisition and security. To that end, DSS has formulated a plan to resolve these problems by instituting a wholesale education process, beginning with DoD's senior acquisition executives and progressing through its contractors, to assist in understanding NISPOM requirements. Also, he described a very effective government/industry forum conducted by the ODNI community that presented a classified summary on threats to our industrial base. He then noted that DSS has presented an update from its field operations that addressed many of the concerns mentioned by

Mr. Conway, especially regarding how they execute their oversight program, to include the CUI program, which they want to be prepared for when that program comes fully online. Further, he noted that both partners recognize there is a shared challenge relating to protecting intellectual property within industry, and that intellectual property is what makes industry such a strong component of national security policy. In addition, he stated that DSS expects to initiate a panel discussion at the next AIA meeting for in depth discussions on the protection of intellectual property in industry.

Finally, he advised that the DoD, Industry, and the ODNI communities have begun discussions on exploring each other's roles pertinent to information sharing. He noted that DSS has to ensure that our government partners are sharing with DSS, so that the former can then pass complete and timely information to industry and noted their greatest impediment is secure communications between government and industry. Kimberly Baugher, DOS asked which internal agencies had been involved in this forum. Mr. Sims responded that many DoD agencies were represented as well as all of the NISP signatories. Ms Baugher then asked that the DOS be notified of future meetings. To this the Chair requested that the participatory list be amended to include all current NISPPAC members, so that all can remain abreast of the forum's progress. The Chair then called for the DSS Operations Analysis Group (OAG) briefing.

B) The DSS OAG Briefing

Mike Buckley, DSS, presented a briefing describing the activities of the DSS OAG (Attachment 8). He described the focus of the Group's mission as the management of risk across the operational components of DSS. The OAG is composed of adjudicators, counterintelligence specialists, industry security representatives, and policy personnel. It focuses on incident reports that go directly to DISCO, suspicious contact cases that are received by counterintelligence specialists, and security violations received by industrial security representatives. He described the information the Group studies as having met or exceeded a predetermined threshold and one which clearly has ramifications across several security disciplines. To date, that threshold has been met in only about 500 of the approximately 19,000 suspicious contact reports brought to its attention. In addition to each case having counterintelligence, industrial security, and policy implications, it will generally involve training, situational awareness, and threat perspectives.

He further explained that the OAG has developed a standard operating procedure, and an implementing directive that is awaiting formal signature. This directive has established 19 single line items or thresholds that DSS expects its field personnel to forward to the OAG subsequent to their completed case action. Some of the most important of these items involve suspicious foreign travel by cleared personnel to foreign intelligence priority countries, credible and relevant reports that suggest the unauthorized disclosure, theft, loss, or compromise of classified information to a foreign power, an agent of a foreign power, or an unauthorized recipient, and information indicating a pattern of neglect, willful disregard, or deliberate improper handling or storage of protected information. In addition, other important threshold items include information, incidents, or reporting anomalies concerning companies or personnel under the purview of the NISP that may result in adverse media attention, senior government or congressional interests, and the unauthorized penetration of information systems containing

classified information or information critical to national security, when the involvement of a foreign power, or terrorist group and/or individuals acting on their behalf, cannot be ruled out.

He then outlined the specific types of vulnerabilities that the OAG has identified throughout FY 2011 and the first quarter of FY 2012 that reached its threshold level, including security violations, unclassified cyber intrusions, insufficiently cleared key management personnel, International Trade and Arms Regulations (ITAR) irregularities, and others. He explained that all vulnerabilities, both internal and external, that reach the OAG's threshold, are tracked from introduction to resolution, and that said resolutions involve everything from working with other government agencies that are investigating the same incident and providing case studies to the Center for the Development of Security Excellence for inclusion in their training plan, to performing security advice and assist exercises for industrial facilities. The Chair then asked for Pat Viscuso, ISOO, to provide an update on the development of the CUI process.

C) CUI Update

Dr. Viscuso stated that on November 4, 2010 the President issued E.O. 13556, "Controlled Unclassified Information," to address the growing concerns caused by the patchwork of control systems and markings historically used for sensitive but unclassified information throughout the Executive branch. The solution was the establishment of a CUI program. The Order outlined several program elements, among which were a registry of CUI categories and subcategories. These categories and subcategories are established in accordance with law, government-wide regulation, or policy, but exclude Freedom of Information (FOIA) materials. He added that the Department of Justice has assisted in clarifying this point, and a joint memorandum has been issued that mandates that CUI and FOIA markings are not to be associated. Next, he provided that there are currently 16 categories and 79 subcategories of CUI information which all government agencies had the opportunity to provide input, and that as this process is ongoing, it is likely these numbers will increase. Further, to ensure process consistency, within 180 days of the issuance of the E.O., and in consultation with federal government entities, state, local, tribal, and private sector officials, and in coordination with OMB, the Executive Agent (EA) issued implementation policy.

Dr. Viscuso then drew a timeline of this initiative to a level of policy hierarchy, progressing from the E.O. to an EA implementation directive, to the current project phase, ultimately resulting in a new directive that will contain instructions governing CUI safeguarding, dissemination, decontrol, and markings. He explained that to achieve this objective, the CUI office will establish several working groups, the first of which is already operating, and concentrating its efforts on safeguarding. It is hoped that this entire project will be completed in the fall of 2012. He noted that the CUI development project contained one additional element: the requirement that all government agencies having any involvement in sensitive but unclassified materials would develop and submit to the EA target-dated compliance plans. The CUI office would then liaison with OMB to establish overall implementation deadlines. He added that the CUI office, in consultation with OMB, is in the midst of evaluating the 55 compliance plans that were submitted. Upon completion of all implementation guidance, agencies will be best equipped to establish firm compliance target dates. He noted that, at that point the CUI office will be able to

coordinate with OMB to establish final Executive branch implementation deadlines. The Chair added that once we arrive at the establishment of implementation guidance, the impact on industry will begin to be appreciated, as their operations personnel will establish their compliance timelines. Finally, Dr. Viscuso mentioned that all phases of this process have been developed through ongoing consultations with industry officials, and that they will continue to be full participants in the establishment of CUI policy.

Fred Riccardi, Industry, then voiced two industry concerns: fear that the CUI initiative could in any way become tied to FOIA, and hope that final agency compliance plans will avoid conflicting industry approaches. Dr. Viscuso responded that the CUI office's partnership with OMB has ensured that these concerns would not become a part of final policy, and the Chair added that once the interagency has completed the basic procedural framework, industry will get to see where the whole concept is heading and to help government ensure that nothing is missing or misaligned. He then called for Steve Lewis to provide the DoD and NISPOM updates.

E) DoD Update

Mr. Lewis presented an update on the DFARS, in which he stated that subsequent to an additional December 2011 round of public comments, the DFARS committee began considering changing the Supplement. He noted that there were many industry comments, and thus the process is ongoing. He next discussed the rewrite of the NISPOM, and indicated that during the Fall of 2011 all NISPOM comments had been adjudicated, except for those relative to Chapter 10, which has been set aside and thus not ready for additional review by the NISPPAC working group. He noted that industry had filed approximately 39 reclama comments voicing dissatisfaction with the adjudication decisions. These comments concerned law, regulation, or failure to acknowledge information previously agreed to by the NISPOM working group. All of these have now been examined, and a small number still require some additional consideration that are expected to be addressed within a few days. Once that is achieved, we will be sharing the final adjudication comments, along with an annotated NISPOM change document, followed by movement forward to the formal coordination process. Next, he spoke to the October 2012 requirement that all non-GSA approved security containers must be deactivated. He explained that we have generated guidance that will permit implementation of the new open storage provisions that are in the draft NISPOM, thus providing industry another option for managing the transition. He concluded with an explanation of recent DoD attention to implementation of the United Kingdom Defense Trade Cooperation Treaty that requires some DoD information security program manual changes, and will prompt issuance of an Industrial Security Letter (ISL). That letter, was just signed, amends the ITAR to allow for an additional exemption on exports to a select United Kingdom (UK) community, and includes the specific government activities and cleared contractor facilities. It essentially advises industry of the existence of the new ITAR exemption, and passes along the key components.

V. Closing Remarks, Action Items Review, and Adjournment

The Chair reminded the assembled that as this meeting is open to the public he asked if any guests and/or other Committee members wanted to provide additional comments/ questions or

concerns. Recognizing none, he briefly reviewed the action items to be addressed prior to and during the next NISPPAC. Included among these are an enhanced metrics presentation for both the PCLWG and the CAWG that will include an observations and takeaway chart, a report on the results of a PCLWG and DISCO dialogue that promotes common concerns on issues related to fingerprint processing, and an examination into possible ways to properly track the progress on JPAS developments to determine whether there are any issues. There being no other questions or points of information, the Chair announced the next NISPPAC meeting as July 11, 2012, with the working groups typically meeting roughly six to eight weeks prior. The meeting was adjourned at 12:27 pm.

Summary of Action Items

1. The PCLWG and the CAWG will each develop an observations and takeaway chart that collects all analysis data and provides a more complete and informative picture.

2. The PCLWG will provide a report on the results of its dialogue with DISCO regarding common concerns on issues related to fingerprint processing.

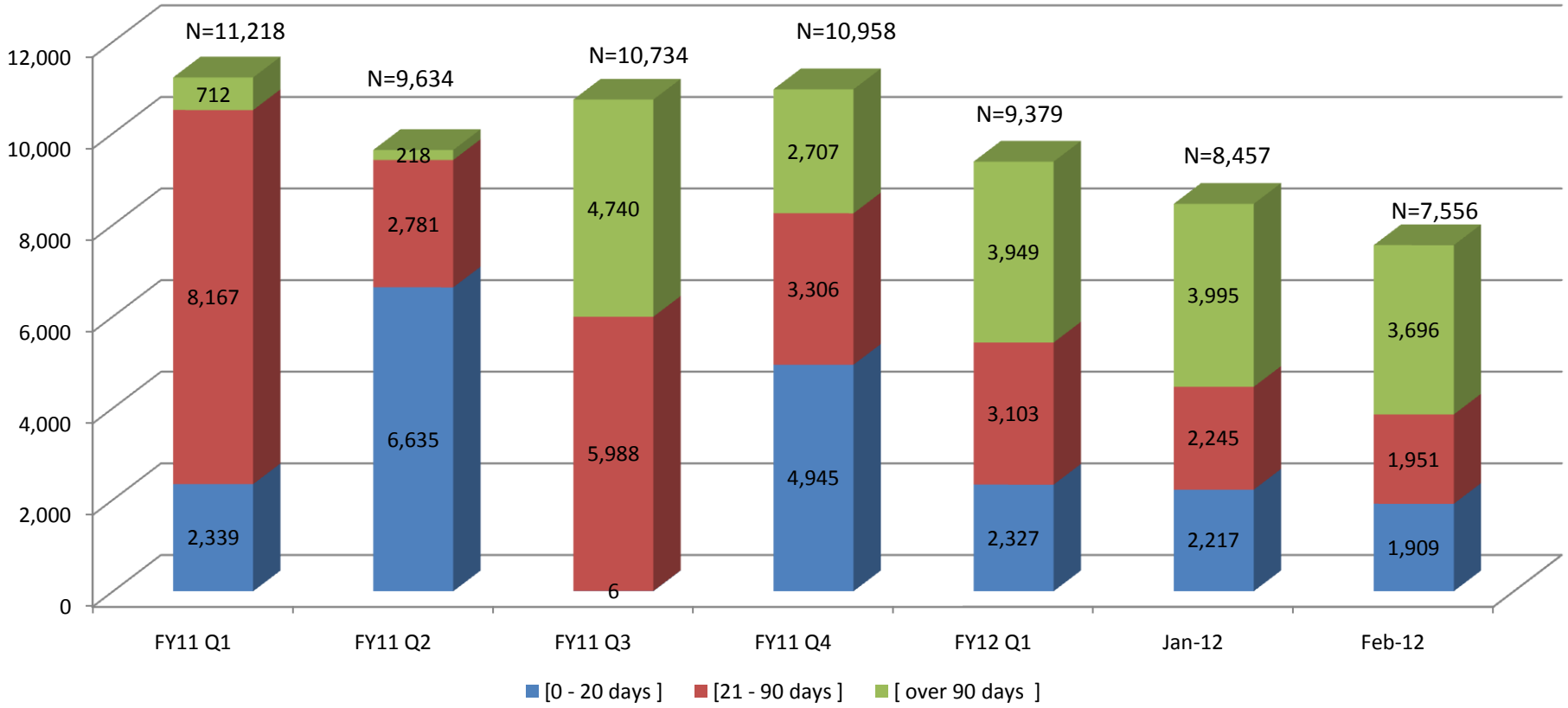
3. DISCO will provide an examination into possible ways to properly track the progress on JPAS developments to determine whether we have any issues on that front.

Attachment 1- DISCO PCL Presentation

Defense Industrial Security Clearance Office

FY11-FY12 Initial Pending Adjudications

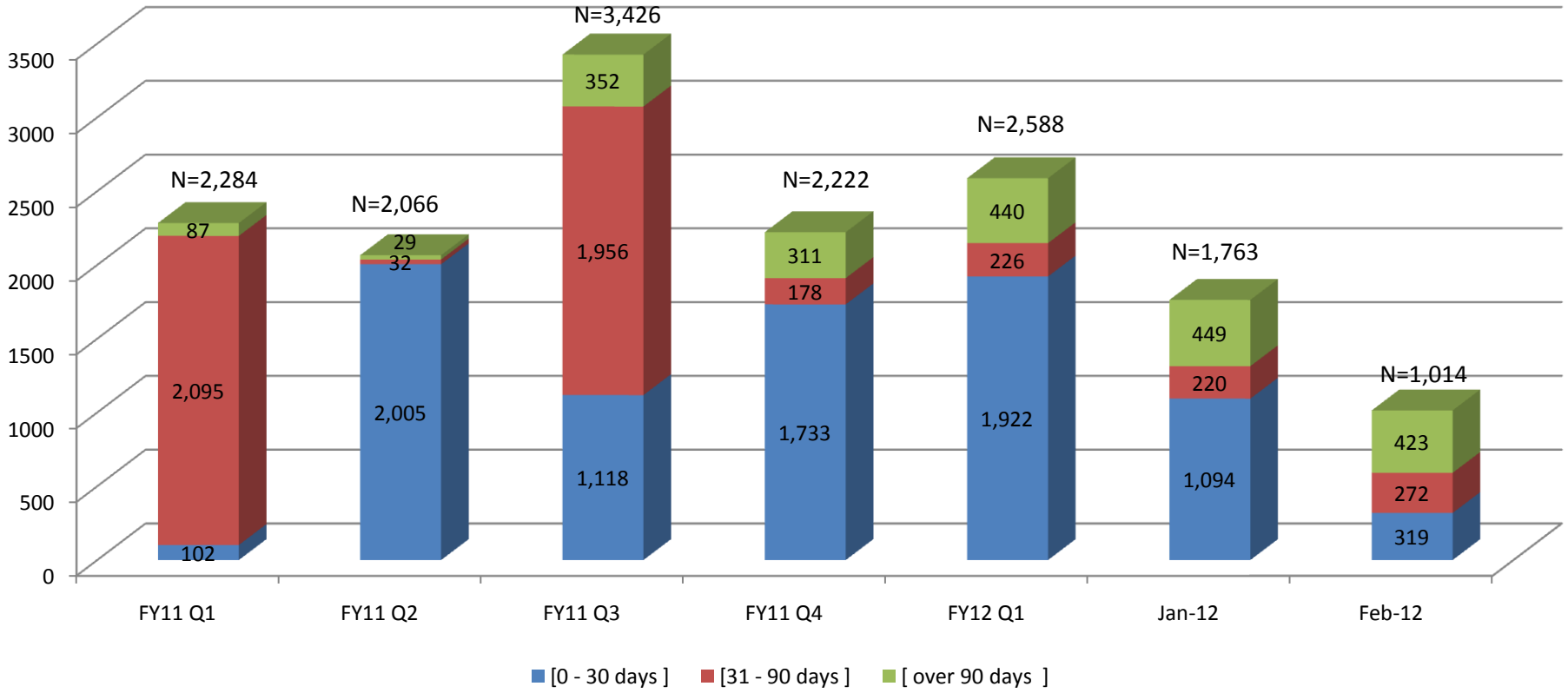
SSBI / NACLC



Case Type	Day Category	FY11 Q1	FY11 Q2	FY11 Q3	FY11 Q4	FY12 Q1	Jan-12	Feb-12
Initial (SSBI and NACLC)	[0 - 20 days]	2,339	6,635	6	4,945	2,327	2,217	1,909
	[21 - 90 days]	8,167	2,781	5,988	3,306	3,103	2,245	1,951
	[over 90 days]	712	218	4,740	2,707	3,949	3,995	3,696
Initial Total		**11,218**	**9,634**	**10,734**	**10,958**	**9,379**	**8,457**	**7,556**

FY11-FY12 Renewal Pending Adjudications

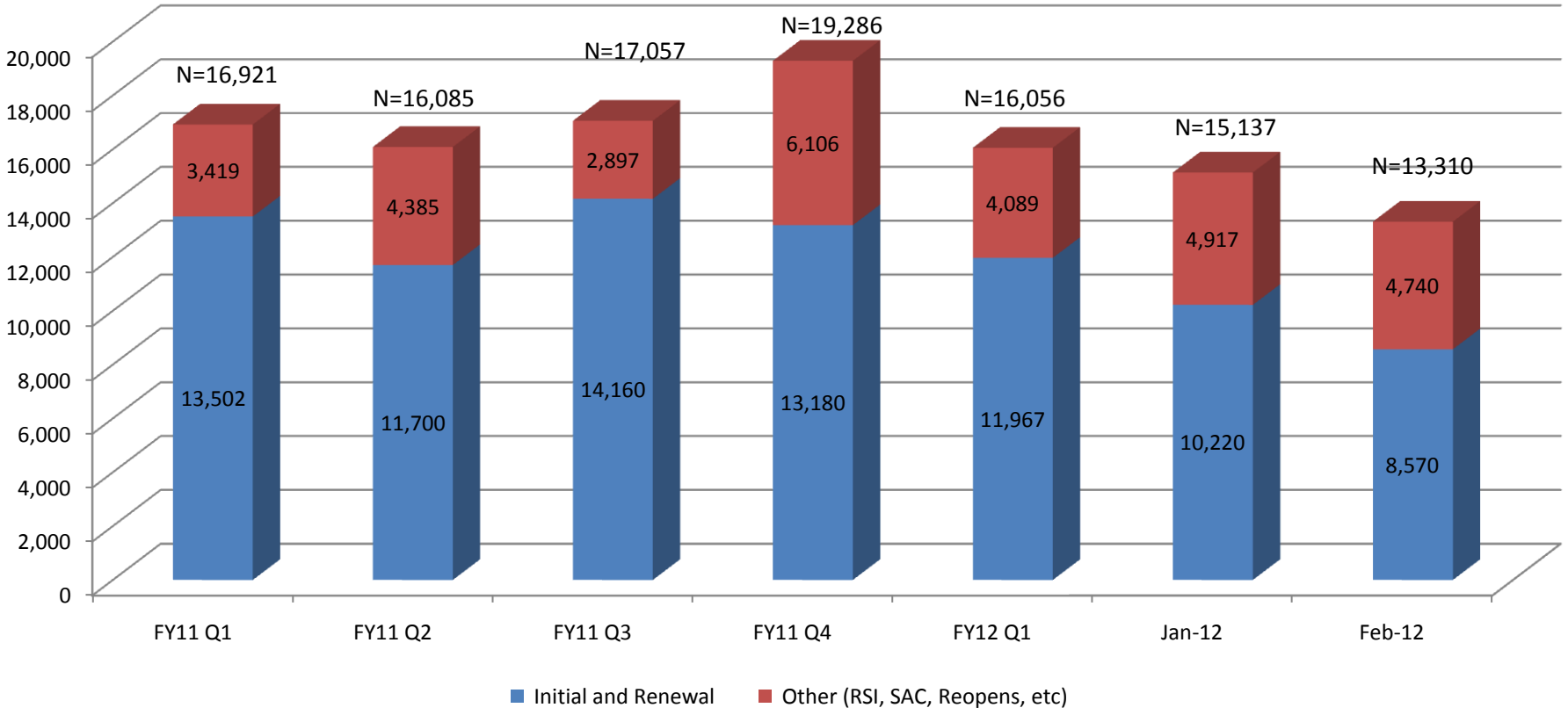
SBPR / PPR



Case Type	Day Category	FY11 Q1	FY11 Q2	FY11 Q3	FY11 Q4	FY12 Q1	Jan-12	Feb-12
Renewal (SBPR and PPR)	[0 - 30 days]	102	2,005	1,118	1,733	1,922	1,094	319
	[31 - 90 days]	2,095	32	1,956	178	226	220	272
	[over 90 days]	87	29	352	311	440	449	423
Renewal Total		**2,284**	**2,066**	**3,426**	**2,222**	**2,588**	**1,763**	**1,014**

FY11-FY12 Overall Pending Adjudications

SSBI / NACLC / TSPR / Other (Suspended Cases)



Case Type	FY11 Q1	FY11 Q2	FY11 Q3	FY11 Q4	FY12 Q1	Jan-12	Feb-12
Initial and Renewal	13,502	11,700	14,160	13,180	11,967	10,220	8,570
Other (RSI, SAC, Reopens, etc)	3,419	4,385	2,897	6,106	4,089	4,917	4,740
Total	**16,921**	**16,085**	**17,057**	**19,286**	**16,056**	**15,137**	**13,310**

Defense Industrial Security Clearance Office

FY11-FY12 Industry Cases Pending at OPM

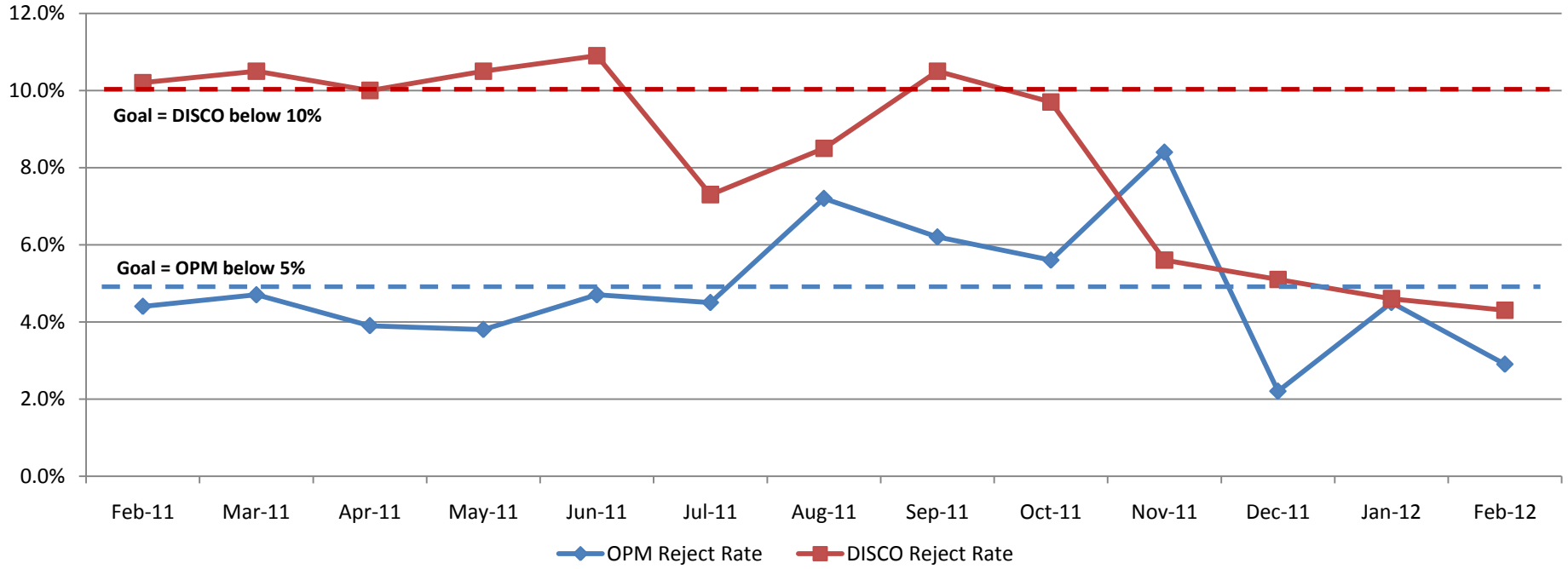
Case Type	FY09				FY10				FY11				FY12		Delta FY11Q1 vs FY12 February
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Feb-12	
NACLC	13,209	13,982	13,900	12,307	11,730	11,685	13,016	13,556	13,118	13,243	13,861	12,929	10,990	10,919	-17%
SSBI	6,626	6,687	6,944	6,561	6,782	7,012	6,561	6,178	6,308	5,578	6,274	5,821	5,292	5,279	-16%
SSBI-PR	3,772	4,160	4,692	3,703	4,096	4,521	4,859	5,115	5,436	7,521	4,662	4,349	4,750	4,717	-13%
Phased PR	5,430	2,771	2,476	2,640	3,158	3,629	3,665	4,248	4,781	5,148	4,097	5,768	8,937	10,278	*115%*
Total Pending	29,037	27,600	28,012	25,211	25,766	26,847	28,101	29,097	29,643	31,490	28,894	28,867	29,969	31,193	5%

NACLC, SSBI, TSPR inventory combined increased 5% from FY11 Q1 to February FY12.

Source: OPM Customer Support Group

FY11-FY12 DISCO and OPM Reject Rates

Initial and Periodic Reinvestigation Clearance Requests



- FY12 - DISCO Received 75,576 investigation requests
  - Rejects – DISCO rejected 4,513 (6%) investigation requests for FSO re-submittal

- FY12 - OPM Received 73,734 investigation requests
  - Rejects – OPM rejected 3,576 (4.8%) investigation requests to DISCO (then FSO) for re-submittal
  - Unacceptable fingerprint cards and fingerprint cards not submitted with the required timeframe account for an estimated 84% of rejections by OPM.

Note: Case rejection and re-submission times is not reflected in timeliness
- When a case is re-submitted, the timeline restarts for the PSI/PCL process
- Source: JPAS / OPM / DISCO Monthly Reports

FY12 DISCO Case Rejections by Facility Category

Month	Facility Category						
	A	AA	B	C	D	E	Others
October	1.7%	0.8%	1.0%	3.5%	8.9%	16.4%	0.1%
November	0.9%	0.4%	0.5%	1.7%	4.8%	8.9%	0.1%
December	1.0%	0.4%	0.6%	1.6%	4.8%	9.0%	0.1%
January	0.5%	0.4%	0.6%	1.0%	4.6%	9.0%	0.0%
February	0.8%	0.5%	0.5%	1.6%	4.7%	8.7%	0.0%
Grand Total	**4.9%**	**2.4%**	**3.2%**	**9.4%**	**27.8%**	**52.0%**	**0.3%**

DISCO Case Rejections

- **79.8% of cases rejected by DISCO originate from smaller Category D and E facilities**

Source: e-Qip

FY12 Reasons for Case Rejection by DISCO

TOP 10 REASONS FOR DISCO REJECTION OF INVESTIGATION REQUEST		
Reason	**Count**	**Percent**
Missing employment information	1,155	36%
Missing family member information	432	13%
Missing financial information	424	13%
Missing cohabitant information	353	11%
Missing Selective Service registration or legal exemption	263	8%
Certification / Release form request number is incorrect	156	5%
Certification / Release forms are illegible	136	4%
Missing education information	133	4%
Certification / Release forms not submitted	131	4%
Name different on Certification / Release forms and SF-86	37	1%
Total	**3,220**	**99%**

- 49% are attributable to missing current employment activity and family member information
- Top 10 reasons account for 99% of DISCO's case rejections

FY12 Reasons for Case Rejection by OPM

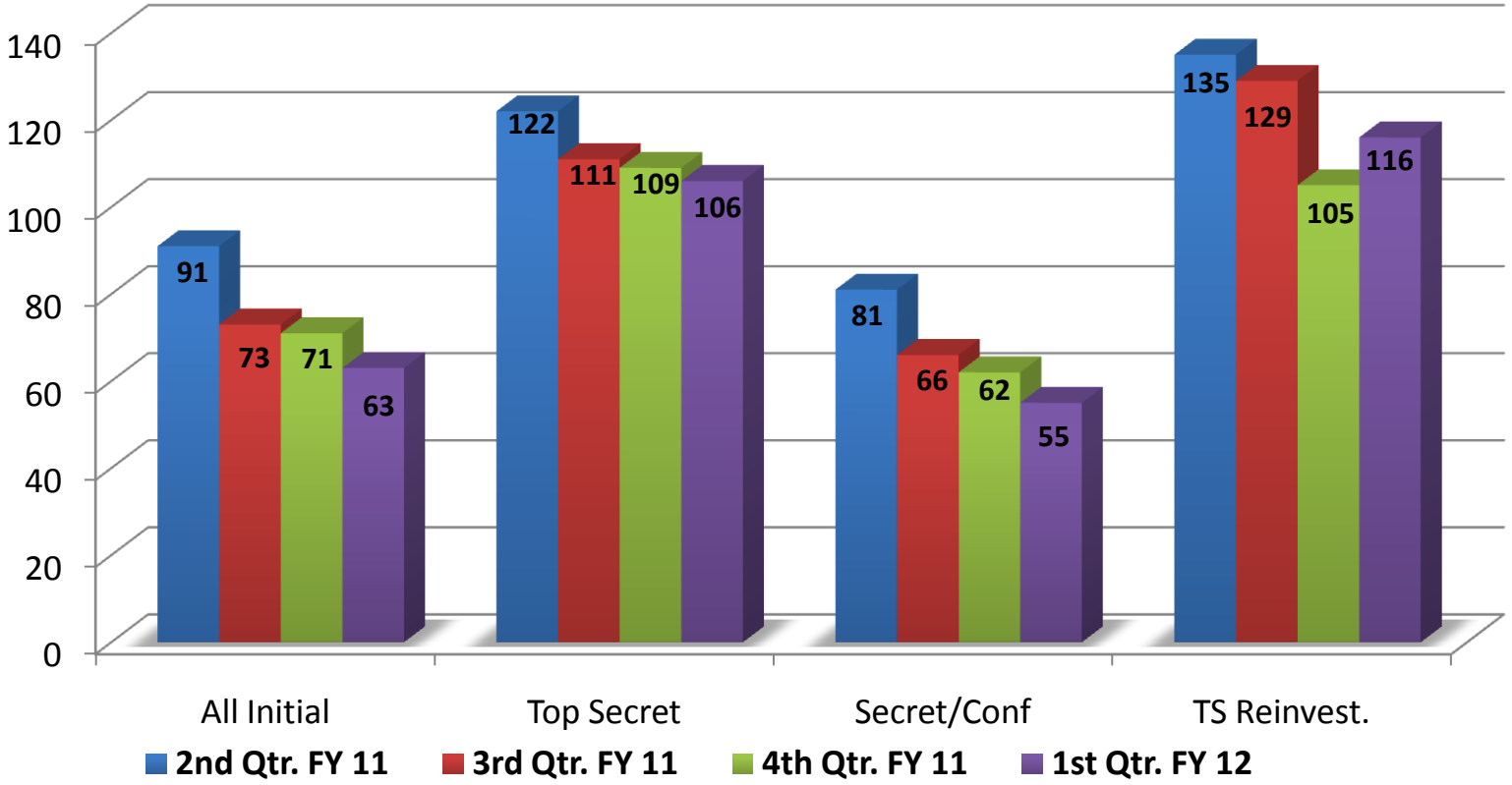
TOP 10 REASONS FOR OPM REJECTION OF INVESTIGATION REQUEST		
Reason	**Count**	**Percent**
Fingerprint card not acceptable	1,192	59%
Fingerprints not submitted within required timeframe	508	25%
Certification / Release forms are illegible	96	5%
Certification / Release forms do not meet date requirements	51	3%
Discrepancy with the subject's Place of Birth (POB)	45	2%
Discrepancy with the subject's Date of Birth (DOB)	24	1%
Certification / Release form request number is incorrect	24	1%
Missing reference information	17	1%
Certification / Release forms not submitted	16	1%
Missing employment information	6	0%
Total	**1,979**	**97%**

- **The majority of OPM case rejections are due to fingerprint cards.**

Attachment 2- OPM PCL Presentation

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

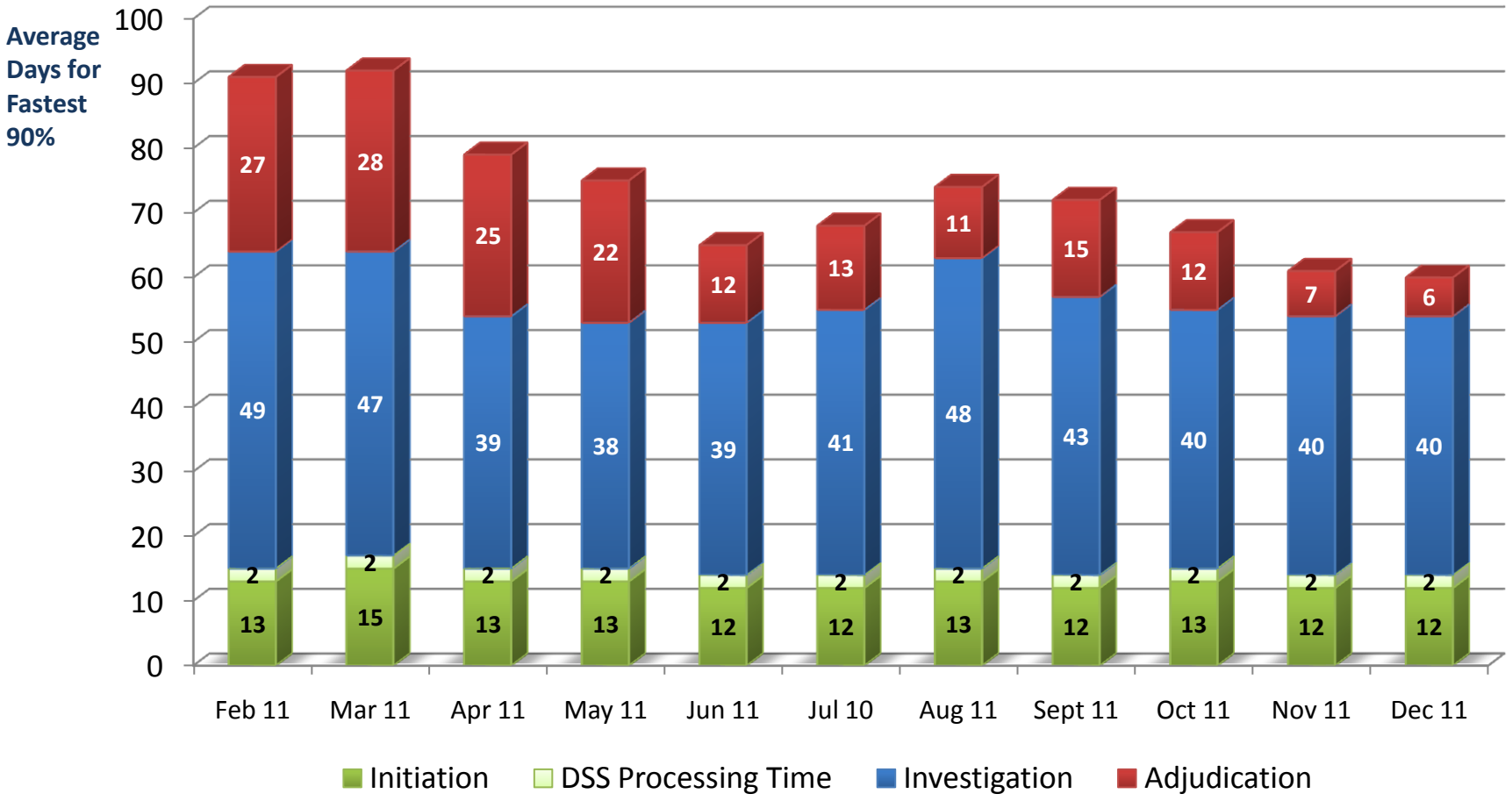
Average Days of Fastest 90% of Reported Clearance Decisions Made



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

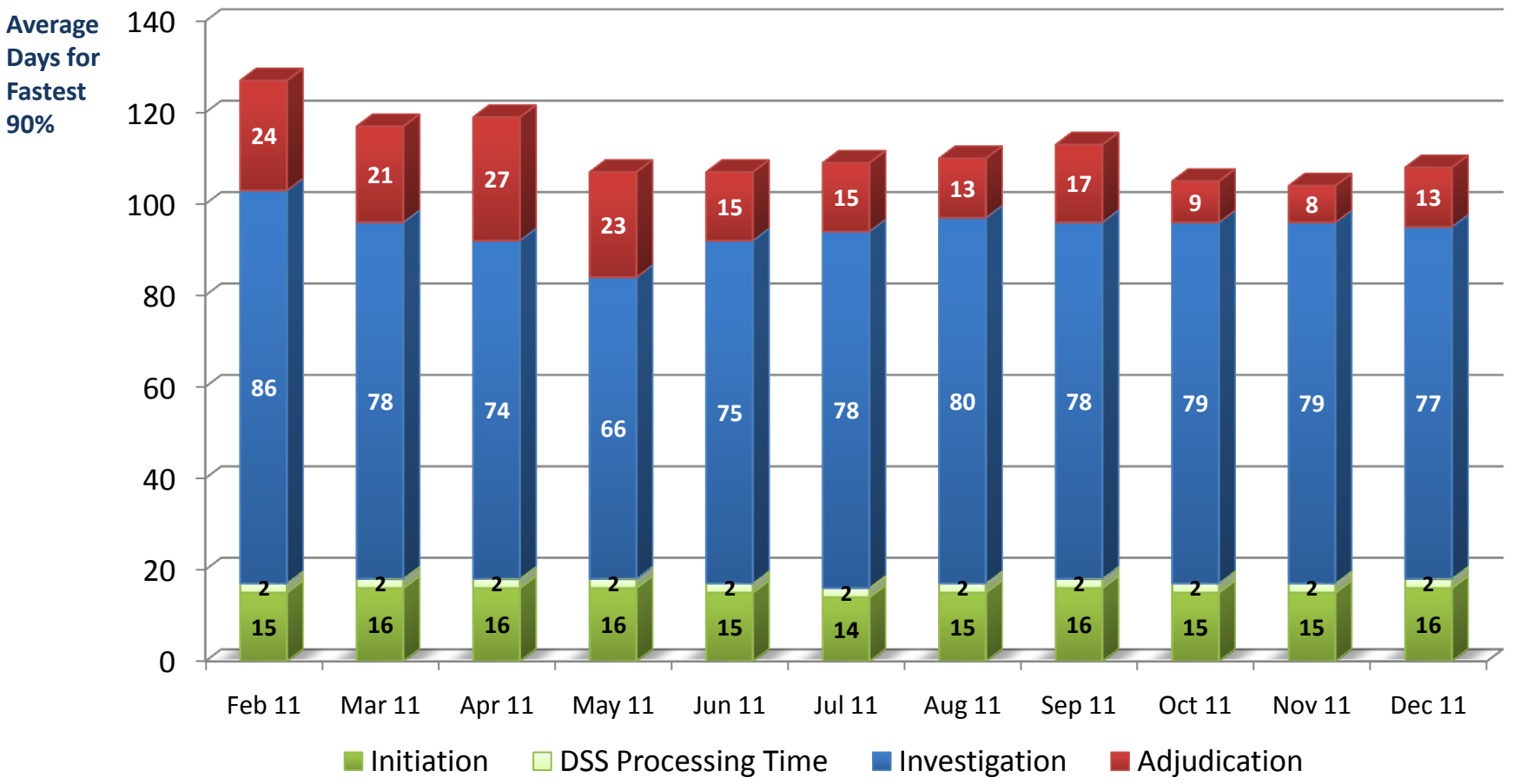
*The adjudication timelines include collateral adjudication by DISCO and SCI adjudication by other DoD adjudication facilities

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



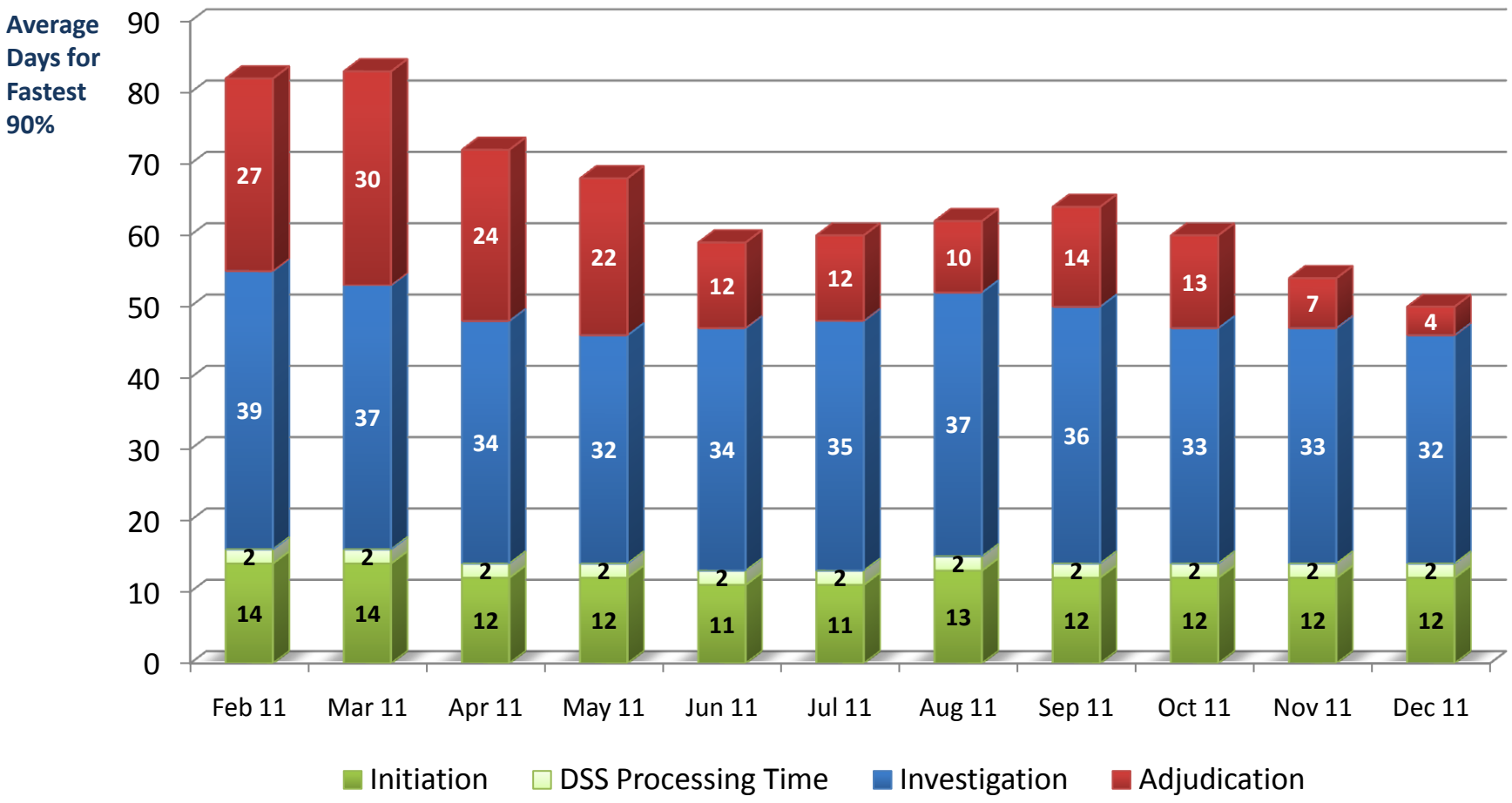
	Feb 11	Mar 11	Apr 11	May 11	Jun 11	Jul 11	Aug 11	Sept 11	Oct 11	Nov 11	Dec 11
100% of Reported Adjudications	8,100	11,678	11,737	11,907	12,358	8,917	8,952	5,116	12,158	9,776	10,106
Average Days for fastest 90%	91 days	92 days	79 days	75 days	65 days	68 days	74 days	72 days	67 days	61 days	60 days

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



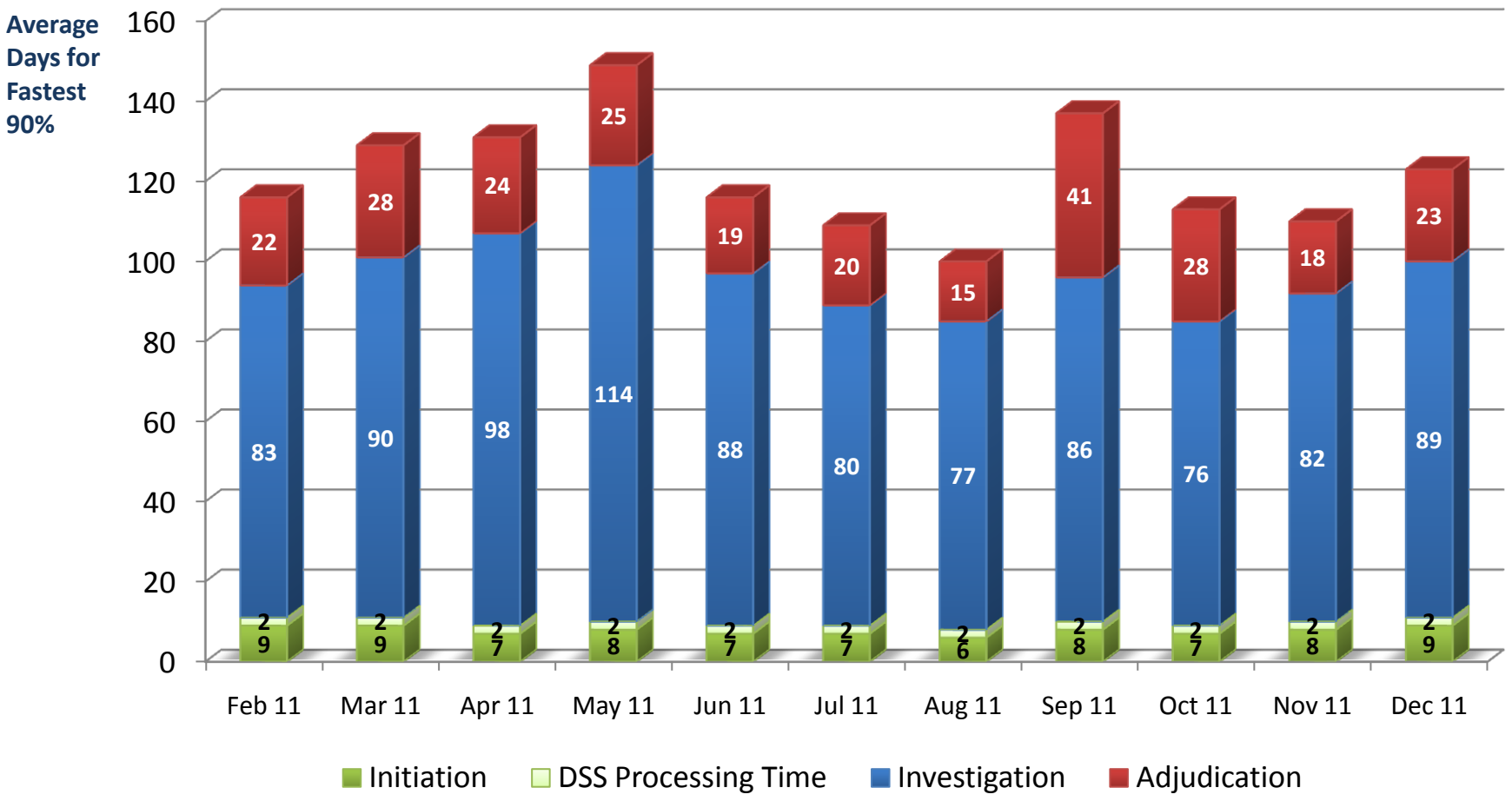
	Feb 11	Mar 11	Apr 11	May 11	Jun 11	Jul 11	Aug 11	Sept 11	Oct 11	Nov 11	Dec 11
100% of Reported Adjudications	1,776	2,943	1,714	2,301	1,743	1,511	2,166	898	2,035	1,514	1,837
Average Days for fastest 90%	127 days	117 days	119 days	107 days	107 days	109 days	110 days	113 days	105 days	104 days	108 days

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



	Feb 11	Mar 11	Apr 11	May 11	Jun 11	Jul 11	Aug 11	Sept 11	Oct 11	Nov 11	Dec 11
100% of Reported Adjudications	6,324	8,735	10,023	9,606	10,615	7,406	6,786	4,218	10,123	8,262	8,269
Average Days for fastest 90%	82 days	83 days	72 days	68 days	59 days	60 days	62 days	64 days	60 days	54 days	50 days

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



	Feb 11	Mar 11	Apr 11	May 11	Jun 11	Jul 11	Aug 11	Sept 11	Oct 11	Nov 11	Dec 11
100% of Reported Adjudications	3,133	1,902	3,362	3,097	5,585	1,841	3,051	921	3,278	2,046	2,958
Average Days for fastest 90%	116 days	129 days	131 days	149 days	116 days	109 days	100 days	137 days	113 days	110 days	123 days

Attachment # 3- ODNI Metrics for industry Performance

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

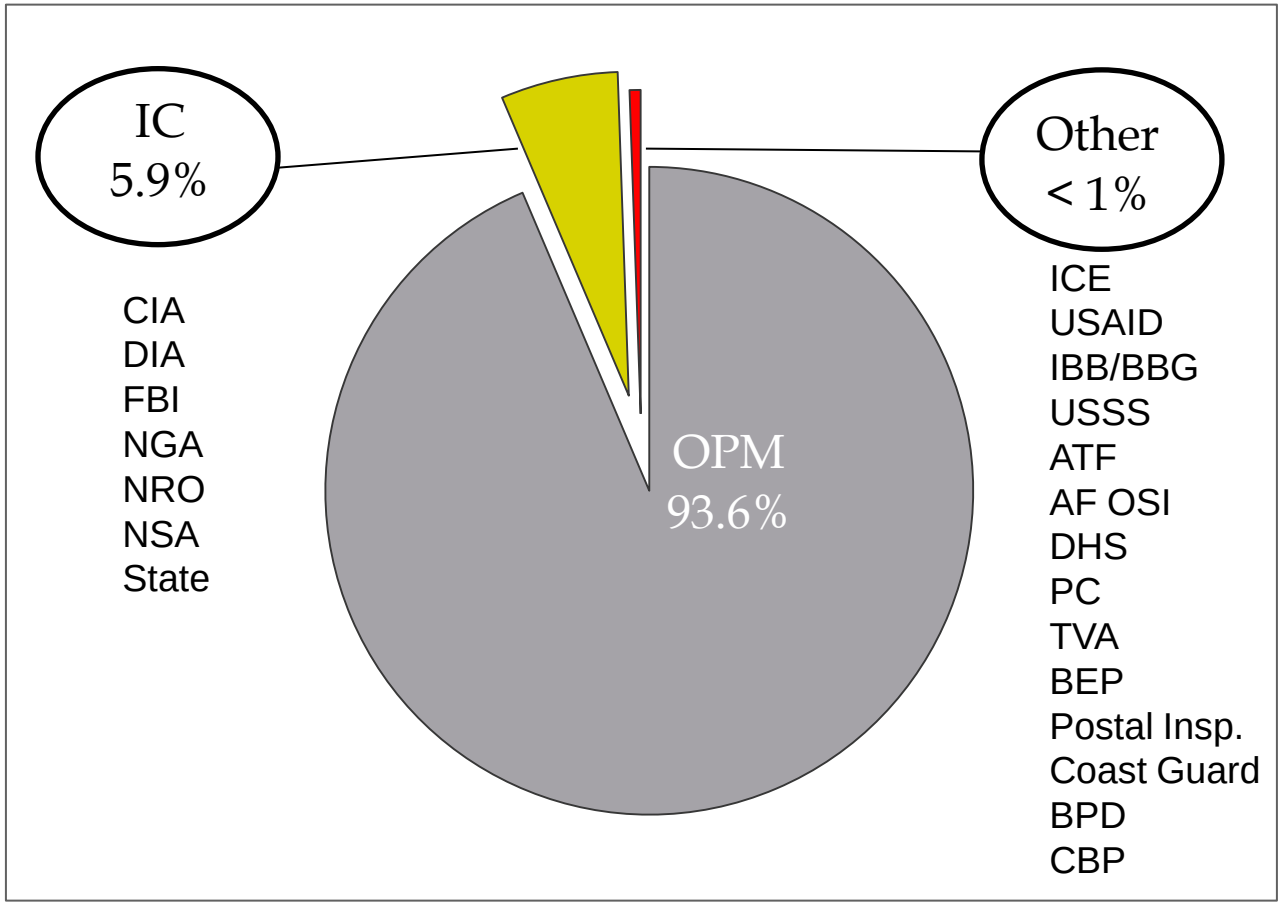
Industry Performance Metrics

ONCIX/Special Security Directorate

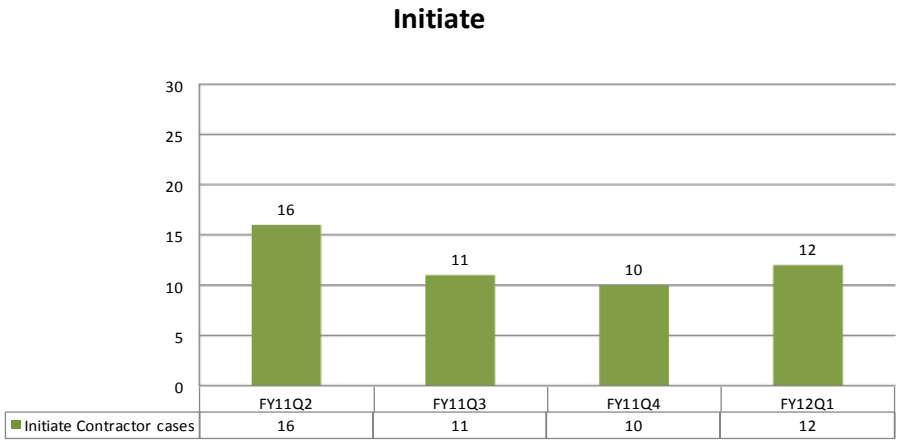
LEADING INTELLIGENCE INTEGRATION

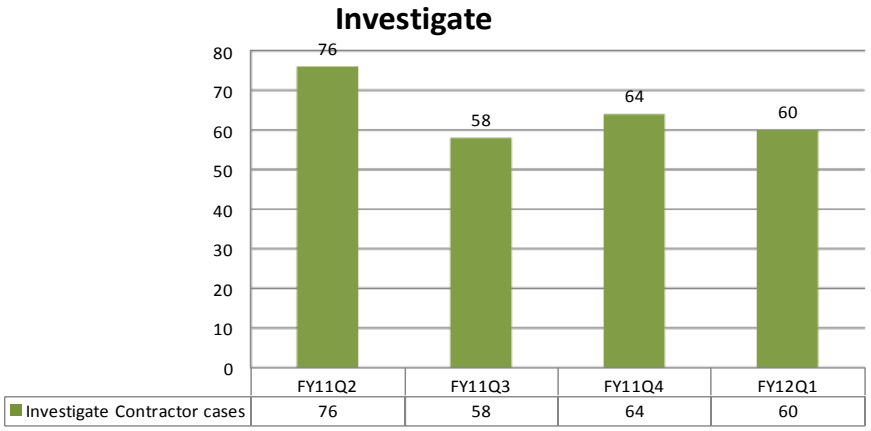
NISPPAC
21 March 2012

Overall Volume by ISP



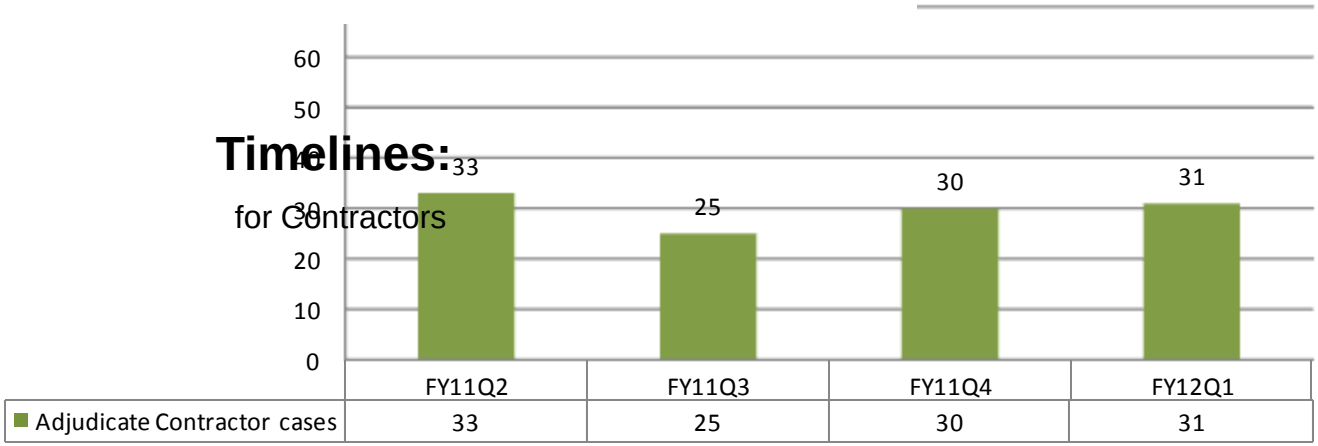
Intelligence Community
Combined Initials
(6% of USG Workload)





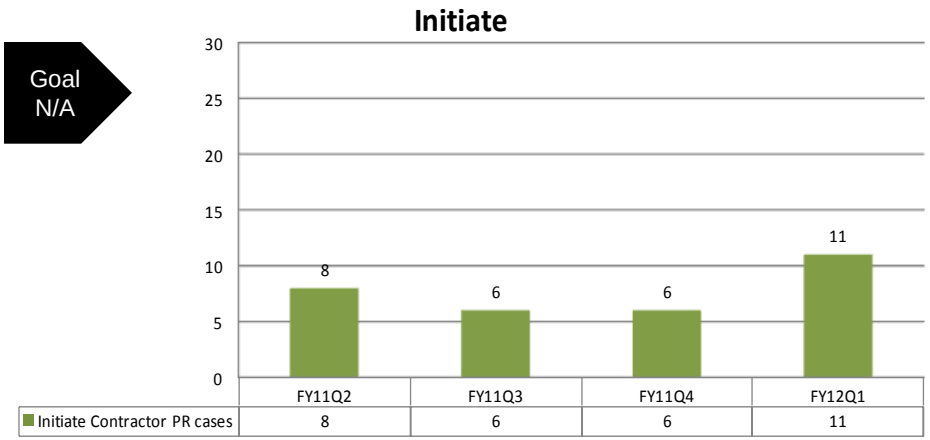
Timelines:

for Contractors

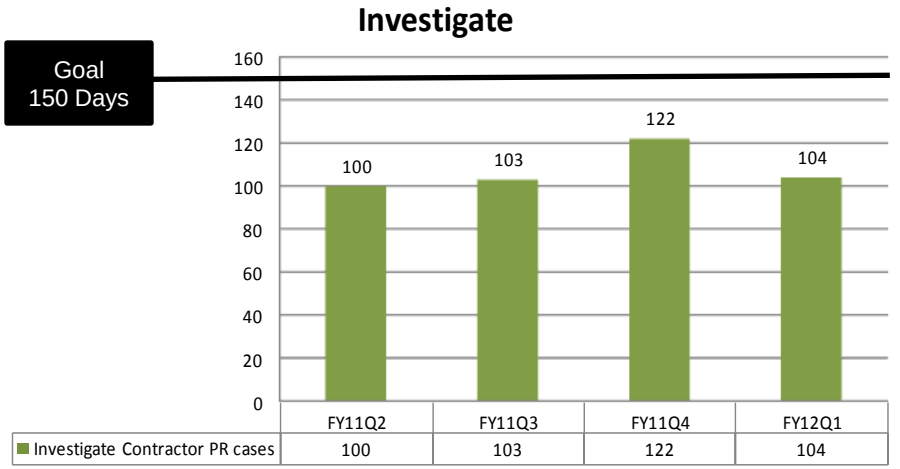


Intelligence Community
Combined Periodic Reinvestigations
(6% of USG Workload)

Goal N/A



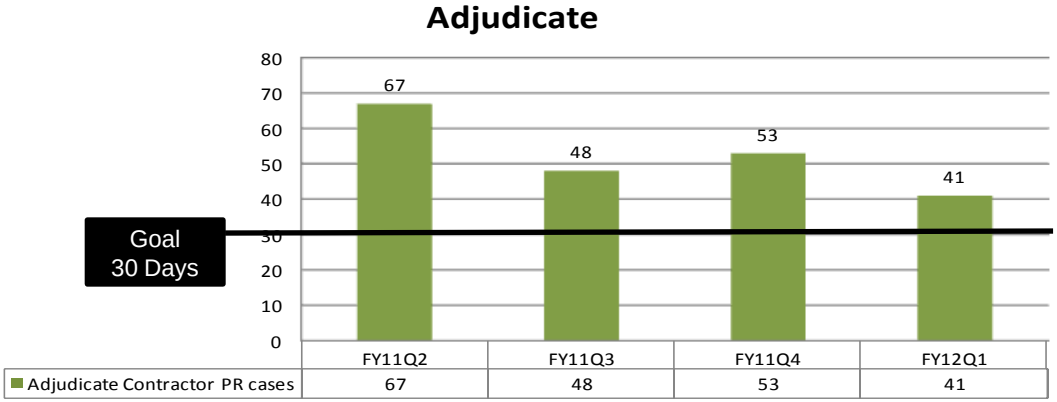
Goal 150 Days



Timelines:

for Contractors

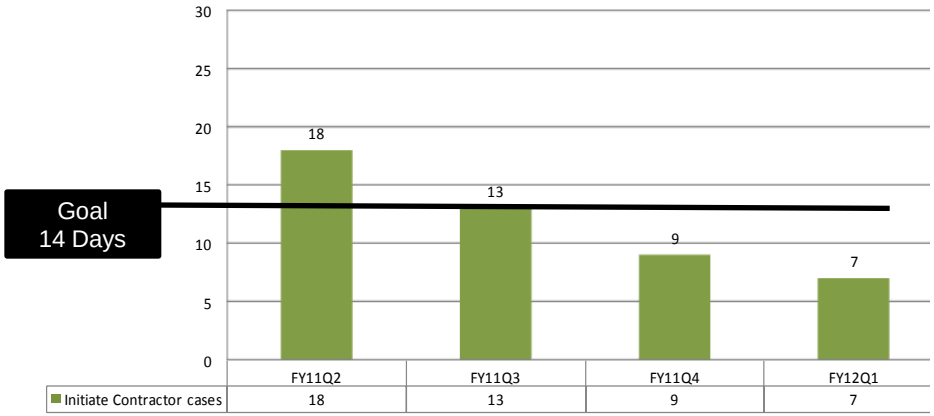
Goal 30 Days



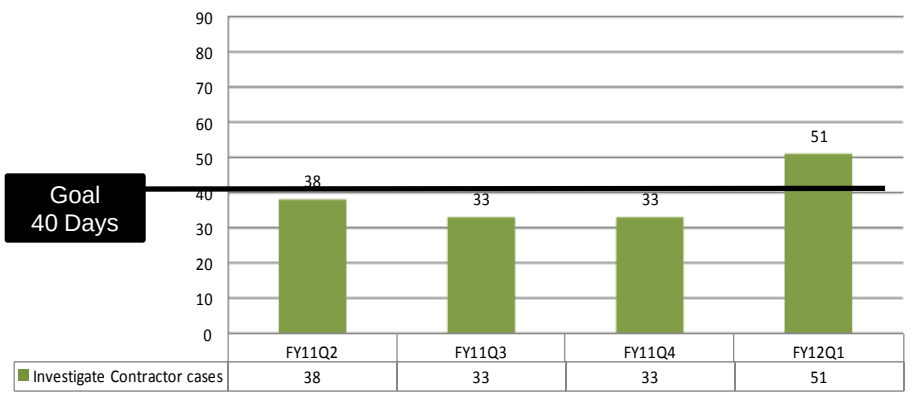
Other Delegated

(Less than 1% of USG Workload Combined Initials)

Initiate



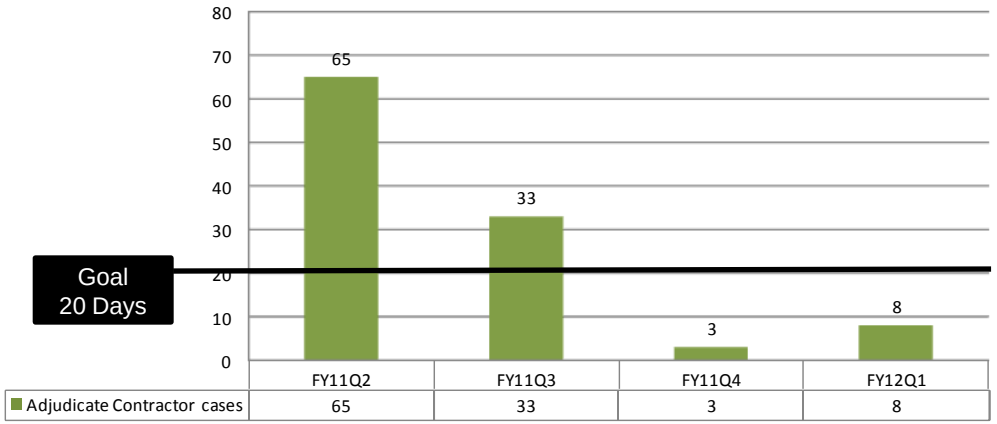
Investigate



Timelines:

for Contractors

Adjudicate

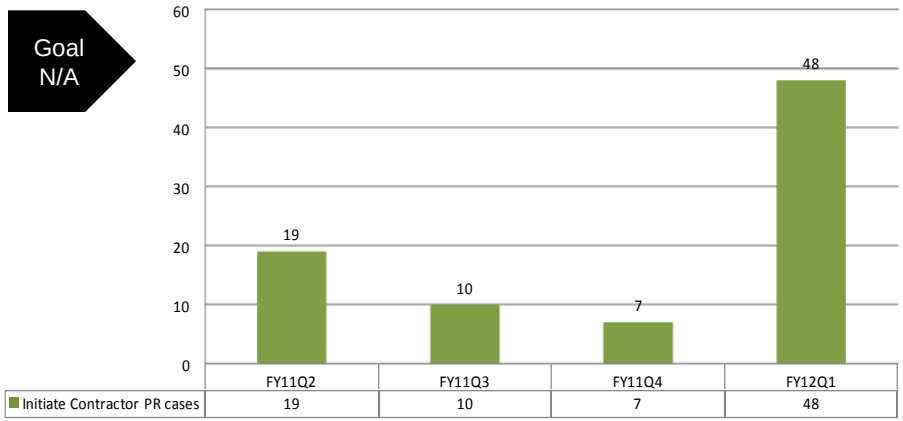


Other Delegated

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

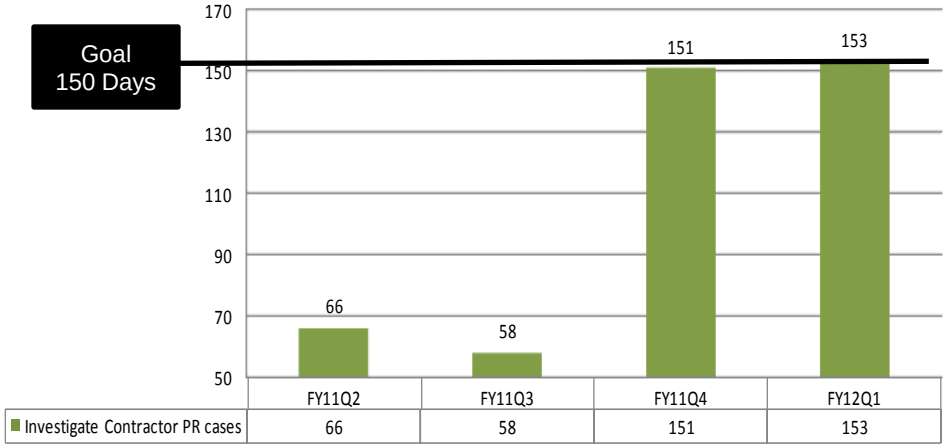
Initiate

Goal N/A



Investigate

Goal 150 Days

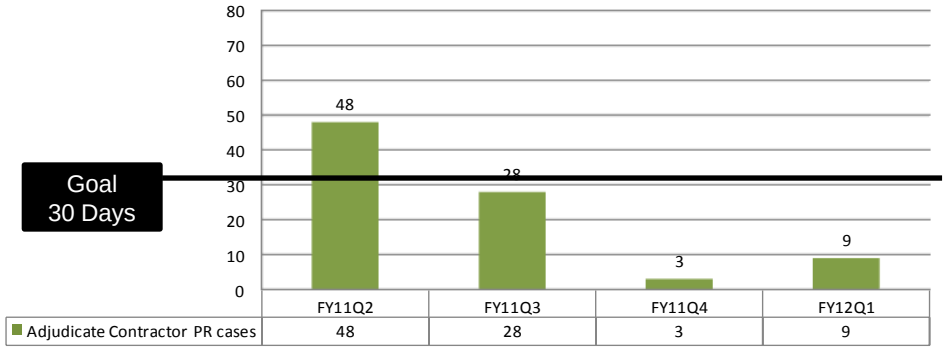


Timelines:

for Contractors

Adjudicate

Goal 30 Days



Attachment 4- Joint Reform and SEC Presentation

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Joint Reform & Security Executive Agent

LEADING INTELLIGENCE INTEGRATION

NISPPAC
March 21, 2012

Joint Reform Update

- Performance Accountability Council (PAC)
  - 6 March 2012 PAC meeting
  - Next Meeting
- Federal Investigative Standards
  - Current Status
  - Timeline
- Training Standards
  - Current Status
  - Timeline

Security Executive Agent Update

- Question 21, SF86 Revision
- Security Executive Agent Directive 1
- Security Executive Agent Website
  - www.ncix.gov
- Reciprocity Initiatives
- Phased PR Triggers
- Performance Metrics

Attachment 5- ODAA C&A Presentation

Defense Security Service

Industrial Security Field Operations (ISFO)

Office of the Designated Approving Authority (ODAA)

February 2012

Defense Security Service

Overview:

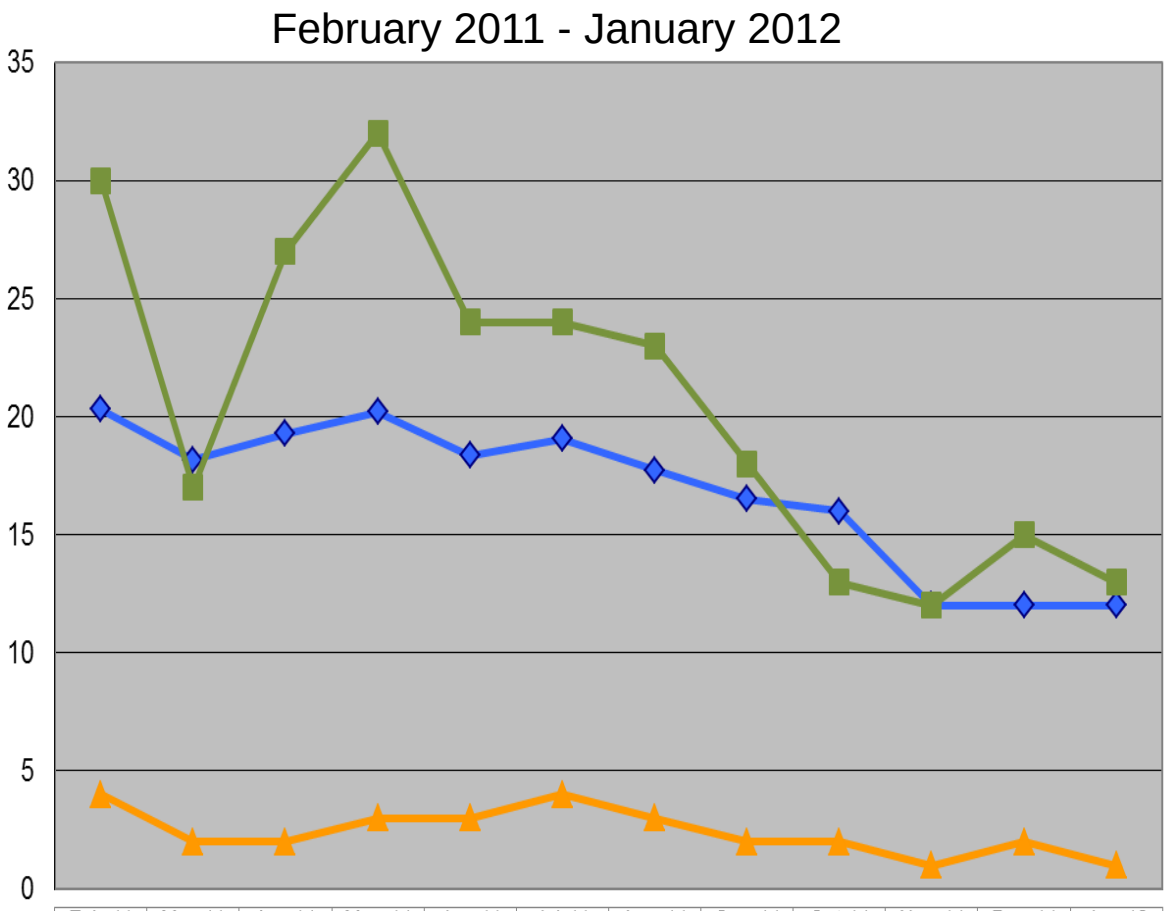
- Security Plan Reviews
  - Security Plan Processing Timeliness
  - Most Common Deficiencies Identified in Security Plans
  - Security Plan Denial and Rejection Rates
  - Second IATOs Issued
- System Onsite Validations
  - Timeliness
  - Most Common Vulnerabilities Identified

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

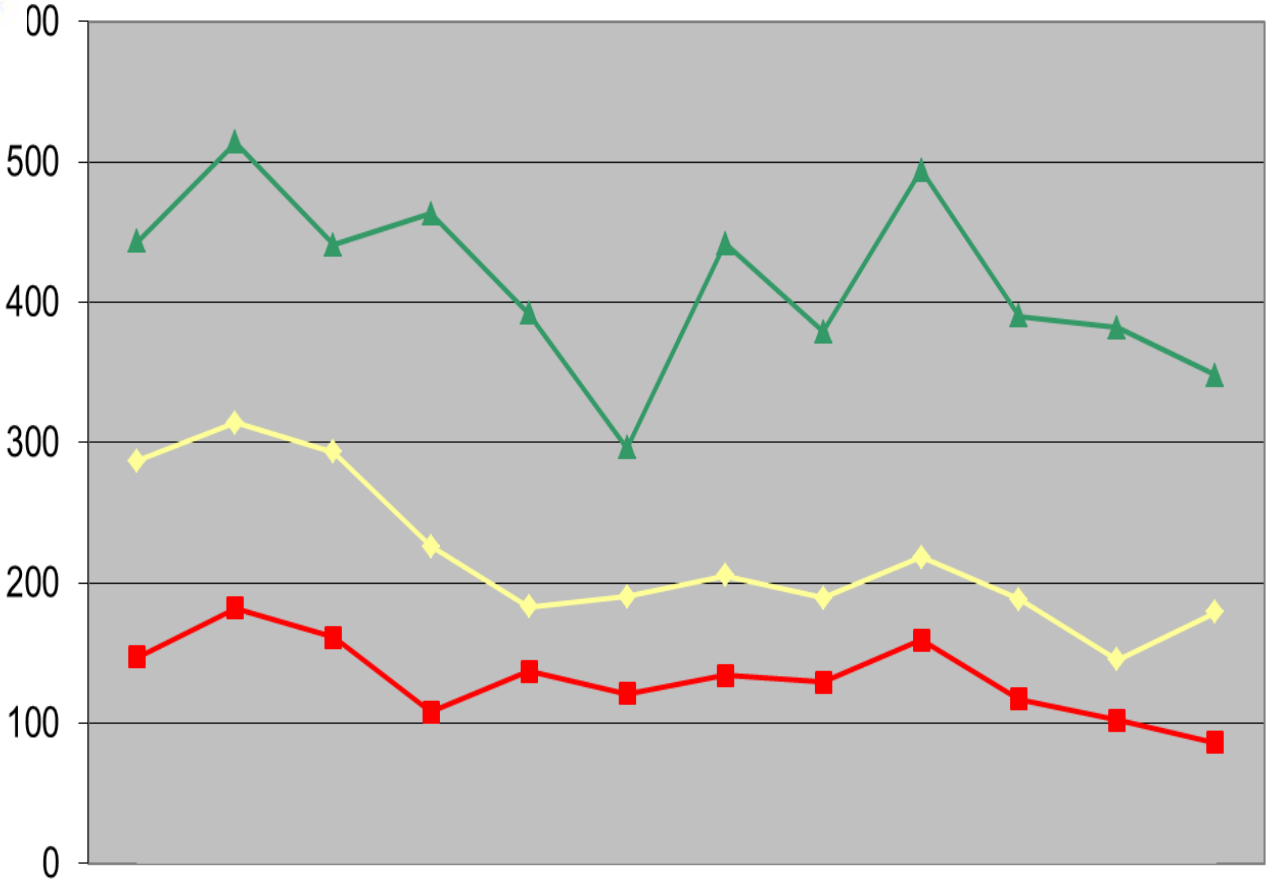


	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Jan-12
Time from DSS Receipt of plans to Granting of IATOs	20	18	19	20	18	19	18	17	16	12	12	12
Time from DSS Receipt of plans to Granting of SATOs	30	17	27	32	24	24	23	18	13	12	15	13
Industry Response Time to DSS Questions/Comments	4	2	2	3	3	4	3	2	2	1	2	1

- 3095 Interim approvals to operate (IATOs) were issued during the preceding 12 month period
- Across the 12 months, it took 17 days on average to issue an IATO after a plan was submitted
- For those systems going “Straight to ATO (SATO)” during the 12 months, it took an average of 19 days to issue the ATO
- 178 IATOs were granted in January with an average turnaround time of 12 days
- 136 SATOs were granted in January with an average turnaround time of 13 days

Results of Security Plan Reviews

February 2011 - January 2012

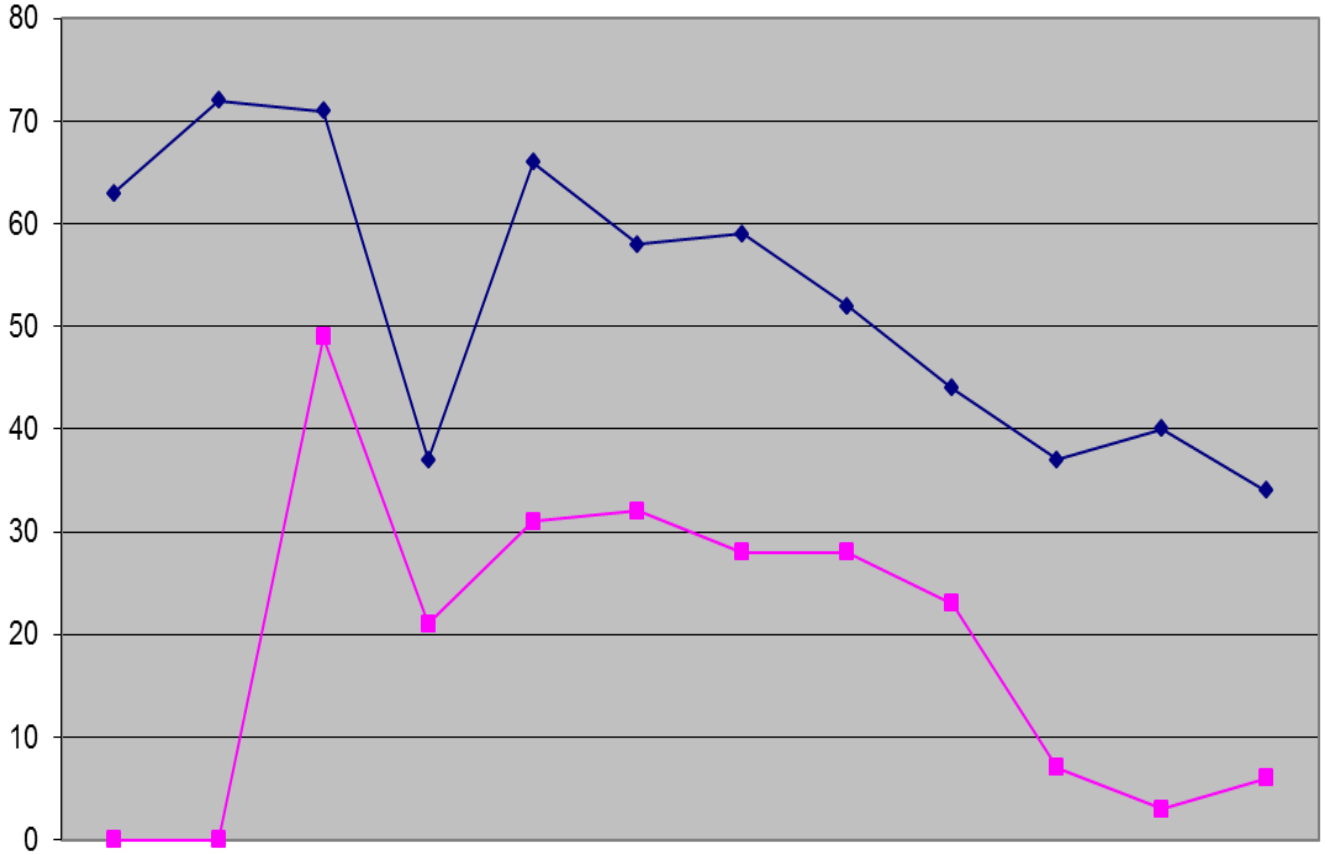


	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Jan-12
# Deficiencies	287	314	293	226	183	190	205	189	218	188	145	179
# Plans w/ Deficiencies	147	182	161	108	137	121	134	129	159	117	102	86
# Plans	443	514	441	463	392	296	442	379	494	390	382	348
Avg Deficiency per Plan	0.65	0.61	0.66	0.49	0.47	0.64	0.46	0.50	0.44	0.48	0.38	0.51

- 4984 System security plans (SSPs) were accepted and reviewed during the 12 months
- 1583 of the SSPs (32%) required some level of correction prior to conducting the onsite validation
- 950 SSPs (19%) were granted IATO with corrections required
- 633 (13%) of the SSPs were denied IATO due to significant corrections needed (processed after corrections made)

Security Plan Denial & Rejection Rate

February 2011 - January 2012



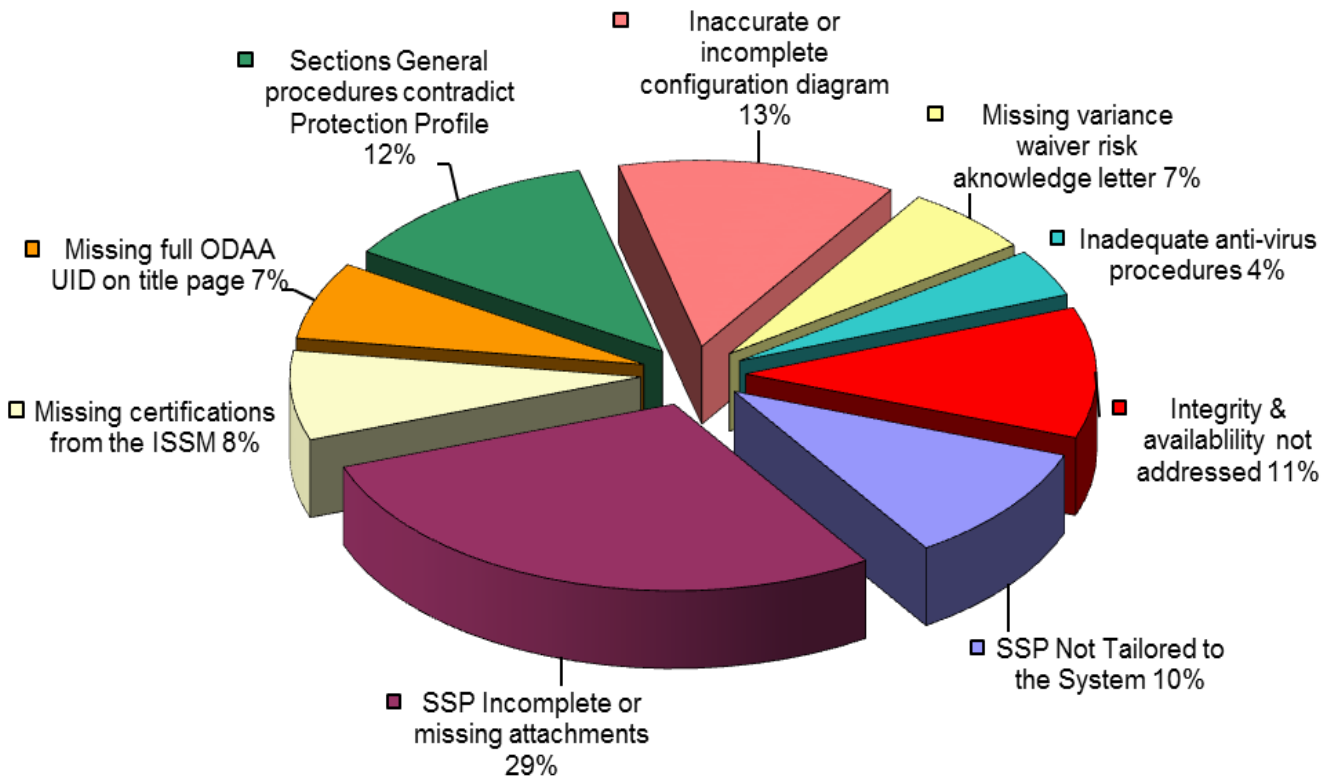
	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Jan-12
Denials	63	72	71	37	66	58	59	52	44	37	40	34
Rejections	0	0	49	21	31	32	28	28	23	7	3	6

- Denials: 633 SSPs (13%) were received and reviewed, but denied IATO until corrections were made to the plan.

- Rejections: 228 SSPs (4.6%) 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

February 2011 - January 2012

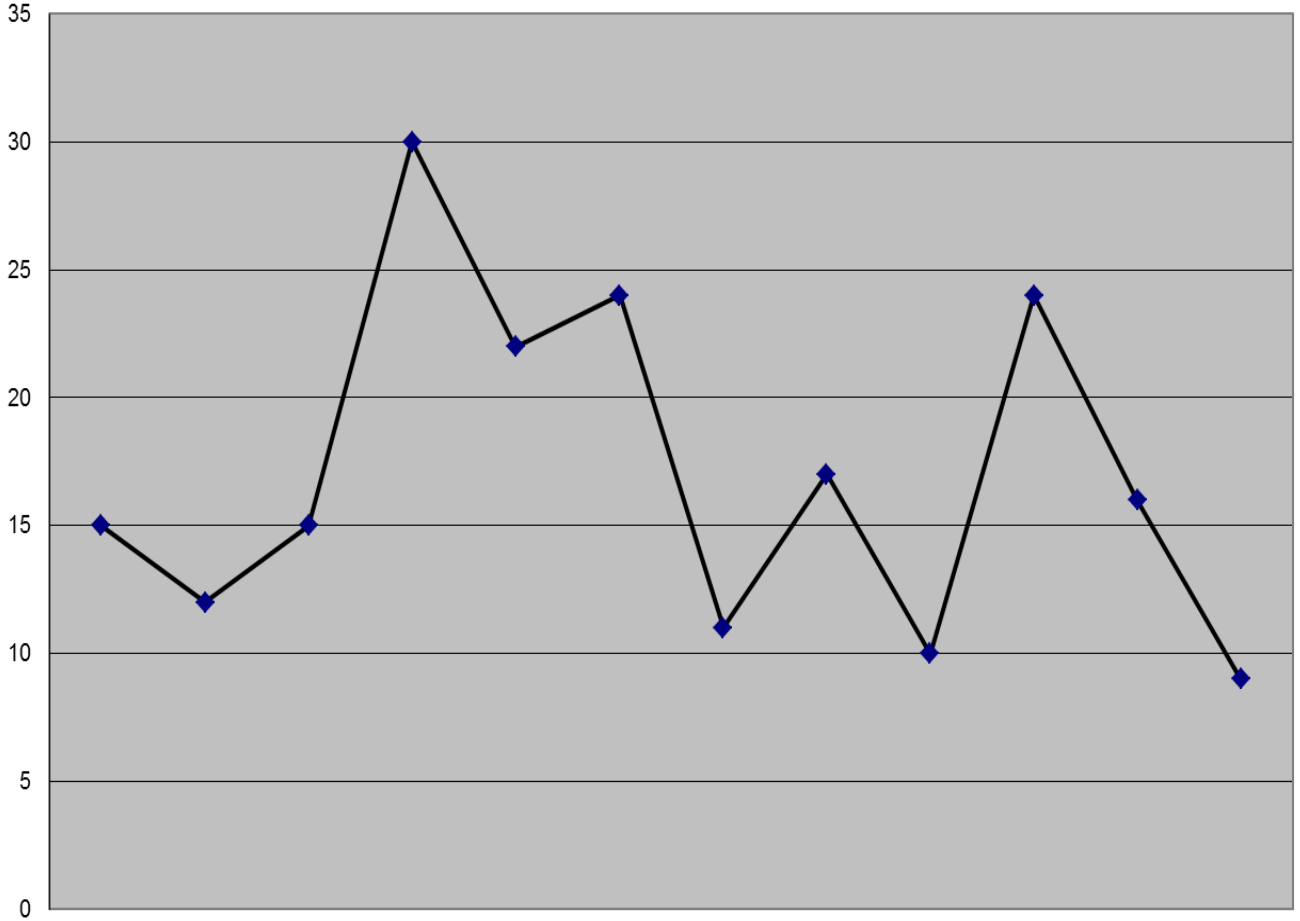


Top Deficiencies

1. SSP was incomplete or missing attachments
2. Inaccurate or incomplete configuration diagram
3. Sections in general procedures contradict protection profile
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

Second IATOs Issued

February 2011 - January 2012



	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Jan-12
Second IATOs	15	12	15	30	22	24	11	17	10	24	16	9

Reasons for granting second IATOs

- Outstanding plan of action and milestone (POAM) items

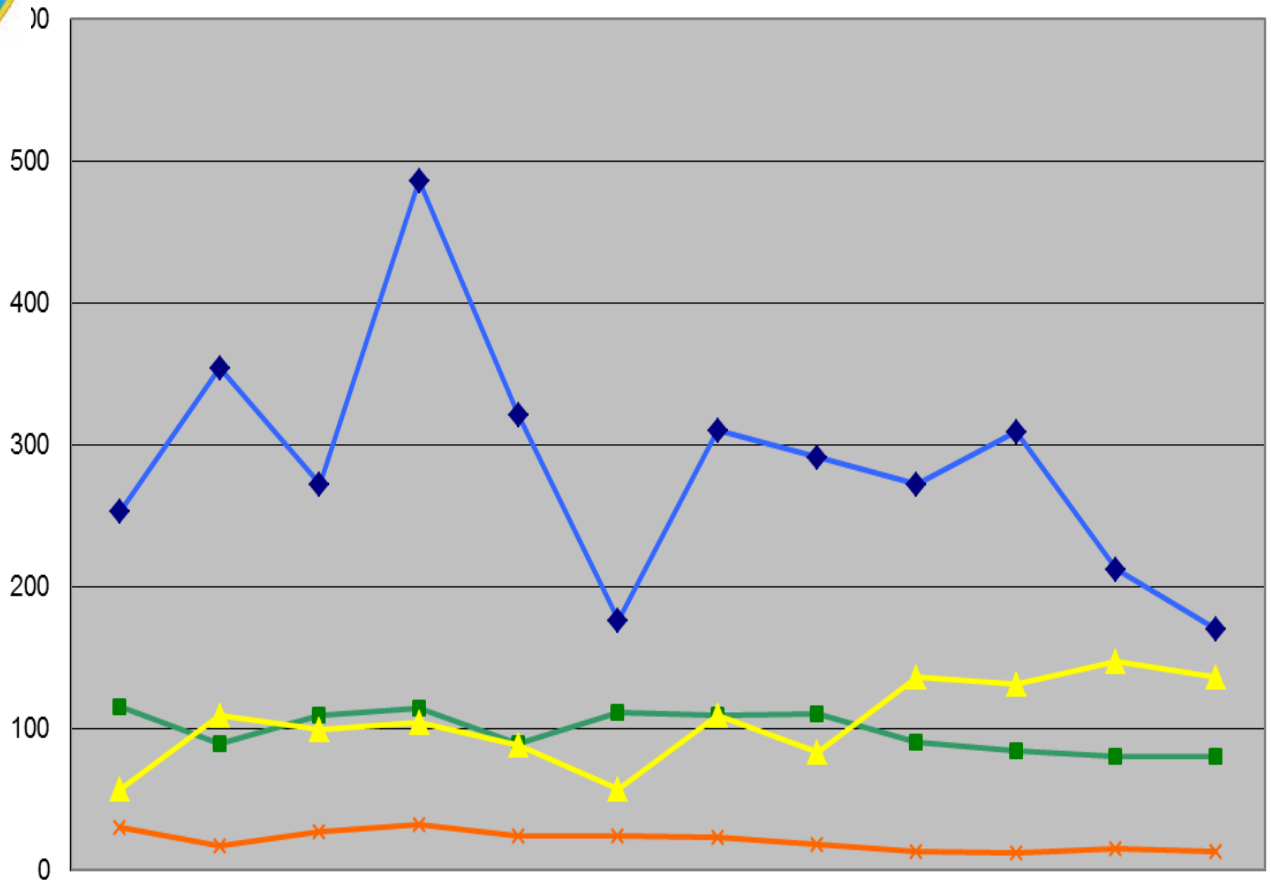
- Host Based Security System (HBSS) not installed

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

- Total number of IATOs for the past twelve months is 205

System Validation Metrics

February 2011 - January 2012

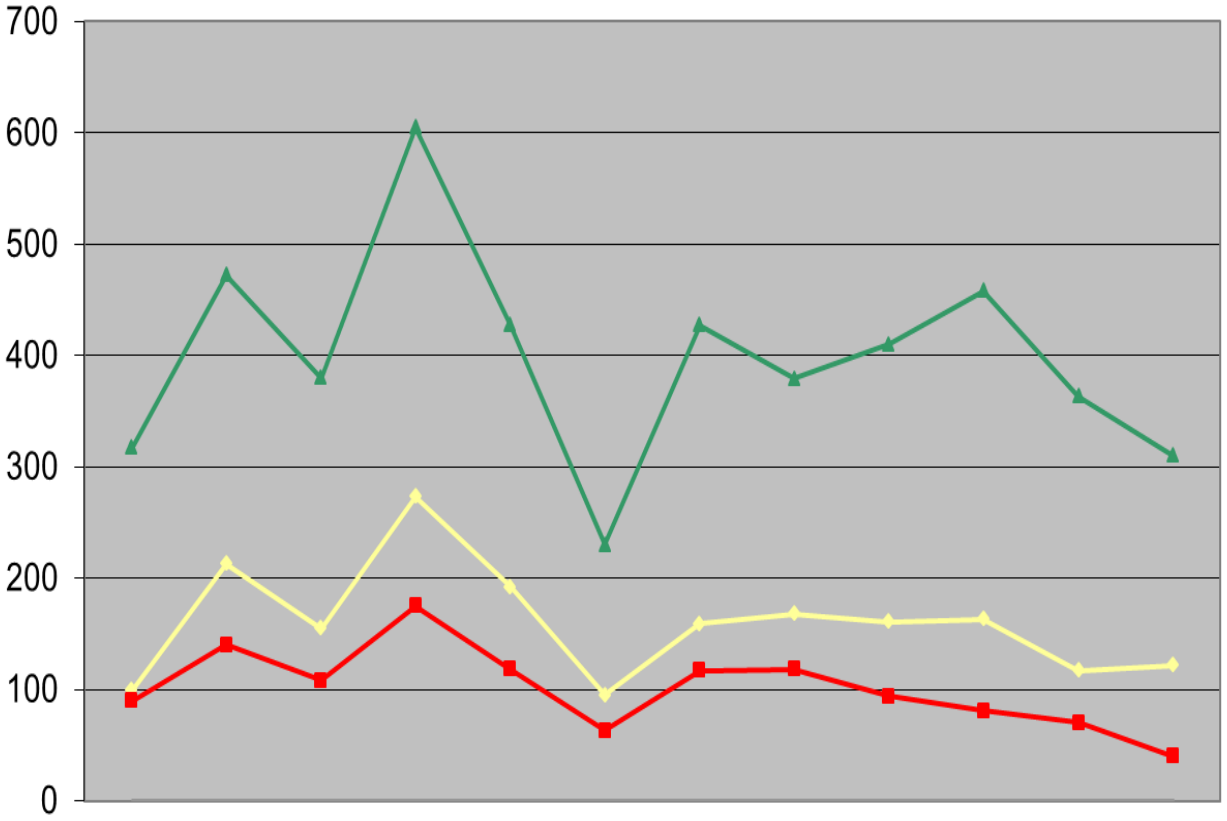


	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Jan-12
Total ATOs	253	354	272	486	321	176	310	291	272	309	212	170
Avg Days to ATO	115	89	109	114	89	111	109	110	90	84	80	80
Total SATOs	57	109	99	104	88	57	109	83	136	131	147	136
Avg Days to SATO	30	17	27	32	24	24	23	18	13	12	15	13

- 3426 systems were processed from IATO to ATO status during the 12 months
- Across the 12 months, it took 99 days on average to process a system from IATO to ATO
- 1256 systems were processed going Straight to ATO status during the 12 months
- Across the 12 months, it took 19 days on average to process a system going Straight to ATO
- 27% of ATOs were Straight to ATO

System Validation Metrics

February 2011 – January 2012

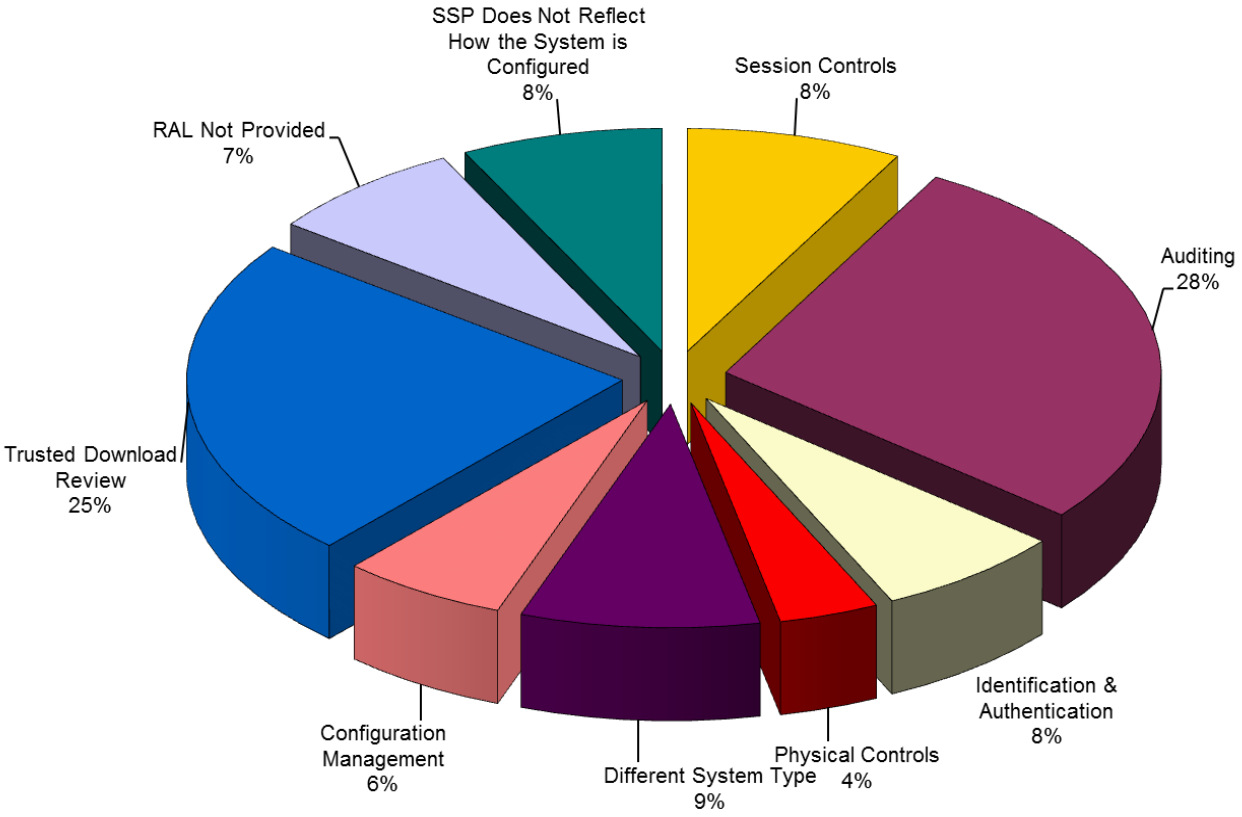


	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Jan-12
# Vulnerabilities	99	213	155	273	192	95	159	168	161	163	117	122
# Onsites w/ vulnerabilities	90	140	108	175	118	63	117	118	94	81	70	40
# Onsites	317	472	380	605	427	230	427	379	410	458	363	310
Avg Vulnerability per Onsite	0.31	0.45	0.41	0.45	0.45	0.41	0.37	0.44	0.39	0.36	0.32	0.39

- Completed validation visits for 4794 systems during the 12 months
- 3393 systems (71%) had no vulnerabilities identified
- 1289 systems (23%) had minor vulnerabilities identified that were corrected while onsite
- 112 systems (2%) had significant vulnerabilities identified, resulting in a second validation visit to the site after corrections were made

Common System Vulnerabilities

February 2011 - January 2012



Top Vulnerabilities

1. Inadequate auditing controls
2. Inadequate trusted download procedures.
3. System type not the same as SSP
4. Improper session controls
5. Identification & authentication controls
6. SSP does not reflect how the system is configured
7. GCA risk acknowledgement letter not provided
8. Inadequate configuration management
9. Physical security controls

Backup Slides

Security Plan Review Discrepancies by Facility Category

Number of Plans Submitted Jan 2012		42	91	57	54	102
	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
SSP Is incomplete or missing attachments	49	13.33%	4.21%	**17.24%**	**16.07%**	**19.42%**
Sections in General Procedures contradict Protection Profile	28	2.22%	1.05%	**10.34%**	**14.29%**	**11.65%**
Integrity & Availability not addressed completely	22	0.00%	0.00%	**8.62%**	**7.14%**	**12.62%**
Inaccurate or Incomplete Configuration diagram/system description	19	**6.67%**	3.16%	**6.90%**	5.36%	**5.83%**
Missing variance/waiver/risk acknowledgement letter	14	**4.44%**	**3.16%**	**10.34%**	1.79%	1.94%
SSP Not Tailored to the System	14	0.00%	0.00%	**1.72%**	**1.79%**	**11.65%**

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

January 2012	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Missing certifications from the ISSM	10	2.22%	0.00%	**3.45%**	**3.57%**	**4.85%**
Missing full ODAA UID on Title Page	10	**4.44%**	0.00%	0.00%	**5.36%**	**4.85%**
Inadequate anti-virus procedures	6	0.00%	**0.00%**	**0.00%**	**1.79%**	**4.85%**
Inadequate trusted download procedures	4	0.00%	**1.05%**	**5.17%**	0.00%	0.00%
Inadequate recovery procedures	1	0.00%	0.00%	**1.72%**	0.00%	0.00%
Other	0	0.00%	0.00%	0.00%	0.00%	0.00%
Total Errors %	**177**	**8.47%**	**6.78%**	**21.47%**	**18.08%**	**45.20%**
Total Errors	**177**	**15**	**12**	**38**	**32**	**80**

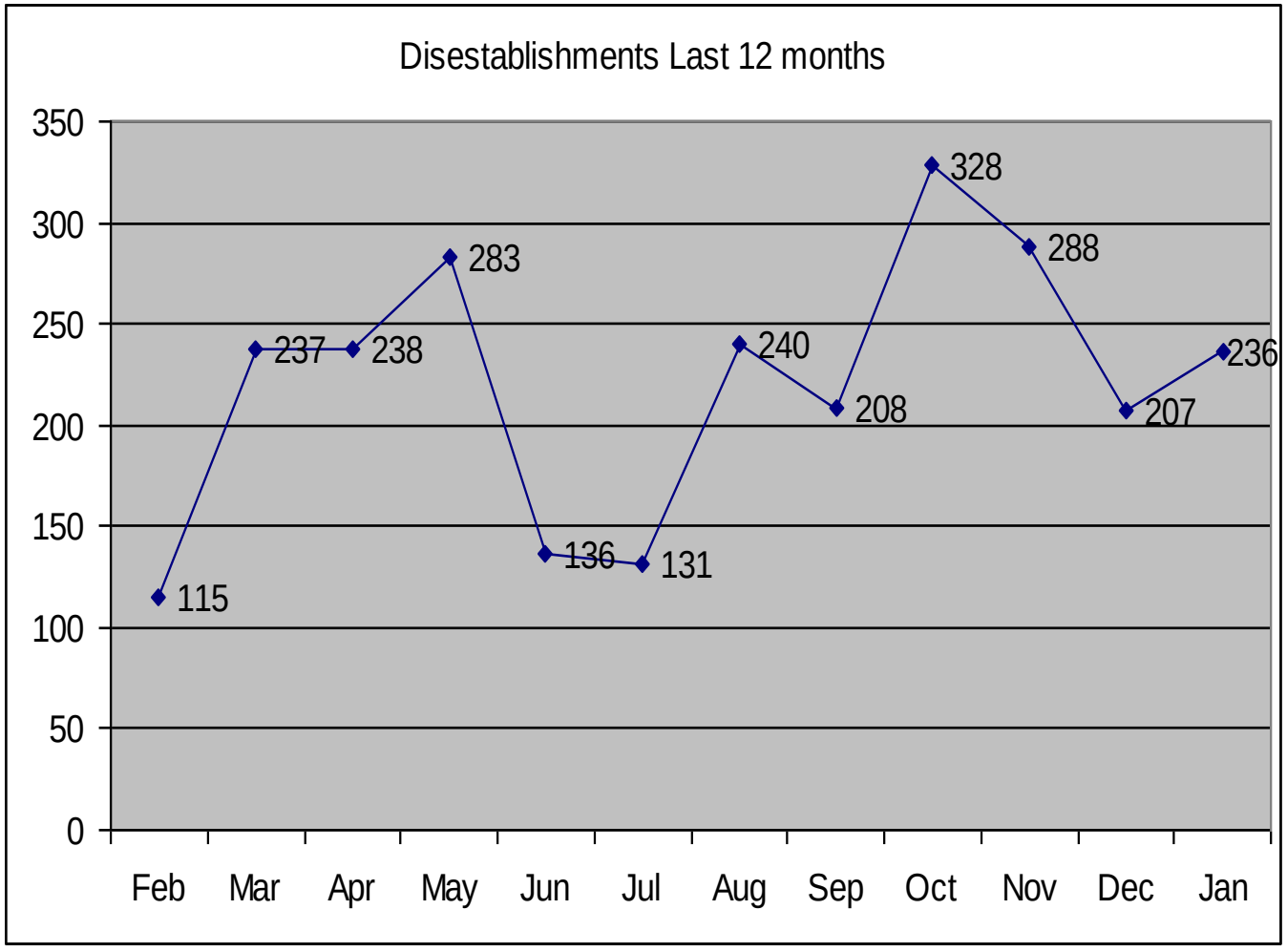
System Validation Vulnerabilities by Facility Category

Systems Validated by Facility Category January 2012		27	30	29	35	49
	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Security Relevant Objects not protected	25	4.26%	3.26%	**16.67%**	**11.54%**	**8.45%**
Auditing	23	2.13%	4.35%	**6.25%**	**13.46%**	**11.27%**
Configuration Management	15	**0.00%**	**2.17%**	**10.42%**	0.00%	**11.27%**
I & A	14	0.00%	1.09%	**6.25%**	**9.62%**	**7.04%**
Session Controls	13	**2.13%**	1.09%	0.00%	**11.54%**	**7.04%**
Physical Controls	9	**4.26%**	0.00%	0.00%	0.00%	**9.86%**
Topology not correctly reflected in (M)SSP	**6**	0.00%	0.00%	0.00%	**7.69%**	**2.82%**
Bios not Protected	**5**	0.00%	0.00%	0.00%	**7.69%**	**1.41%**
SSP Does Not Reflect How the System is Configured	5	**2.13%**	0.00%	**0.00%**	**1.92%**	**4.23%**
RAL Not Provided	2	**4.26%**	0.00%	**0.00%**	**0.00%**	0.00%

System Validation Vulnerabilities by Facility Category (cont'd)

January 2012	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Inadequate anti-virus procedures	1	0.00%	0.00%	**0.00%**	**0.00%**	**1.41%**
Root/Admin Account misconfigured	1	0.00%	**1.09%**	0.00%	0.00%	**0.00%**
Trusted Download Review	1	0.00%	**1.09%**	0.00%	0.00%	**0.00%**
All Users are Configured as Administrators	1	0.00%	0.00%	**2.08%**	**0.00%**	0.00%
PL Not Adequately Addressed	1	0.00%	0.00%	0.00%	1.92%	0.00%
POA&M not Implemented	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%
Compilation	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	**122**	**7.38%**	**10.66%**	**16.39%**	**27.87%**	**37.70%**
Total Errors # Slide One and Two	**122**	**9**	**13**	**20**	**34**	**46**

System Disestablishments



Disestablishments for Month Jan 2012:

Total: 236

Capital: 20 (8.47%)

Northern: 50 (21.19%)

Southern: 96 (40.68%)

Western: 70 (29.66%)

Attachment # 6- SAP Presentation

SPECIAL ACCESS PROGRAM (SAP) WORKING GROUP REPORT

March 21, 2012

Greg Pannoni

Associate Director, ISOO

SAP Working Group Overview

- **Industry requested SAP working group through NISPPAC**
- **Provided Industry White paper on SAP issues/concerns**
- **ISOO concluded at least two sessions were necessary**

Government session (held 1/25/2012) – with agencies authorized in E.O. 13526 to create SAPs

- **Address specific issues in Industry white paper**
- **Discuss government response to Industry issues**

Joint Government/Industry Session (held 2/15/2012) with SAP agencies and NISPPAC Industry representatives

- **Discuss results of Government session**
- **Address Industry specific issues**
- **Framework for future processes, policies, etc.**

Government Agencies in SAPWG

- **Department of Defense**
  - **Acquisition, Technology and Logistics**
  - **Office of the Undersecretary of Defense for Intelligence**
  - **Components: Army, Navy, and Air Force**
  - **Defense Security Service**
- **Department of State**
- **Department of Justice**
- **Department of Energy**
  - **National Nuclear Security Administration**
- **Department of Homeland Security**
- **Department of Justice**
- **Office of the Director of National Intelligence**
- **Information Security Oversight Office (Chair)**

Summary of January 25 2012 Meeting

- A discussion of industry's characterization of **a "compliance only" culture** resulted in agreement that there may be a few situations where "compliance only" and risk avoidance exists, but when such a culture is identified actions are normally taken to encourage a more proactive approach geared at ensuring effective security in more austere fiscal environments.

- Regarding industry comments on integration of more **risk management** into security processes related to SAPs, the members suggested that more definition of the problem from industry would assist in identifying specific security risk management related issues.

- **Several government members suggested that industry address their issues and concerns relating to physical security, information assurance, and personnel security clearance/access reciprocity in more detail.**

Summary of February 15, 2012 Meeting

- Industry stressed that risk management (RM) is key to future SAP operations and that defining a composite risk management methodology, common to all agencies and departments, is essential to effectively assess threats, vulnerabilities, and consequences. They encouraged:
  - The linkage of assessment processes to a common set of RM principles
  - The development of a holistic picture of the SAP environment, and
  - Harmonizing RM and future baseline/common standards for reciprocity across the executive branch agency and departments.
- **The government suggested the establishment of a forum through which industry can communicate problems and issues for quick resolution.**
  - The Contractor Special security Working Group was suggested as the forum for working problems and issues
- **The group agreed that the NISPOM supplement would remain the primary document for use by industry until there is a formal replacement.**

QUESTIONS?

Attachment # 7- Combined Industry Presentation

NATIONAL INDUSTRIAL SECURITY PROGRAM

POLICY ADVISORY COMMITTEE

(NISPPAC)

MARCH 21, 2012

Outline

- Current NISPPAC/MOU Membership
- Charter
- Working Groups
- Areas of Interest

National Industrial Security Program

Policy Advisory Committee Industry Members

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	**Tony Ingenito**
NDIA	**Jim Hallo**
Tech America	**Kirk Poulsen**

National Industrial Security Program

Policy Advisory Committee

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

National Industrial Security Program Policy Advisory Committee Working Groups

- **Personnel Security Clearance Processing**
  - **Expanding the metric collection process to capture all personnel security processes including clearances processed by NISP Agencies. (To date the scope of this group has been limited to DISCO-based process)**
  - **Expand to include SAP & SCI Access Metrics**
  - **Interim Secret Security Clearance changes**
- **Automated Information System Certification and Accreditation**
  - **Industrial Security Field Operations Manual Revisions**
  - **Industry Error Rates**
  - **End-to-End processing time metrics**
- **Ad-Hoc**
  - **NISPOM Rewrite Working Group (11 meetings)**
  - **Threat Information Working**
  - **Small and Mid-Sized Company Issues**

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**
  - **Discuss next steps**

Security Policy Changes of Interest

Executive Orders

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- DSS OAG Presentation

Defense Security Service
Operations Analysis Group

Operational Integration

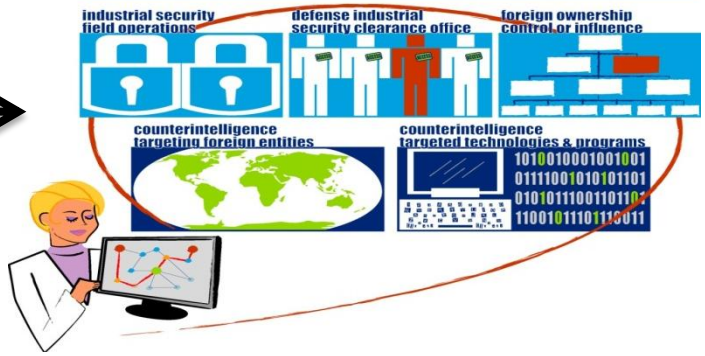
Operations Analysis Group Mission
Operations Analysis Group Overview
Organizational Impact
Case Studies

"The OAG is leading the way!"

Mr. Stan Sims, Director, DSS

Unacceptable Risks to National Security

Operations Analysis Group



Effective Mission Execution

OAG Mission & Vision

Instilling a risk culture within DSS

- **Mission**: To manage risk across the operational components of the Defense Security Service
- **Vision**: The Defense Security Service action arm for orchestration of cross-functional security, counterintelligence, and FOCI operations
- What the OAG IS:
  - An Agency function that reviews and identifies systemic and non-systemic vulnerabilities, that when taken in concert with *threat* & *consequence,* present an unacceptable *risk* to US information & technology resident in cleared industry.

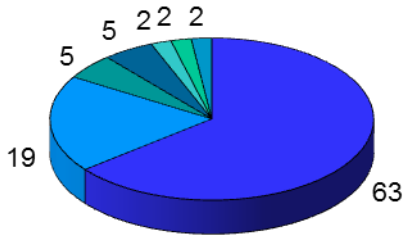
Risk is a function of Vulnerability, Threat, and Consequence/Value

OAG Reporting Thresholds

- Incidents or trends crossing two or more DSS equities which, when looked at individually, may not present the entire picture but when viewed in the aggregate may indicate vulnerabilities resulting from policy or process gaps or failure to follow policy/process
- Suspicious foreign travel to national foreign intelligence priority countries by cleared personnel
- Credible/relevant information which indicates the unauthorized disclosure, theft, loss, or compromise of classified information to a foreign power, an agent of a foreign power, or unauthorized recipient
- Information which indicates a pattern of negligent, willful disregard, or deliberate improper conduct in handling or storing classified or protected information
- Information, incidents or reporting concerning companies and personnel under the purview of the National Industrial Security Program that may result in adverse media attention, senior government or congressional interest
- The unauthorized penetration or disruption of information systems containing classified information or information critical to national security, when the involvement of a foreign power or terrorist group or individuals acting on their behalf cannot be ruled out

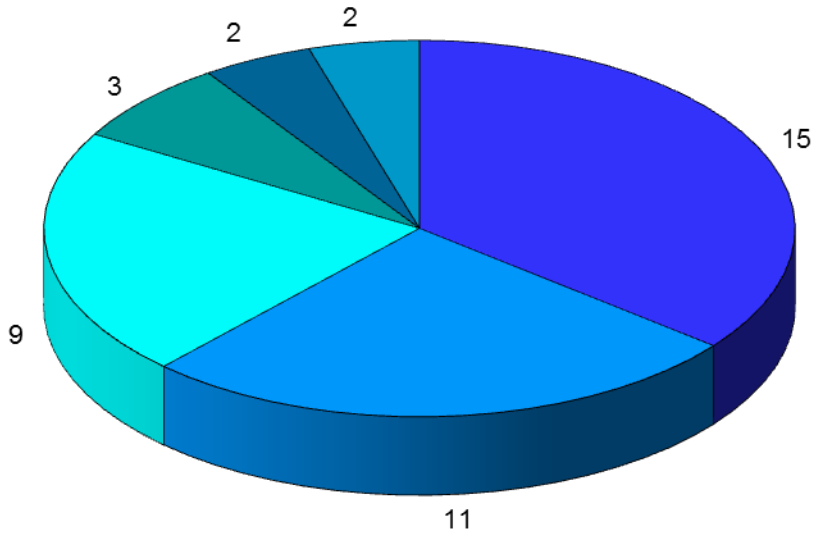
OAG Identified Vulnerabilities

FY11: 98



- Unmitigated FOCI: 2
- SCRM: 2
- Other: 2

FY12: 42



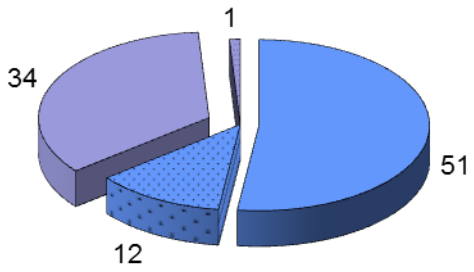
- PCL/PEI: 15
- Security Violations: 11
- Unclass Cyber Intrusion: 9
- Insufficiently Cleared KMP: 3
- ITAR: 2
- Other: 2

What the OAG is Seeing

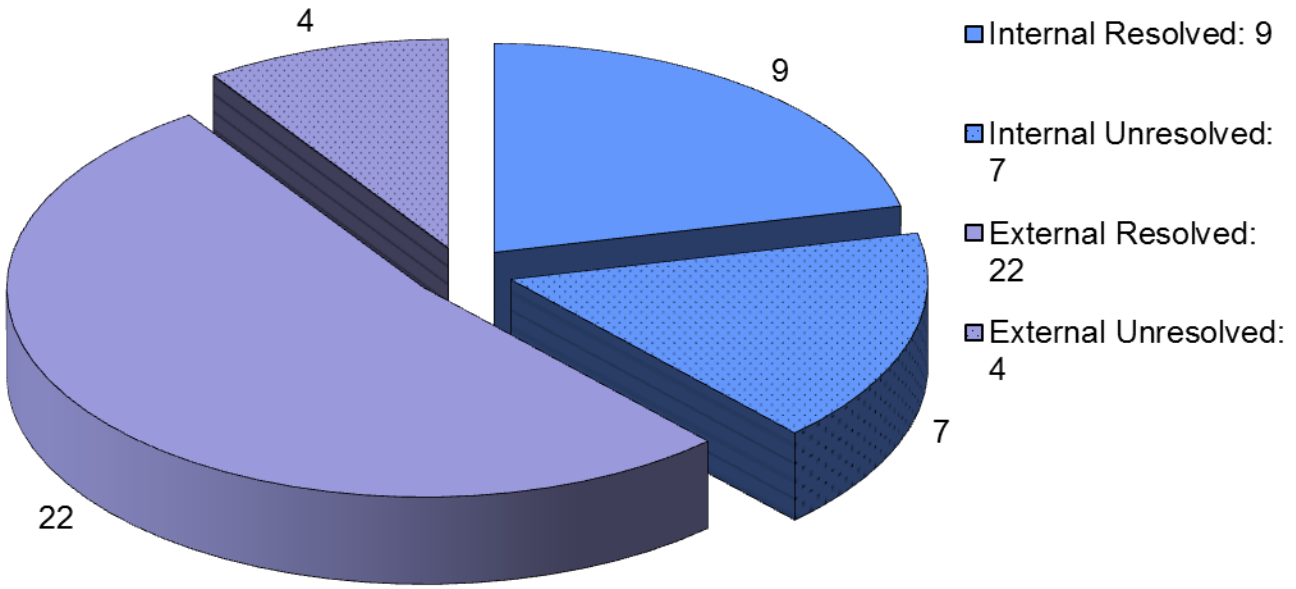
- Inconsistent & timely processing of security incident reports in JPAS
  - Cleared employees who have committed violations that warrant dismissal are permitted to resign in lieu of termination, allowing them to move to other cleared positions within cleared industry with no incident report filing
  - Failure to appropriately annotate warranted violations in JPAS allows a threat to leave one company and to present itself as a threat at another
    - Case Study: Great Imposter
- Exercising Dual Citizenship privileges
  - Dual Citizens relinquishing country of origin passports to facilitate favorable adjudication, and then obtaining a new one surreptitiously

(U) Vulnerabilities, Internal/External

FY11: 98



FY12: 42



Questions?