NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

SUMMARY MINUTES OF THE MEETING

The NISPPAC held its 44th meeting on Wednesday, March 20, 2013, at 10:00 a.m. at the National Archives and Records Administration (NARA), 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 April 30, 2013.

I. Welcome and Administrative Matters

Mr. Fitzpatrick welcomed the attendees, and reminded everyone that NISPPAC meetings are recorded events. He announced that because of sequestration the next and probably subsequent meetings will be held in a different room at NARA that provides a teleconferencing capability, thereby obviating travel for our industry members. He asked the attendees to await more information regarding future meeting conditions as they develop. He then asked Greg Pannoni, ISOO and NISPPAC Designated Federal Official, to review old business. See Attachment 1 for a list of members and guests in attendance.

II. Old Business

Mr. Pannoni reminded the membership that we were approaching the biennial renewal requirement for the NISPPAC Charter and Bylaws. He explained that today's agenda packet contained updated copies of each, and summarized the changes as (1) updating the operating costs of the NISPPAC to $350,000.00, which raised the total federal staff support to 2.5 man years, (2) that NARA will ensure that the Committee's composition does not violate the Presidential Memorandum requiring any federal employees who are appointed to a federal advisory committee, either as primary or alternate members, to file a confidential financial disclosure report with the NARA Office of General Counsel (NGC) on or before the date of their first participation in a Committee meeting, and annually thereafter, and (3) that NARA will ensure the Committee's non-federal composition does not violate the President's mandate that prohibits any appointments or reappointments of federally registered lobbyists to federal advisory committees, boards, or commissions.

In reviewing the action items from the last meeting, he noted that the Personnel Security Clearance Working Group (PCLWG) report will include an analysis of the risk factors involved in the possible suspension of Periodic Reinvestigations (PR), and the subsequent need to discuss these contingencies among senior-level officials. He noted that the Defense Security Service (DSS) complied with the Chair's request to provide industry with detailed information regarding their options for electronic fingerprinting, and published their "Electronic Fingerprint Capture Options for Industry" guide in January 2013, a copy of which is in today's packet and also available on their website. He remarked that the Office of the Director of National Intelligence (ODNI) would present an overview of its policies currently under development that could impact industry to include an update on the status of the national polygraph policy. He stated that the Department of Defense (DoD) update will provide the current status of the conforming change

two to the National Industrial Security Program Operating Manual (NISPOM) that addresses how the National Insider Threat Policy will be implemented across the National Industrial Security Program (NISP). Finally, he noted that ISOO will continue to facilitate an ad hoc working group that will recommend changes to the DD Form 254, "Contract Security Classification Specification," and ultimately produce an automated version of the form. Action items for this meeting are provided at Attachment 2.

III. Reports

(A) The Combined Industry Presentation

Fred Riccardi, Industry Spokesperson, began his presentation (see Attachment 3) by introducing Jim Shamess, the newest member of the industry Memorandum of Understanding (MOU) team, who represents the American Society for Industrial Security (ASIS). He reminded the NISPPAC that both he and Shawn Daley will complete their Committee service at the end of September and that there will be a search started for new industry representatives to the Committee, emphasizing that they were especially interested in recruiting members who are affiliated with small companies. He emphasized that the sequestration will have an impact on industry and their contribution to the NISP. He noted that while it is too soon to know all the ramifications of the sequestration, everyone needs to understand that industry will continue to advocate for better policy reciprocity, especially in Special Access Programs (SAP) and Sensitive Compartmented Information (SCI) Programs. He noted that industry had recently received an excellent Joint Personnel Adjudication System (JPAS) briefing, and reports that everything is on track there, and that industry and the JPAS entities continue to enjoy an excellent rapport. He opined that while there are still problems related to the RAPIDGate system, industry continues to work the issue with the Navy.

He pointed to good news items, such as the improving certification and accreditation metrics, and the work done on the NISPOM rewrite. He expressed industries concern with the potential for conflicting guidance stemming from the various executive orders and task force requirements being implemented. He noted that most of industry will need to understand what network configurations may be required in order to comply with emerging requirements, especially those concerning controlled unclassified information. He commented that industry welcomed the opportunity to provide inputs to the recent Industrial Security Letter (ISL) on threat information, and to have the opportunity to offer recommended changes to the DD Form 254. He noted that the draft volumes of the SAP manual are progressing, and requested that industry soon be allowed to comment on the final drafts. He cautioned that industry was very concerned with insider threat policy and with the specific new data requirements, especially for improving critical infrastructure cyber security, and how they will map to existing policy documents. He expressed appreciation to George Stukenbroeker, National Insider Threat Task Force (NITTF)) for the excellent insider threat program briefing that was presented at the industry stakeholder's meeting. He noted that industry would like to have a better understanding of the specific investments that they are going to have to make, and where they can leverage existing investments, as opposed to having to develop entirely new processes. He pledged that as more is learned, industry will commit to providing the Committee with substantive feedback.

(B) DoD and NISPOM Update

Steve Lewis, OUSD(I), explained that the rescission of funding for PRs will have an impact on the reciprocity of clearances for military service members, the DoD civilian workforce and the contractor community. He noted that OUSD(I) is discussing the myriad of policy implications related to this issue with ODNI. He reminded the Committee that ODNI is working on a reciprocity policy, and that DoD has asked to have a conversation to determine the impact of these delayed PRs as we move forward. In addition, he described an ongoing dialogue with the Office of Personnel Management (OPM), which from the standpoint of their workload, clearly has a stake in easing the delays caused by this funding shortfall. He added that once the complete rewrite of the NISPOM, which is in DoD coordination, is approved it will need to be coordinated with the other Cognizant Security Agencies (CSA) and other affected government agencies, before it enters the Federal Register process and the final DoD signature process. He reported later in the meeting that NISPOM Conforming Change # 1, which implements the United States/United Kingdom defense and trade cooperation treaty, as well as the myriad of changes emanating from Executive Order 13526, "Classified National Security Information," had been approved.

He updated the Committee on the progress on NISPOM Conforming Change #2, explaining that there has been considerable work on the application of insider threat requirements to industry, and the government is ready to share these proposed changes with NISPPAC industry members. He noted that it is not just a change to the NISPOM, but also to 32 CFR Part 2004, "NISP Directive No. 1," which will levy requirements on how government agencies interface with industry regarding insider threat requirements. He emphasized that there are many elements of the insider threat program that are beyond the scope of industry, and in which industry does not have the same insight that is available to the government, especially from a law enforcement and employment history perspective. He noted it will be of paramount importance that we clearly delineate between government and industry responsibilities for implementation of insider threat policy. Further, he mentioned that an ISL will be issued informing industry of the implications of the United Kingdom Defense, Trade, and Cooperation Treaty, which affords additional opportunities for industry exports of defense articles without an independent export authorization, thus creating another class of exemptions from the International Traffic in Arms Regulations. Finally, he noted that the final item involving Conforming Change #2 includes the implementation of Section 941 of the Fiscal Year (FY) 2013 National Defense Authorization Act, which tasks DoD to impose cyber intrusion and reporting requirements on cleared defense contractors. He further noted that these requirements may necessitate a change in the scope of Executive Order 12928, "The National Industrial Security Program." He added that discussions regarding its implementation are ongoing within the DoD, but that this is the approach being considered.

(C) ODNI Policy Update

Charles Sowell provided ODNI updates on items of current interest to the NISPPAC. These included the revised federal investigative standards, the adjudicative guidelines for determining eligibility for access to classified information, and the reporting requirements for any new security executive agent directive (SEAD). He explained that there is an interagency

implementation working group, co-chaired by OPM and ODNI, which meets weekly to discuss implementation of policy and brings the affected agencies together to discuss appropriateness, scope, concerns, and ultimately, consistency across government. He noted that the Security Executive Agent Advisory Committee (SEAAC) timeline for providing an overarching government-wide adjudications standards implementation plan was June 2013. Regarding the revised adjudicative guidelines, he noted that there have been a few substantive changes, such as the focus on foreign preference and the Bond amendment requirements. Additionally, he noted that the guidelines are to be used for all national security eligibility determinations, including sensitive positions, regardless of access requirements, thus promoting standardization and consistency in their application, and thus establishing a single adjudicative standard for both collateral and SCI access. He emphasized that SEAD 200, the policy for the adjudicative guidelines, should be ready for informal coordination by SEAAC by late April 2013 and that it remains to be determined whether or not the SEAAC will require Office of Management and Budget (OMB) coordination. He noted that by the next NISPPAC meeting he will be able to advise the Committee on the determination of the SEAAC regarding formal interagency coordination. He informed the Committee that ODNI closely collaborated with the NITTF on SEAD 400, "The National Reporting Requirements," and has established the minimum reporting requirements for all individuals in national security positions or with access to classified information. He noted that SEAD 400 focused on foreign travel contacts, other related activities, and any other information of adjudicative significance. He anticipated that this directive would be submitted for ODNI coordination later this month, and due to its impact on law, through the OMB process. The Chair asked when industry would be invited to review the directive, and Mr. Sowell assured him that interface with industry would come through the NISPPAC, and would occur whether it is in the SEAAC informal coordination process and/or the formal OMB process.

The Chair asked Mr. Sowell to update the Committee on ODNI's new polygraph policy, and address the degree to which reciprocity should be expected with regards to the different types of polygraph. Mr. Sowell explained that ODNI's new polygraph policy was under discussion with OMB, and it was unclear as to the outcome of that coordination. The Chair requested that ODNI provide the NISPPAC updates to the polygraph policy through the PCLWG, and clarified that this policy was important for both our industry and government partners. Mr. Sowell noted that these new policy objectives mostly clarify existing practices for agencies that use the polygraph and ensure that standardization and consistency is applied. The Chair reiterated that even if it does not say anything surprisingly new or revise existing practices, it will at least express the government's intent to have polygraphs work in a certain way, and perform specific functions.

(D) DSS Update

Stan Sims, DSS, reminded the committee that, as is customary, DSS held its stakeholder meetings on Monday (government) and Tuesday (industry), immediately preceding this NISPPAC meeting. Next, he updated the Committee relative to changes in the JPAS call center, noting that the transition from DSS to the Defense Manpower Data Center (DMDC) will be completed on June 1, 2013. He assured the Committee that DSS has made every attempt to ensure as seamless a transition as possible, for both our government and industry partners. He addressed discussions he recently had with the director of the DMDC regarding data quality initiatives and data purging efforts, and was assured that DMDC will continue to post their latest

processes on their web site. He reiterated that the DMDC website will continue to be linked to the DSS website and provide assistance to Facility Security Officers (FSOs) as they partner in the file cleanup effort. He reminded the Committee that their information packet contained a copy of DSS's overview of the "Electronic Fingerprint Capture Options for Industry," which includes all the options by which to matriculate to the electronic fingerprint submission process, and reiterated that the DoD deadline for mandatory compliance is December 31, 2013. He noted that after that date OPM will no longer accept paper fingerprint cards, and he suspected that today's PCLWG's report would again cite the failure of numerous industry partners to have completed enrollment as the number one reason for untimely completion of the clearance process. He reminded the Committee that there are still some 80% of all fingerprints being submitted in paper format. He also reminded everyone that they can link to DSS' website for answers to any procedural questions, and should that prove ineffective, that they could telephone for a step-by-step walk through of the process. He encouraged all to remember that we have numerous ways that all companies, regardless of size and/or complexity can adapt their resources to meet this requirement, and that DSS was poised to assist anyone who seeks help. Finally, he voiced concerns about sequestration, especially its impact on industry partners, and advised that DSS continues to manage funding procedures and timelines affecting industry clearances. He advised everyone to continue to monitor the www.dss.mil website for the latest in all manner of news on this topic.

He reminded the Committee that approximately ten months ago DSS changed the PR submission time from 180 to 90 days, in order to better manage the funding process, and that as of April 1, 2013, they are again forced to further decrease submission time from 90 days to 30 days, and reiterated that an industry PR may be submitted only 30 days before it is due. In addition, he noted that DSS has taken other substantive funding cuts, and could be forced to suspend PR processing altogether as had already been the case with some other DoD entities. He promised to inform industry if this condition occurs and that there may be additional guidance by the end of April 2013. He reiterated his promise of a free flow of new information and decisions as soon as circumstances permit.

(E) DoD Consolidated Adjudication Facility (CAF) Update

R. B. Peele, DoD CAF, began by describing the CAF's efforts to separate, identify, and quantify its adjudication of industry personnel security clearance cases (see Attachment 4). He explained that DoD only recently completed its consolidation of seven of its 10 CAFs into a single entity, so metrics specific to its total industry caseload were not yet available. However, the CAF Director is striving to address all adjudication needs and to do so with as much transparency as possible. He described the CAF's efforts to achieve full transparency as dependent on OPM initiating a monthly Intelligence Reform and Terrorism Prevention Act (IRTPA) compliance report for the CAF and for the CAF to complete its development of version 4 of the Clearance Adjudication and Tracking System (CATS), which will provide the enhanced capability in reporting and metrics required by FY 2014. He reported that the metrics for their total pending adjudications consisted of a backlog of 15,550 initial cases, and a 2,680 case backlog on Single Scope Background-Periodic Reinvestigations (SSBI-PR) and the Phased PRs (PPR). He cautioned against too much concern associated with the size of the 15,550 backlog, as that number represents only 2% of the annual ingest of all DoD CAF actions. Concerning the 2,680

backlog, he described this as representing 3.5% of the total current inventory, or less than 1% of the total DoD CAF annual ingest. In response to a question from Chair regarding the status of the aforementioned cases, Mr. Peele described the cases as being in various stages in their life cycle. He then clarified that the backlog totals include all cases ingested by DOD sources and not just those from industry. In response to a question from Ros Baybutt, Industry, regarding the rather large pending backlog, he explained that the DoD CAF is currently not separating cases by types, but rather is simultaneously examining both Defense Office of Hearings and Appeals (DOHA) and Defense Industrial Security Office (DISCO) cases. The Chair observed that this was an ambitious and much welcomed effort that fits with our efforts to present the most inclusive view of the industry experience as they engage different government partners. He added that where the Committee focused on the bulk of that information, which was from the OPM/DISCO, we are now broadening that scope to include all partners. In addition, the Chair noted that it is indeed important to understand that backlogs come and go, and what factors affect them, because PR sequestration choices are absolutely going to change the statistical picture. In response to an inquiry from Mr. Pannoni, Mr. Peele assured the Committee that the analysis being linked to IRTPA in fact represents the fastest 90% of the cases.

He then recapped his presentation by stating that the CAF is well within the IRTPA standards, and will continue to be. He acknowledged that there was work to be done with complying with the 30-day requirement for PRs, but that the focus is on achieving that goal. He also noted that as the CAF continues to comply with IRTPA standards, there will nevertheless be an increase in IRTPA timelines, as we look for ways to address these larger projected backlogs. Mr. Sims added that Mr. Peele, given the impact of suggested sequestration furloughs, was correct in this analysis, and that it is unimaginable that if the furlough plan is executed as has been advertised, wherein every civilian employee in DoD has his work week reduced by one day, there will be a dramatic negative impact on expectations over which we have little to no control. The Chair gave one final caution on the subject, noting that while our responses to these forecasts give us much cause for concern, let us not forget that in the worse-case scenario, eight days for adjudication remains well below the 20 days required under IRTPA.

(F) PCLWG Update Report

Lisa Loss, OPM, updated timeliness performance metrics for DoD's industry personnel submissions, investigations, and adjudications (see Attachment 5). She noted that the first quarter of FY 2013 reflected the expected fluctuations in overall timeliness, due largely to ongoing reform efforts, even though we have made many improvements in investigation and end-to-end processes. She noted that OPM showed decreased timeliness for Top Secret investigations which are exceeding the 80-day investigative timeframe. She explained that in order to reduce stress on SSBI investigations OPM redistributed work among its various contractors and the federal workforce, and provided additional guidance as to what could be worked by the contract investigators. Continuing, she noted that over the same period they experienced unanticipated capacity issues with some of their contractors, which in turn were compounded by problems with resource constraints at their National Agency Check (NAC) repositories. She noted that this influx in workload fluctuations also impacted adjudications, and resulted in an increase in the end-to-end performance timelines. She explained that historically, industrial Top Secret investigations hovered around the 70- 80 day timeframe, but now we are

seeing trends that increase this timeframe to between 100 to 102 days. She noted that the good news is that as a result of this redistribution of workload and other corrective actions, by the end of the year they should be back on track to meet the desired 80-day investigation timeframe for industry. She opined that as work is redirected back to the SSBIs, the PRs already in the system will continue to age and that of course makes the process more difficult when trying to adjudicate an older PR.

Mr. Sims recommended that we seize the opportunity and in the near future we should stop submitting PRs, which would then provide OPM with the time and resources necessary to reduce some of their backlog. He suggested that once DoD and ODNI can reopen PRs it should be done in a very measured and collective manner that prioritizes the critical investigations, and that allows for the management of both the workflow and the finances involved. Further, he recommended that another working group be initiated to develop a timeline that permits the reopening of investigations, while avoiding systemic oversaturation. The Chair agreed in principle noting that while we already maintain databases of the caseloads we have, this working group would focus on the impact of holding PRs in abeyance in the long term, and would among other things, learn how to portray the future timeliness metrics of all our partners. Mr. Sowell agreed, and proffered that ODNI has already begun to report its PR performance metrics and backlog numbers, and thus should be capable of capturing all that data. The Chair suggested that the Committee reach out to our industry partners who play a vital role in this process, and develop an understanding as to what actually works and best serves our needs. He opined that since we know the performance measures established by the security executive agent for each type of case, we should be able to show target numbers on any portrayal and be able to predict if we are within, or approaching, our optimum target. Ms. Loss concluded by validating the importance of working with the CAF to make certain the correct levels are being reflected, and that the CAF gets the metrics they need.

The PCLWG report continued with an update on DSS's Personnel Security Management Office (PSMO) from Laura Hickman (see Attachment 6). Ms. Hickman reminded the Committee that the primary responsibility of her office was to review industry's submissions of the Electronic Questionnaires for Investigations Processing (e-QIP) to OPM, and as such, to determine investigations' quality and rejection rate. She informed the membership that the current rejection rate for DSS/OPM was hovering at 5%, adding that the primary reason for these rejections was due to missing employment information, and most often where the subject failed to name the submitting company as the current employer. She further explained that the PCLWG was still working with OPM to determine whether there was an actual requirement for submission of this information in precisely that way, and noted that once this decision is made one of the primary reasons for e-Qip rejections could be eliminated. She continued by explaining that the number one reason for rejection at OPM was missing fingerprints, and noted that fingerprints are required to be submitted within fourteen days of OPM receiving the investigation. She encouraged electronic fingerprint submissions, which would ultimately eliminate the number one reason for e-Qip rejections.

Christie Wilder, ODNI continued the PCLWG's report with the performance metrics for the intelligence community (IC) (see Attachment 7). She updated metrics related to those investigations and adjudications that are conducted by Investigative Service Providers (ISP)

agencies other than OPM. She reiterated that while almost six percent of the government's investigations and adjudications for industry were conducted for the IC, that less than one percent of those investigations are conducted by the other ISP agencies. She reminded members that the timeliness goals set for completing each phase of the clearance process are the same for any agency. She noted that the goals are fourteen days for the initiation of any type of investigation, 40 days for a Secret investigations (80 days for a Top Secret investigation) and 20 days for the adjudication phases regardless of investigation level. She reiterated that for PRs the goal for initiation is 15 days, the investigation goal is 150 days, and 30 days for adjudication. She noted that these goals were originally established by the Performance Measurement Management Subcommittee of the Performance Accountability Council (PAC) and that annually the ODNI issues feedback performance letters that hold each agency accountable for these metrics. She reminded the Committee that the PAC methodology is an end-to-end process that is closely scrutinized because they want to know how long it takes for an applicant to get a clearance. She explained that IRTPA requirements are measured differently, in that they track the number of investigations completed, as well as the quarterly timeliness of the investigations and adjudications. She also explained that since the IRTPA process does not mirror that of the PAC, in that each measures different groups in different populations, it is often difficult to determine exactly how long it takes for an applicant to get a clearance. She added that it is important to remember that this measurement takes into account the entire process, beginning with how long it takes for agencies to initiate the packet and submit it to the ISP, to how long it takes the ISP to conduct the investigation, to how long it takes the adjudicative facility to complete its' deliberations and make a decision. She then reviewed the end-to-end timeliness of the IC's performance metrics which showed an increase in Top Secret timeliness from 141 to 131 days, and a slight decrease in the timeliness of Secret investigations. In detailing PR performance metrics, she noted an increase in initiation timeliness and a decrease in investigation and adjudication end-to-end timeliness from 181 days to 228 days. Finally, she informed the Committee that the reporting required to Congress under the Intelligence Authorization Act (IAA) has been completed, and thanked the DoD and OPM for their assistance in compiling the metrics from the JPAS, the Clearance Verification System (CVS), and Scattered Castles that went into that report. She noted that while the reporting methodology was the same as in previous releases, this time it included metrics for both those in access as well as for those eligible for access but not yet holding a clearance. She noted that the two primary benefits resulting from this approach were: (1) these metrics reflect favorable determinations for the entire year; and (2) they provide a high degree of specificity to IAA objectives. The Chair expressed appreciation for the work required to gather, track, and report these metrics, as these often represent the unique language and talking points between executive branch agencies and Congressional members and staff on the subject of security clearances. In addition, he suggested that we extend the scope of this initiative to include the same regular scrutiny in the timeliness metrics for industry, as opposed to simply what we now see only in an annual report. He directed the PCLWG to examine the possibility of tracking and rolling-up the overall performance timeliness for industry investigations similar to the IRTPA criteria, showing the breakdown in total number of clearances between government and industry.

The Chair then called for updated performance metrics for the Department of Energy (DOE), and Mark Pekrul, presented the DOE report (see Attachment 8). He noted that there were few substantive updates, and reported that in the DOE there are 61,387 Q (Top Secret) access

authorizations, and 23,158 L (Secret) access authorizations. He explained that the DOE has a total population of approximately 110,000 cleared employees, approximately 84,000 of whom are contractors. He also reminded the Committee that OPM is DOE's ISP, but that the agency performs its own adjudications. He noted that while the adjudicative metrics for the first quarter of FY 2013 were slightly higher than normal, they have continuously met IRTPA adjudication goals since FY 2009.

The Chair welcomed Valerie Kerben, Nuclear Regulatory Commission (NRC) to the NISPPAC, and informed the committee that she would be providing the NRC timeliness metrics for the first time as part of the PCLWG report. Ms. Kerben provided a brief overview of the role NRC plays as one of the four CSAs (see Attachment 9). She described their primary function as management of the contractor and licensee staff who operate the nation's power plant utilities and fuel cycle facilities. She noted that OPM conducts NRCs' background investigations and that the agency adjudicates the clearances for (Q and L accesses) all federal, contractor, and licensee employees. She informed the Committee that NRC has approximately 4,500 cleared federal and licensee employees, and approximately 813 contractors that require access to classified information. She explained that NRC maintains a staff of contractors at their headquarters who are investigated and vetted for access, but who do not receive a security clearance. With regard to end-to-end metrics, she reported that NRC is generally pleased with its historical performance, and confirmed that they are achieving timeliness goals for initiations and adjudication of PRs. She noted that due largely to budget constraints, NRC is decreasing the number of PRs it is submitting to OPM, while trying to maintain timeliness goals. In closing, she noted that NRC partners with DOE in conducting their hearings and appeals process. The Chair thanked Ms. Kerben for her report and welcomed NRC to the continuing efforts of the NISPPAC.

(G) Certification & Accreditation Working Group (C&AWG) Update Report

The Chair called for Randy Riley, DSS to provide the report for the C&AWG (see Attachment 10). Mr. Riley reminded the Committee of the working group's initiatives, and provided updates on each. First, he noted that the Office of the Designated Approval Authority (ODAA) has received and reviewed comments from our industry partners relating to the system configurations and updates for the Windows 7 & 2008 Server Baseline Standards, and that they will be incorporated in the final document being prepared for coordination. He reiterated that a review is being conducted of continuous monitoring as it applies to NISP systems, since those systems are not typical DoD networks and we have to apply the rules in slightly different ways. He noted that the final draft of updates to the DSS ODAA manual will be offered for coordination and comments in the near future. Finally, he reminded the Committee that the ODAA was examining how to leverage some of the commercially available tools, such as the Security Content Automation Protocol (SCAP), a possible tool for use in assessing compliance in a NISP information systems environment. He then reported on the System Security Plan (SSP) metrics and declared success with the present and continuing results, as we're averaging about 15 days to issue an Interim Approval to Operate (IATO) and the Straight to Approval to Operate (SATO) systems, and approximately 83 days for systems that go through the standard two-step process, IATO to ATO. He explained that Command Cyber Readiness Inspection (CCRI) efforts are expected to have an impact on our system approval timelines, as we get our evaluators

trained and certified to conduct these reviews, in that it takes them away from normal duties. Finally, he mentioned that in future reporting of common vulnerabilities encountered during system validations, the working group would be splitting the "Auditing" piece into two categories of measurement: audit trails, and system configuration technicalities. He stated that this will help to achieve more granularity so that we can better address the actual cause for concerns at the site, and to actually perform a review of the audit trail. Mr. Sims reminded everyone that sequestration would have an impact on these processes as well, although it is too early to determine what kind or to what extent. Mr. Riley concluded his remarks by reminding the Committee that the same common deficiencies are constantly being found during reviews, including such SSP errors as missing attachments, documentation errors, and integrity and availability requirements. He noted that the typical vulnerabilities being identified during system validations include audit controls, configuration management problems, and failure to properly protect security relevant objects. He reminded everyone that in the June 2013 timeframe they would be rolling out the ODAA Business Management System, and that prior to that event they would be providing live briefings and demonstrations in conjunction with the National Classification Management Conference in Chicago, IL, conducting familiarity training in the form of webinars that can be accessed through the internet other forms of interactive sessions. In addition, he announced that once the system goes live as a final product, they will provide a training program available through the DSS training portal.

IV. Closing Remarks and Adjournment

The Chair reminded everyone that, as he had mentioned at the beginning of today's meeting, the next NISPPAC meetings, tentatively scheduled for July 17 and November 13, 2013, would be held at NARA, and that due to sequestration, the meetings would be presented in a virtual format with details to be announced at a later date. In addition, he noted that ISOO, notwithstanding sequestration impacts, plans to engage with the membership at the National Classification Management Society annual seminar, and that the PCLWG plans to hold a meeting during that event. There being no further business, the meeting adjourned at 11:58 am.

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

Action Items - 3/20/2013 NISPPAC Meeting

1. ISOO, in its role as the NISPPAC Executive Secretariat, will coordinate required changes to the NISPPAC Charter and Bylaws, required under the Federal Advisory Committee ACT (FACA), that must be approved and in place prior to the Committees required recertification on 1 October. Actions required to complete this item includes:

   - Formal coordination of changes to the NISPPAC charter and bylaw with NISPPAC government and industry representatives, so a final vote can be taken at the July 2013 meeting.

   - Coordination with NISPPAC government representatives and their alternates regarding FACA requirements for providing required financial disclosure information available to the NARA Office of the General Counsel.

   - Coordination with NISPPAC Industry representatives, in accordance with FACA requirements, to certify that they are not registered lobbyists.

2. ISOO will continue to facilitate working group meetings and monitor activities related to the update and automation of the DD-254.

3. The Personal Security Clearance Working Group (PCLWG) will :

   - Work with the ODNI to clarify management intentions regarding updates to the National Polygraph Policy and ensure reciprocity requirements are appropriately addressed in that policy.

   - Review collective measures to lessen the impact of delayed periodic reinvestigations (PRs) on the overall timeliness of industry clearance submissions, investigations, and adjudications.

   - Track the overall performance timeliness for industry investigations using Intelligence Reform and Terrorism Prevention Act (IRTPA) reporting criteria which portray the total number of personnel security clearances granted to both government and industry.

   - Ensure that PCLWG presentations use the standardized performance criteria developed by the Security Executive Agent (SEA) when reporting metrics for each type of background investigation.

Attachment #3- Combined Industry Presentation

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

MARCH 20, 2013

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	J.C. Dodson
ASIS	Jim Shamess
CSSWG	Mark Rush
ISWG	Karen Duprey
NCMS	Rhonda Peyton
NDIA	Bob Harney
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**
  - **USN's RapidGate Program challenges**
- **Automated Information System Certification and Accreditation**
  - ***Focus - implementation***
- **Ad-Hoc**
  - **NISPOM Rewrite Working Group - on-going progress**
  - **CI Working Group – implementation of uncertain requirements**
  - **Current Threat information sharing / distribution is still challenge**
  - **Potential revision to DD 254 – Industry attended DSS / Army Demo and is engaged with requirements process**

Working Groups continued

- **Industry requested an ISOO sponsored Ad-Hoc SAP Working Group**

- **Meetings continued in March 2013 – SAP draft volumes to be shared with NISP signatories and industry**
  - **DOD to issue NISPOM SAP Manual in late FY 13**

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

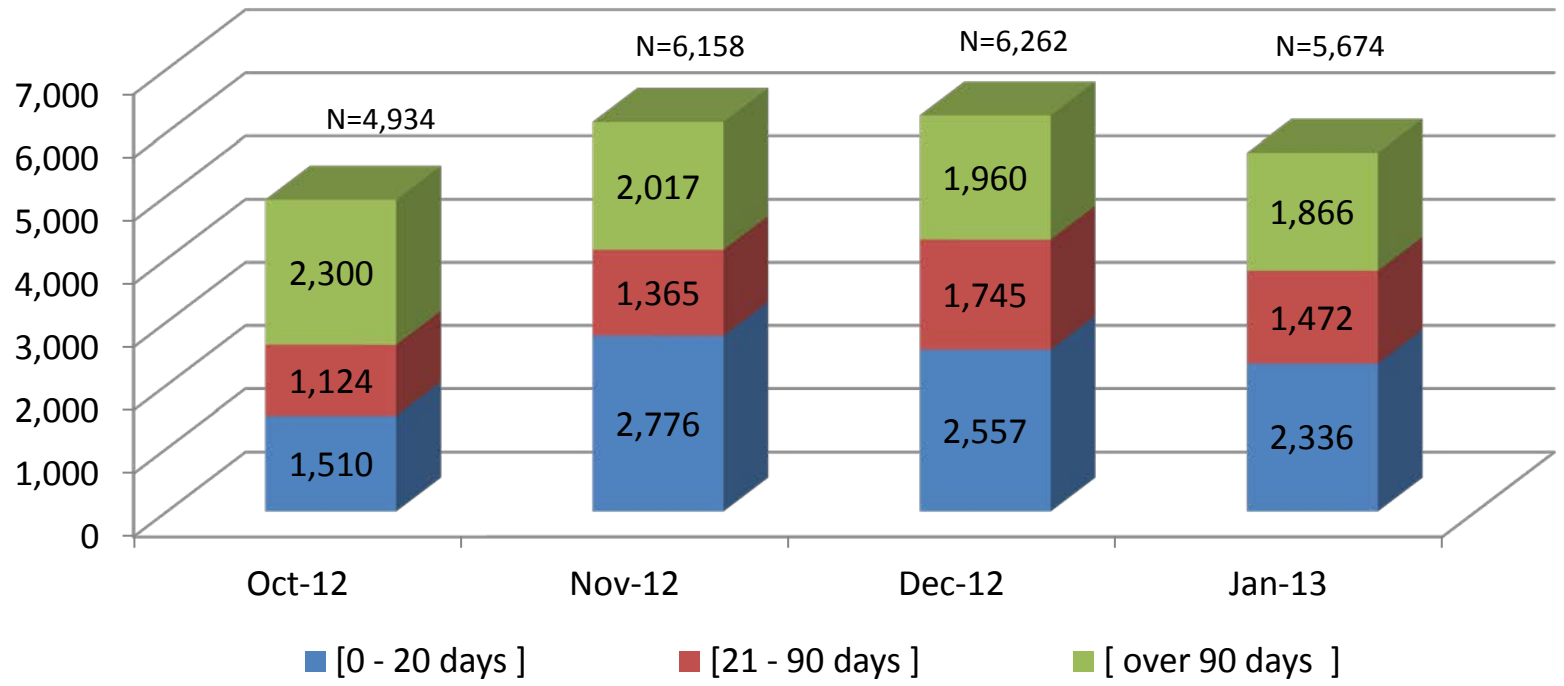
Draft FAR Clause

THANK YOU

Attachment #4- DoD CAF Presentation

DOD CAF Industry Division A

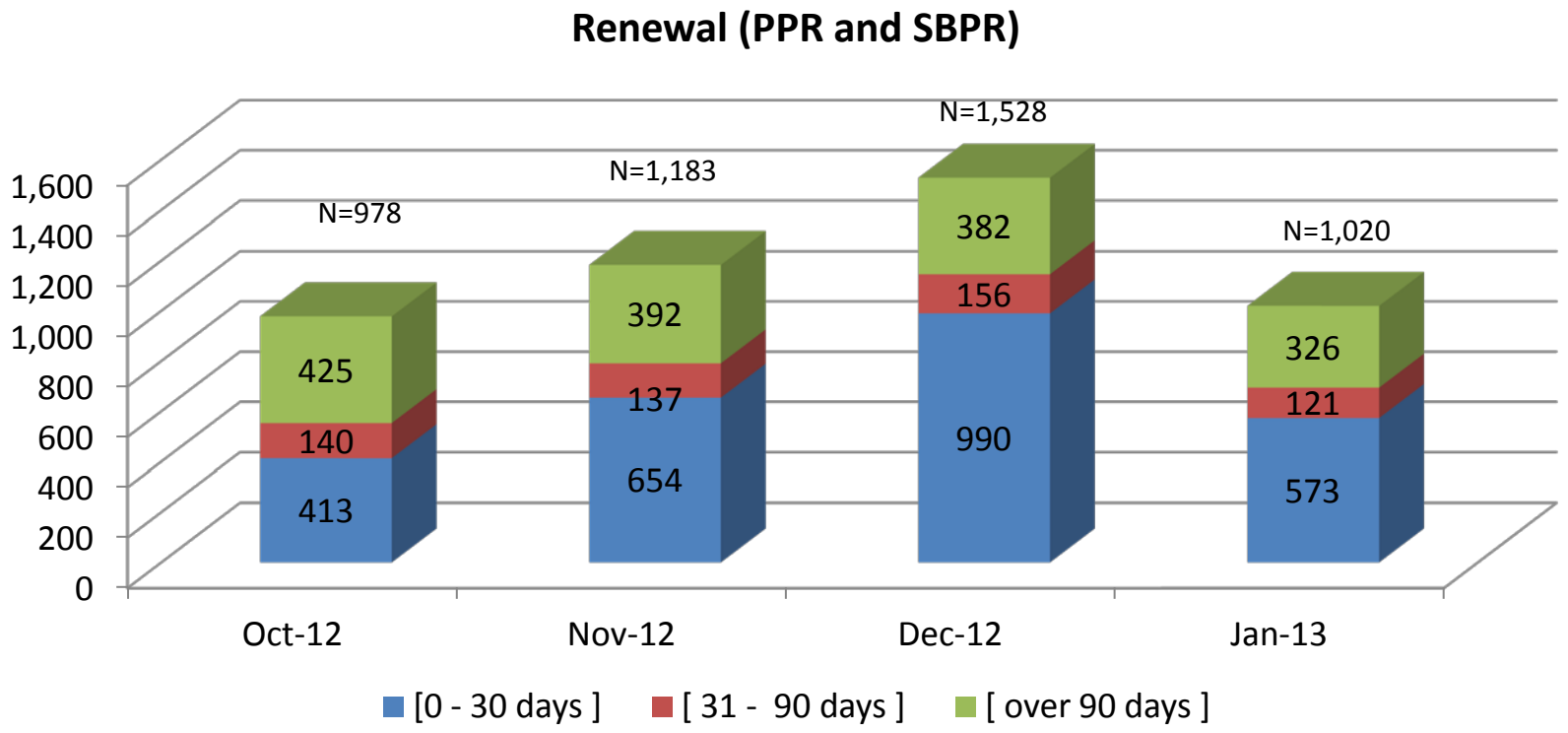
FY13 Initial Pending Adjudications



Case Type	Day Category	Oct-12	Nov-12	Dec-12	Jan-13
Initial (SSBI and NACLC)	[0 - 20 days]	1,510	2,776	2,557	2,336
	[21 - 90 days]	1,124	1,365	1,745	1,472
	[over 90 days]	2,300	2,017	1,960	1,866
Initial Total		**4,934**	**6,158**	**6,262**	**5,674**

Does not include cases with no investigation closed date

FY13 Renewal Pending Adjudications

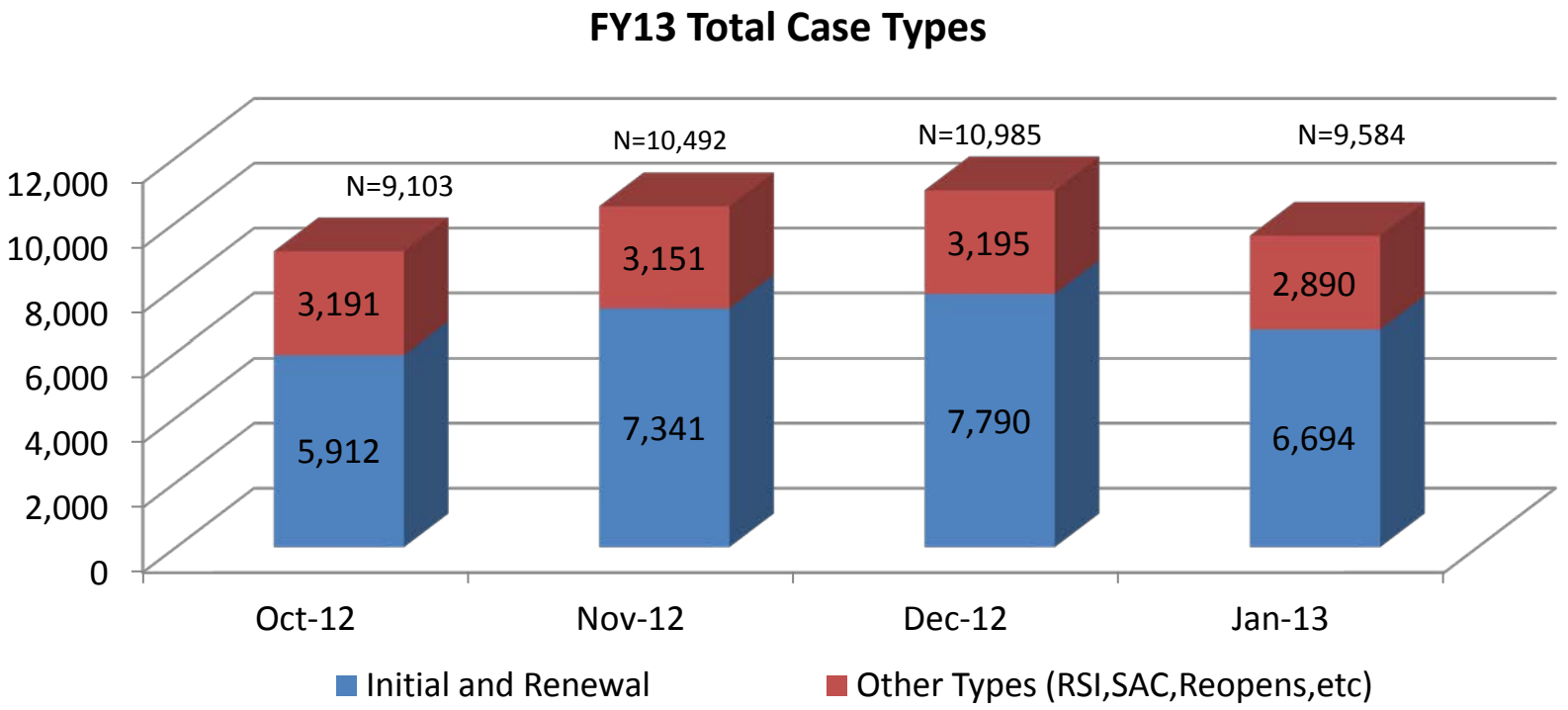


Case Type	Day Category	Oct-12	Nov-12	Dec-12	Jan-13
Renewal (SBPR and PPR)	[0 - 30 days]	413	654	990	573
	[31 - 90 days]	140	137	156	121
	[over 90 days]	425	392	382	326
Renewal Total		**978**	**1,183**	**1,528**	**1,020**

Does not include cases with no investigation closed date

FY13 Overall Pending Adjudications

SSBI / NACLC / TSPR / Other (Suspended Cases)

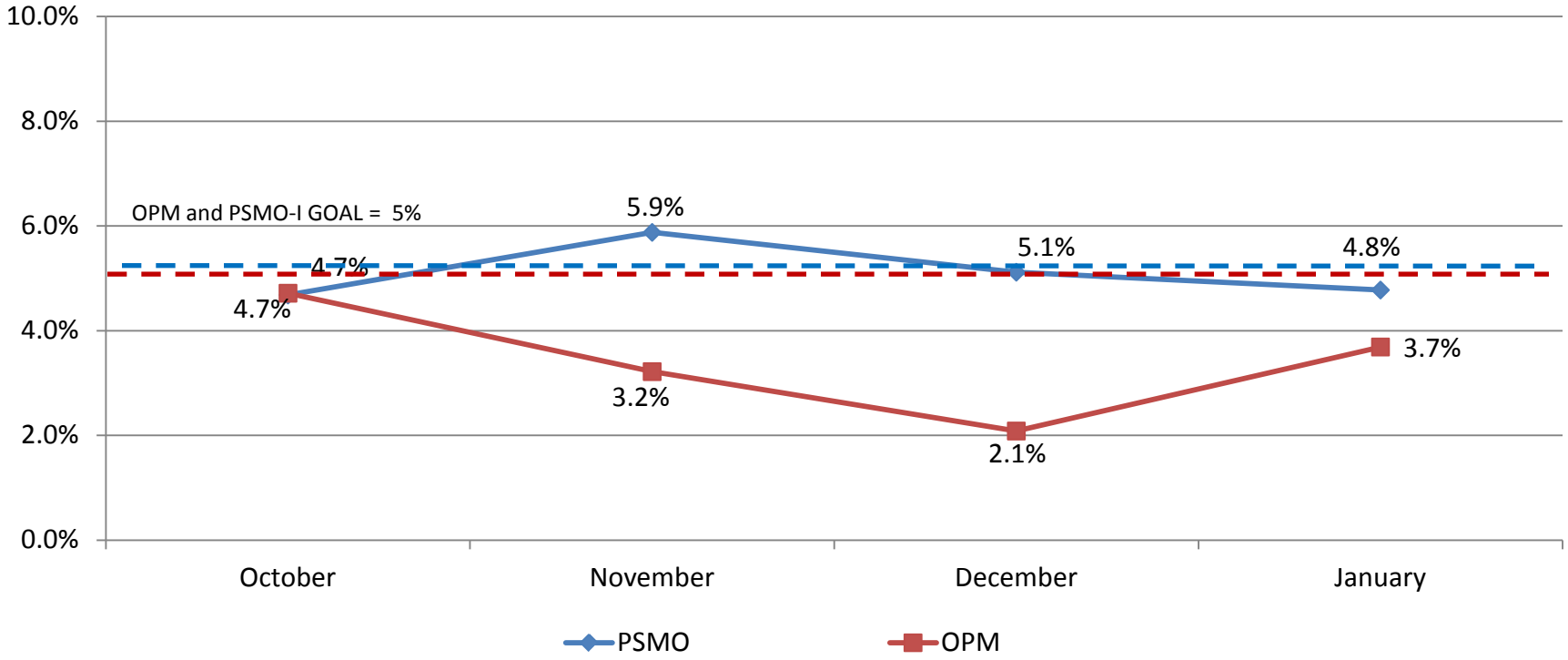


Case Type	Oct-12	Nov-12	Dec-12	Jan-13
Initial and Renewal	5,912	7,341	7,790	6,694
Other (RSI, SAC, Reopens, etc)	3,191	3,151	3,195	2,890
Total	**9,103**	**10,492**	**10,985**	**9,584**

Does not include cases with no investigation closed date

FY 13 PSMO and OPM Reject Rates

Initial and Periodic Reinvestigation Clearance Requests



Source: JPAS / OPM / PSMO Reports

- FY13 – PSMO-I received 55,666 investigation requests
  - Rejects – PSMO-I rejected 2,971 (5.3% on average) investigation requests for FSO re-submittal
- FY13 - OPM Received 61,819 investigation requests
  - Rejects – OPM rejected 2,208 (3.6% on average) investigation requests to PSMO-I (then FSO) for re-submittal

Defense Security Service (DSS)
FY13 Reasons for Case Rejection by DSS

Top Five PSMO-I Rejection Reasons	Count	Percent
Missing employment information (submitting organization)	686	54%
Missing social security number of spouse or co-habitant	184	15%
Missing relative information	150	12%
Missing Selective Service registration information	135	11%
Incomplete information concerning debts or bankruptcy	112	9%
Top Five Grand Total	**1,267**	**100%**

Source: JPAS/e-QIP

Defense Security Service (DSS)
FY13 Reasons for Case Rejection by OPM

Top Five OPM Rejection Reasons	Count	Percent
Fingerprint card not submitted within required timeframe (14 days)	885	59%
Missing or Illegible Certification / Release Forms	459	31%
Discrepancy with applicant's place of birth and date of birth	97	7%
Missing or Discrepant Reference Information	35	2%
Missing or Discrepant Employment Information	16	1%
Top Five Grand Total	**1,492**	**100%**

Source: PSMO-I Manual Count

Defense Security Service (DSS)
FY13 eQIP Rejections by Facility Category

Month	Facility Category						
	A	AA	B	C	D	E	Others
October	0.6%	0.8%	1.0%	1.9%	7.6%	14.5%	0.1%
November	0.3%	0.6%	0.8%	1.3%	5.3%	12.5%	0.1%
December	0.6%	0.7%	1.0%	2.2%	5.4%	12.2%	0.1%
January	1.0%	0.8%	1.1%	2.5%	7.4%	17.5%	0.2%
Grand Total	**2.5%**	**2.9%**	**3.8%**	**7.9%**	**25.7%**	**56.7%**	**0.5%**

Case Rejections

82.4% of cases rejected by DISCO and OPM originate from smaller Category D and E facilities

Source: JPAS/e-QIP

Defense Security Service

Summary and Takeaways:

- IRTPA
  - Industry Division A continues to exceed IRTPA timelines (avg 8 days)
  - Industry Division A case inventory is at a very healthy level (~10K)
- Cases Pending at OPM
  - 30 to 40% increase in number of PRs submitted to OPM led to 20% increase in OPM inventory of Industry PSIs
- e-QIP Rejects Decrease
  - Significant reduction since 2010 version of SF86 implemented
  - Missing employment information still #1 PSMO 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- OPM PCL Presentation

a New Day for Federal Service

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

March 20, 2013 NISPPAC

Summary

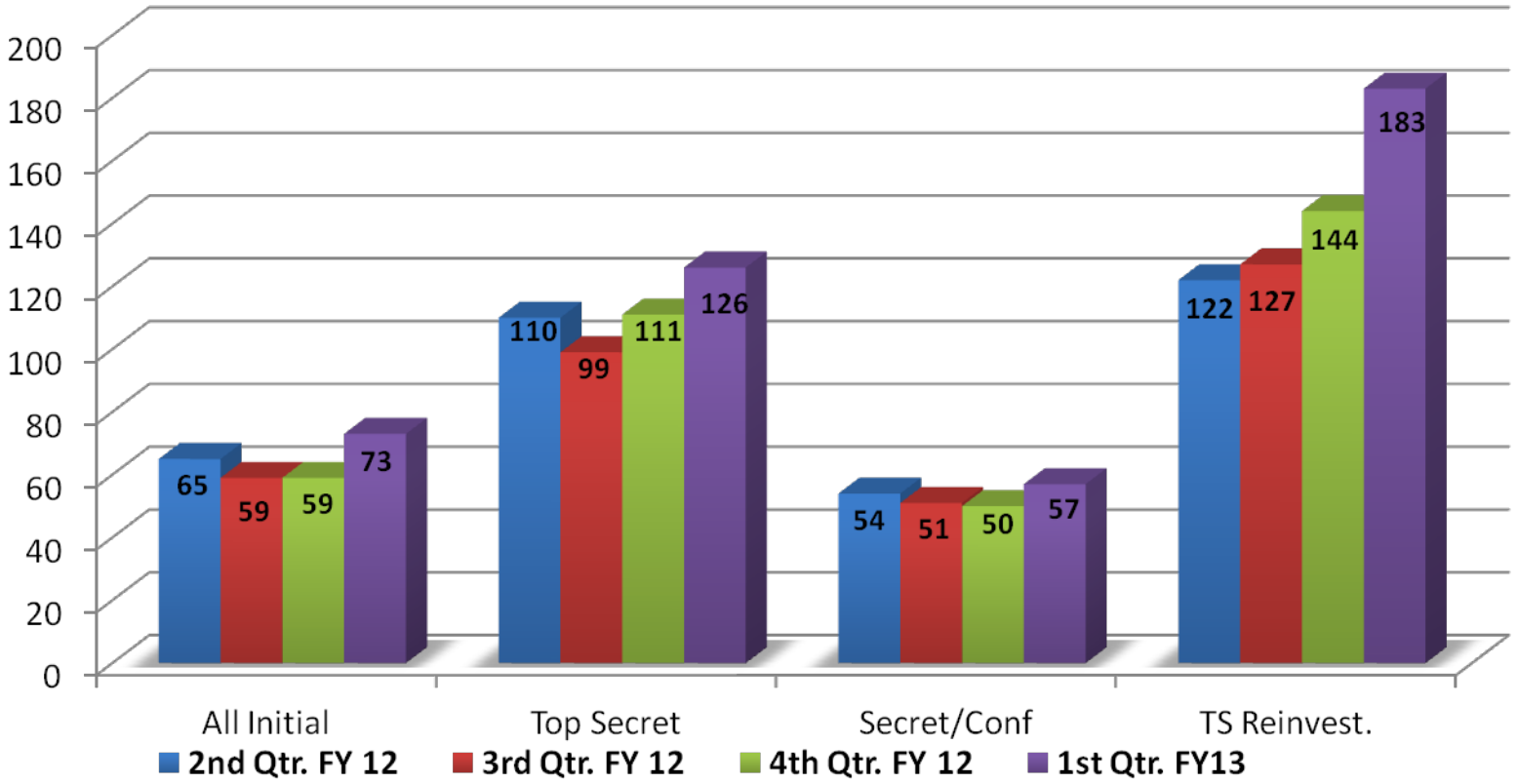
Data reflects consequences of changes in workload distribution (receipts), which impacted all investigation workloads

- PR Workload increased
- NACLC receipts (non NISP) decreased

- **Increase in "investigate" time for SSBIs:**
  - Contractor field performance untimely
  - Resource Management (Contractor Capacity)
  - NAC Timeliness
  - Policy Changes
- **"Adjudicate" time impacted by workload fluctuations**

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

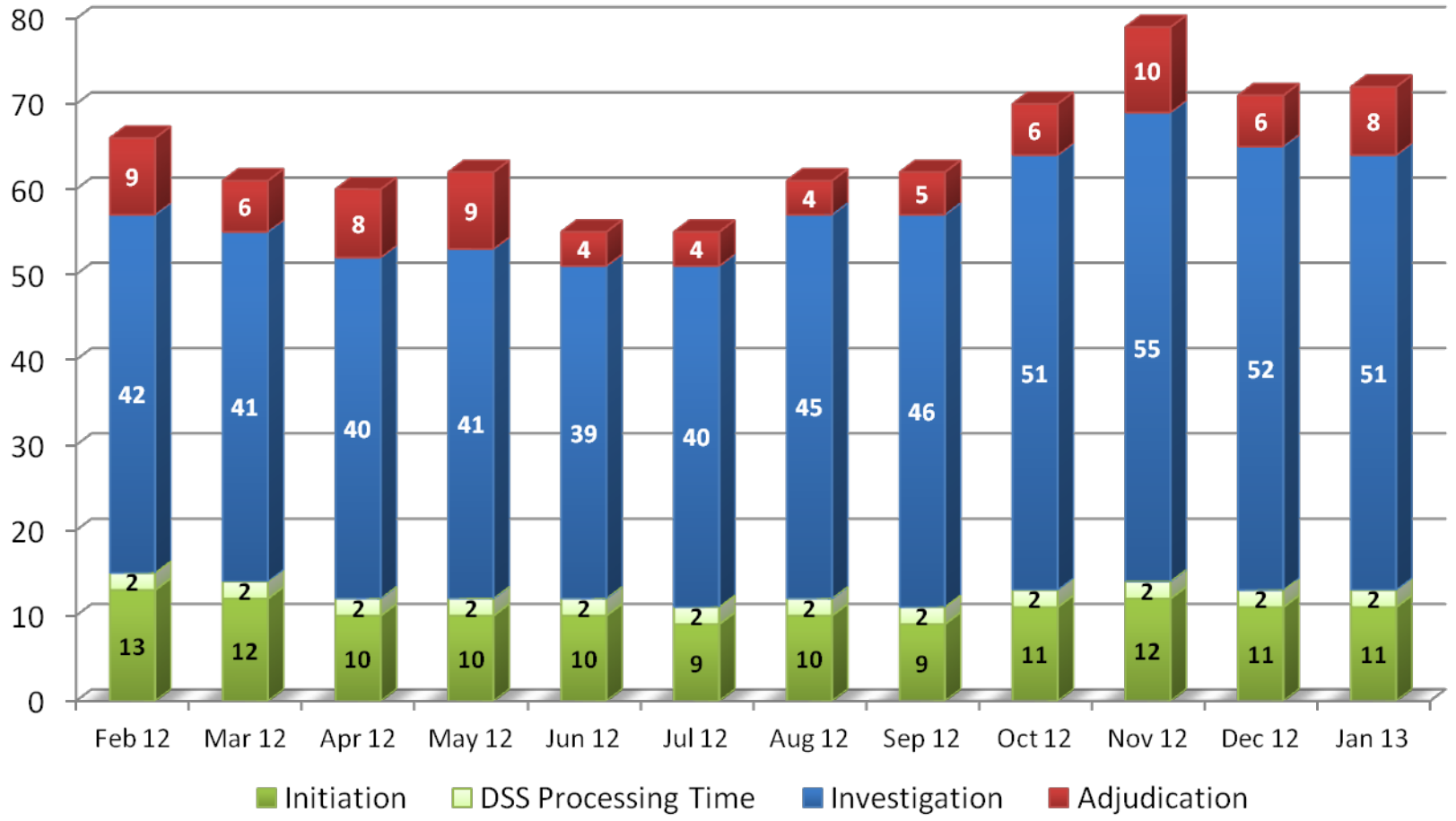
Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 2nd Q 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	4,321	22,675	12,492
Adjudication actions taken – 1st Q FY13	15,074	3,454	11,620	7,089

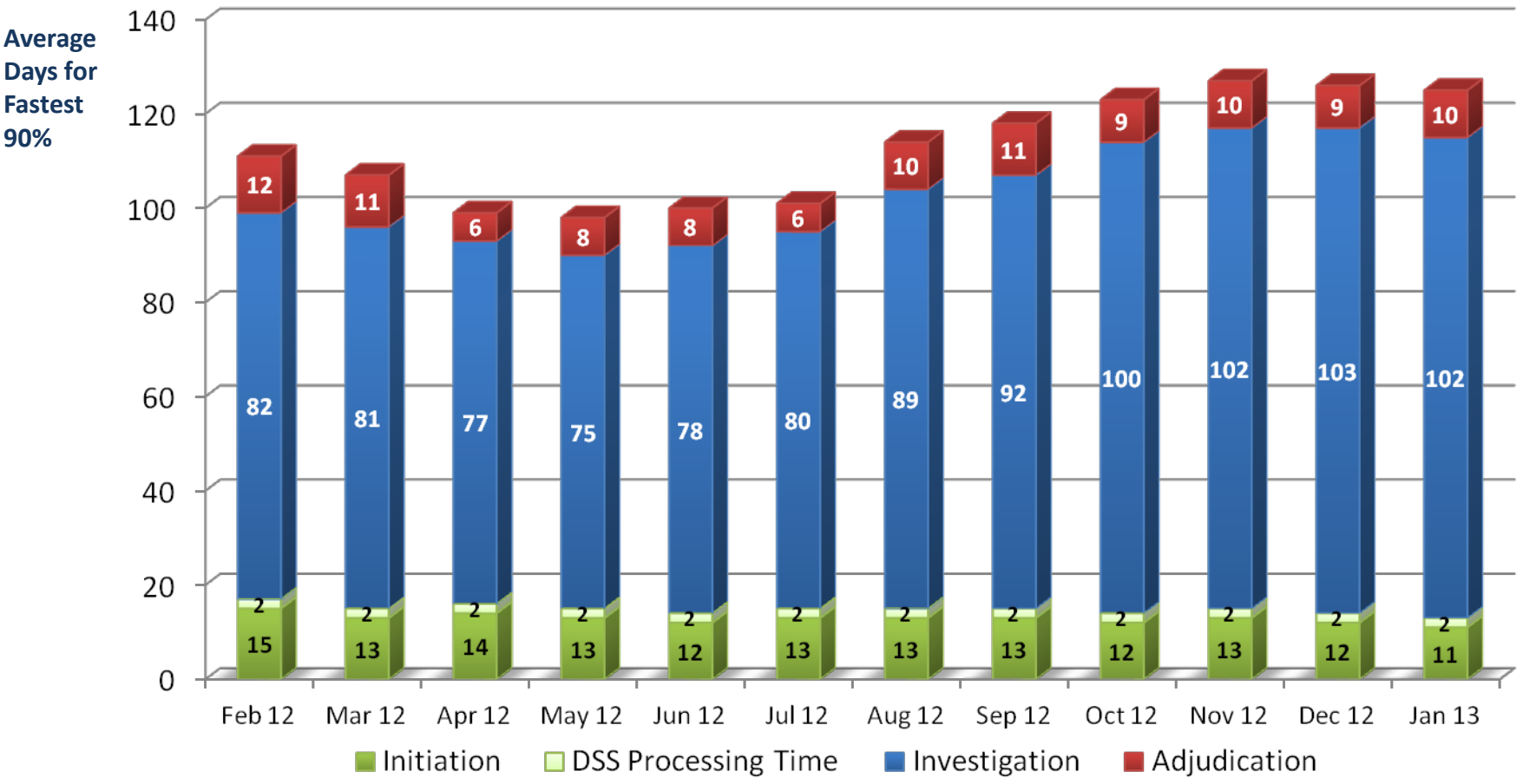
*The adjudication timeliness include collateral adjudication by DISCO and SCI adjudication by other DoD adjudication facilities

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



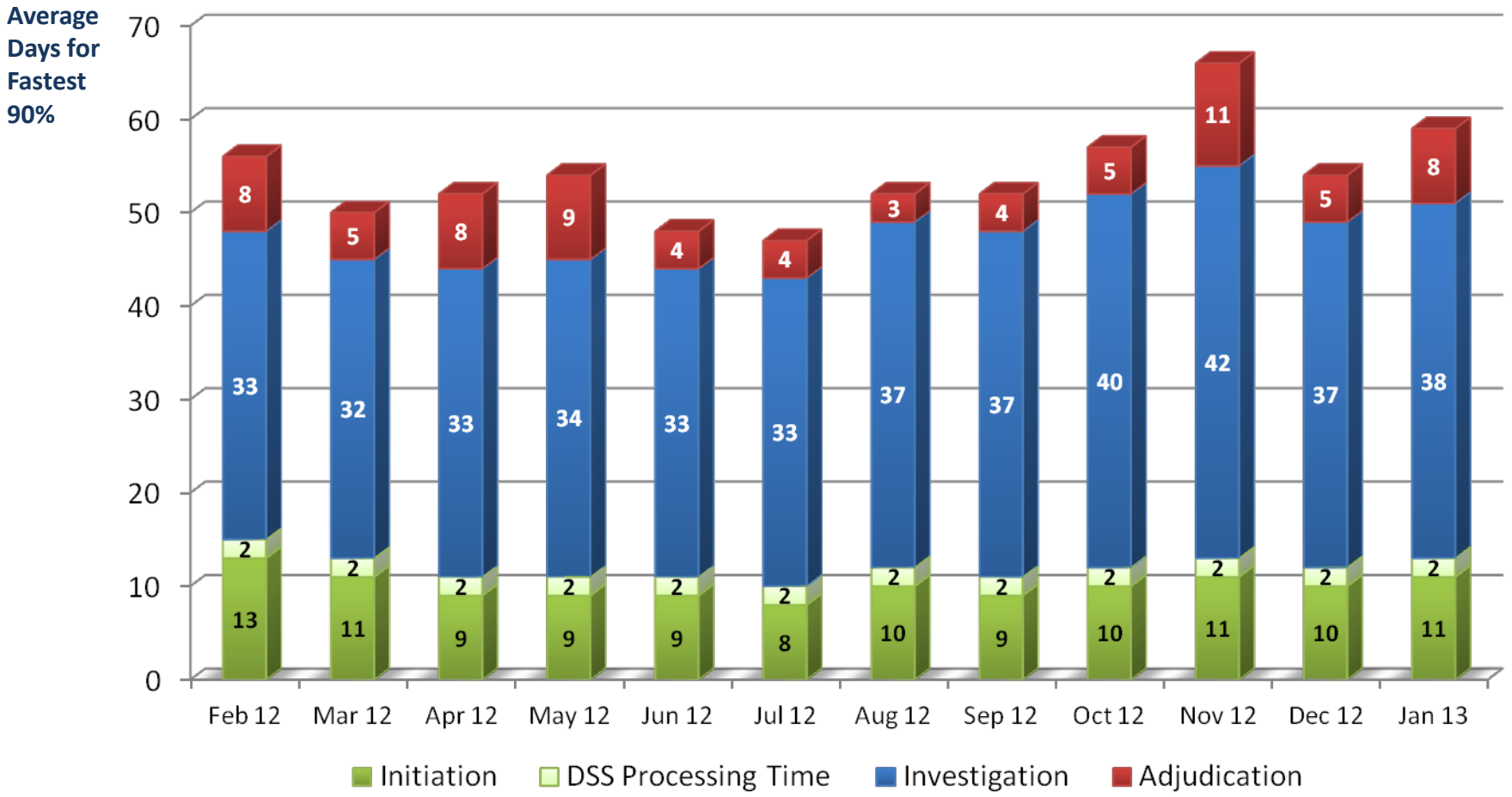
	Feb 12	Mar 12	Apr 12	May 12	Jun 12	Jul 12	Aug 12	Sep 12	Oct 12	Nov 12	Dec 12	Jan 13
100% of Reported Adjudications	8,940	10,769	8,755	10,633	10,980	4,013	10,333	8,054	3,745	3,343	7,901	8,710
Average Days for Fastest 90%	66 days	61 days	60 days	62 days	55 days	55 days	61 days	62 days	70 days	79 days	71 days	72 days

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



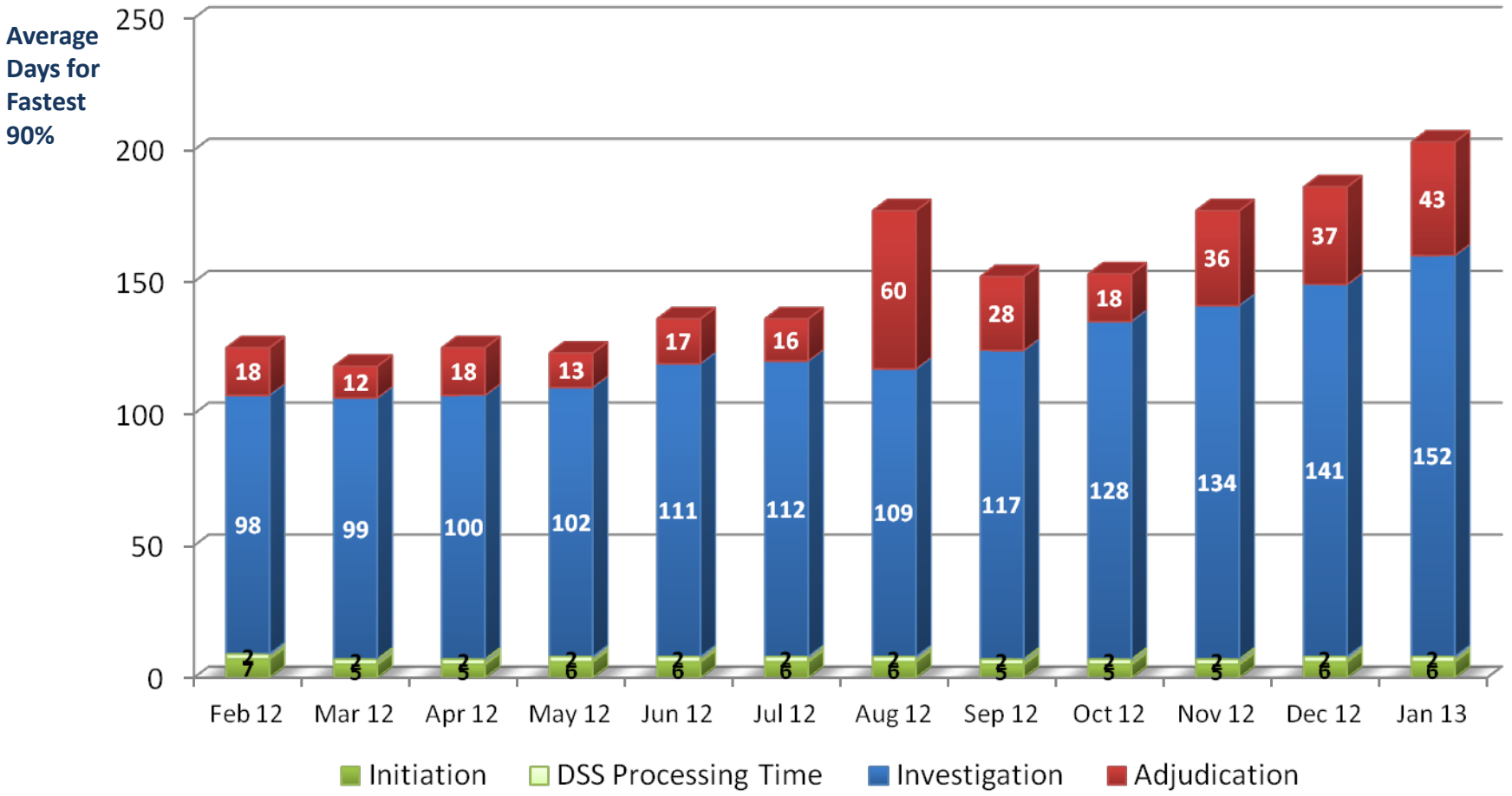
	Feb 12	Mar 12	Apr 12	May 12	Jun 12	Jul 12	Aug 12	Sep 12	Oct 12	Nov 12	Dec 12	Jan 13
100% of Reported Adjudications	1,688	2,099	1,519	2,023	1,625	595	1,573	1,420	740	718	1,945	1,805
Average Days for fastest 90%	111 days	107 days	99 days	98 days	100 days	101 days	114 days	118 days	123 days	127 days	126 days	125 days

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



	Feb 12	Mar 12	Apr 12	May 12	Jun 12	Jul 12	Aug 12	Sep 12	Oct 12	Nov 12	Dec 12	Jan 13
100% of Reported Adjudications	7,252	8,670	7,236	8,610	9,355	3,418	8,760	6,634	3,005	2,625	5,956	6,905
Average Days for fastest 90%	56 days	50 days	52 days	54 days	48 days	47 days	52 days	52 days	57 days	66 days	54 days	59 days

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



	Feb 12	Mar 12	Apr 12	May 12	Jun 12	Jul 12	Aug 12	Sep 12	Oct 12	Nov 12	Dec 12	Jan 13
100% of Reported Adjudications	2,726	4,087	2,813	3,841	3,988	3,053	4,678	3,024	1,317	1,783	3,443	3,125
Average Days for fastest 90%	125 days	118 days	125 days	123 days	136 days	136 days	177 days	152 days	153 days	177 days	186 days	203 days

Takeaways

Enterprise most efficient when the level of field work is consistent with our planning

- Variances between workload projections and actual submissions affect workload management
- Unexpected workload surges, or unanticipated events such as the large scale impact of Hurricane Sandy, will impact the month by month timeliness view
- NAC Timeliness a continuing concern due to resource constraints

Work is moved and resources are realigned to achieve timeliness expectations

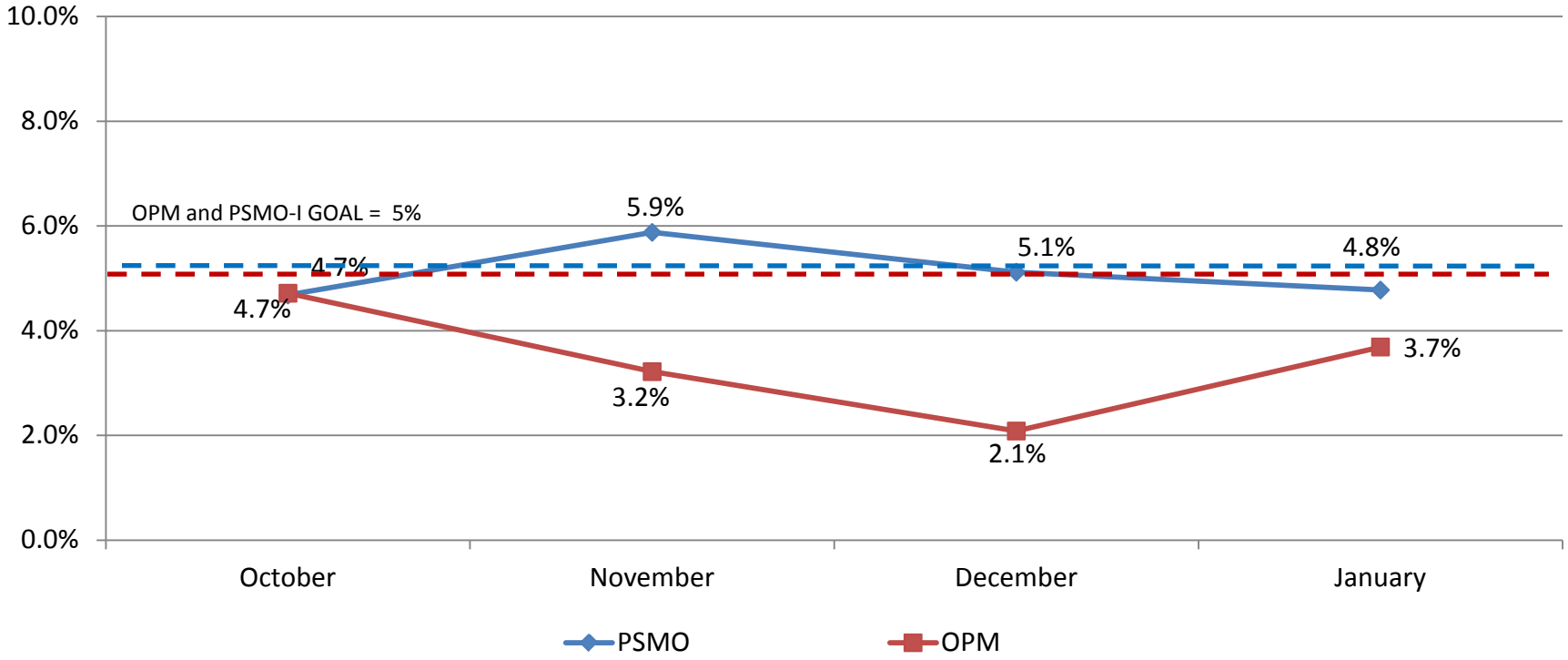
Looking Ahead

- Overall SSBI IRTPA “investigate” timeliness has returned to acceptable level
- PRs aging

Attachment #6- PSMO PCL Presentation

FY 13 PSMO and OPM Reject Rates

Initial and Periodic Reinvestigation Clearance Requests



Source: JPAS / OPM / PSMO Reports

- FY13 – DSS received 55,666 investigation requests
  - Rejects – DSS rejected 2,971 (5.3% on average) investigation requests for FSO re-submittal
- FY13 - OPM Received 61,819 investigation requests
  - Rejects – OPM rejected 2,208 (3.6% on average) investigation requests to DSS (then FSO) for re-submittal

Defense Security Service (DSS)
FY13 Reasons for Case Rejection by DSS

Top Five PSMO-I Rejection Reasons	Count	Percent
Missing employment information (submitting organization)	686	54%
Missing social security number of spouse or co-habitant	184	15%
Missing relative information	150	12%
Missing Selective Service registration information	135	11%
Incomplete information concerning debts or bankruptcy	112	9%
Top Five Grand Total	**1,267**	**100%**

Source: JPAS/e-QIP

Defense Security Service (DSS)
FY13 Reasons for Case Rejection by OPM

Top Five OPM Rejection Reasons	Count	Percent
Fingerprint card not submitted within required timeframe (14 days)	885	59%
Missing or Illegible Certification / Release Forms	459	31%
Discrepancy with applicant's place of birth and date of birth	97	7%
Missing or Discrepant Reference Information	35	2%
Missing or Discrepant Employment Information	16	1%
Top Five Grand Total	**1,492**	**100%**

Source: PSMO-I Manual Count

Defense Security Service (DSS)
FY13 eQIP Rejections by Facility Category

Month	Facility Category						
	A	AA	B	C	D	E	Others
October	0.6%	0.8%	1.0%	1.9%	7.6%	14.5%	0.1%
November	0.3%	0.6%	0.8%	1.3%	5.3%	12.5%	0.1%
December	0.6%	0.7%	1.0%	2.2%	5.4%	12.2%	0.1%
January	1.0%	0.8%	1.1%	2.5%	7.4%	17.5%	0.2%
Grand Total	**2.5%**	**2.9%**	**3.8%**	**7.9%**	**25.7%**	**56.7%**	**0.5%**

Case Rejections

82.4% of cases rejected by DSS and OPM originate from smaller Category D and E facilities

Source: JPAS/e-QIP

Defense Security Service

Summary and Takeaway:

- e-QIP Rejects Decrease
  - Significant reduction since 2010 version of SF86 implemented
  - Missing employment information still #1 DSS 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 #7- ODNI PCL Presentation

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

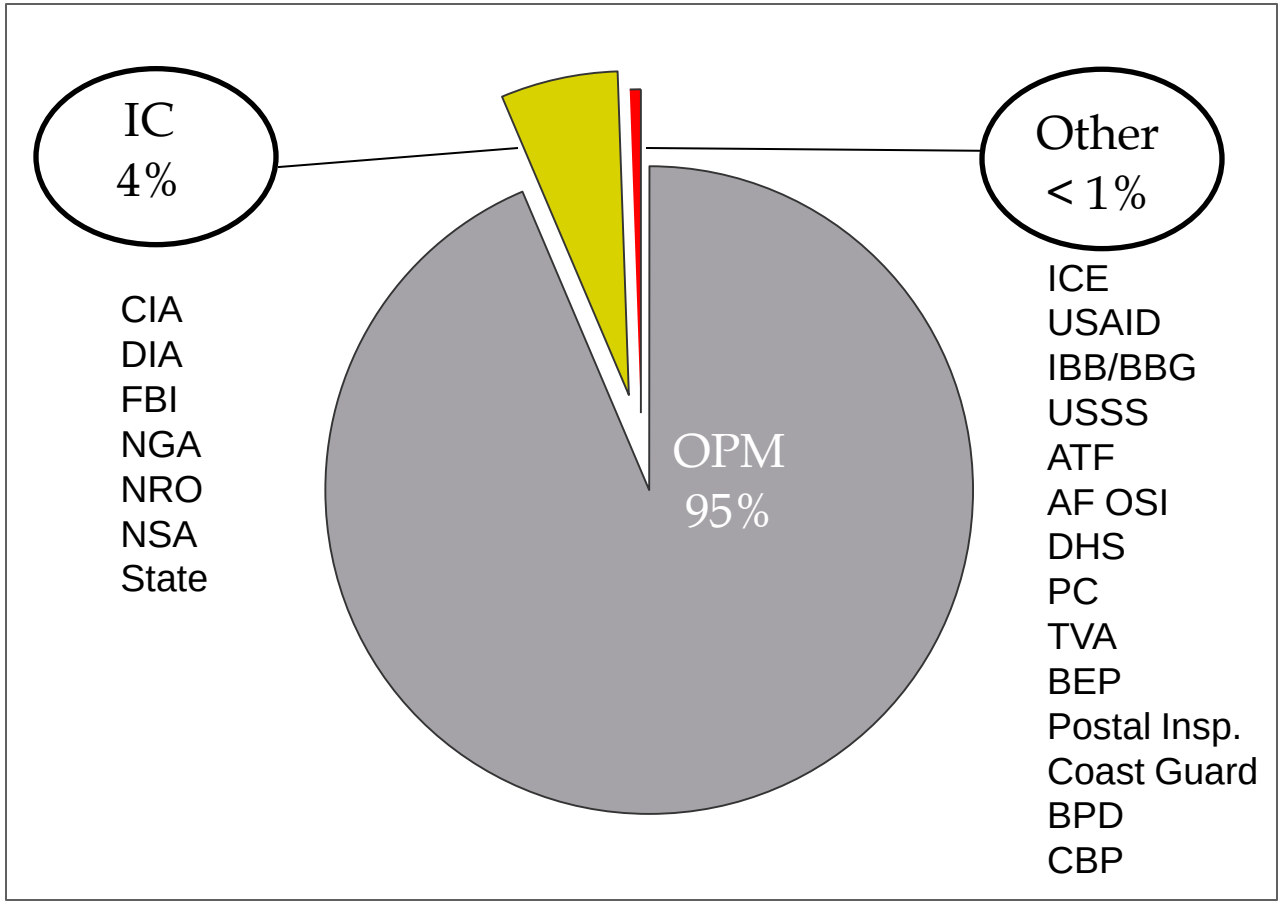
Industry Performance Metrics

ONCIX/Special Security Directorate

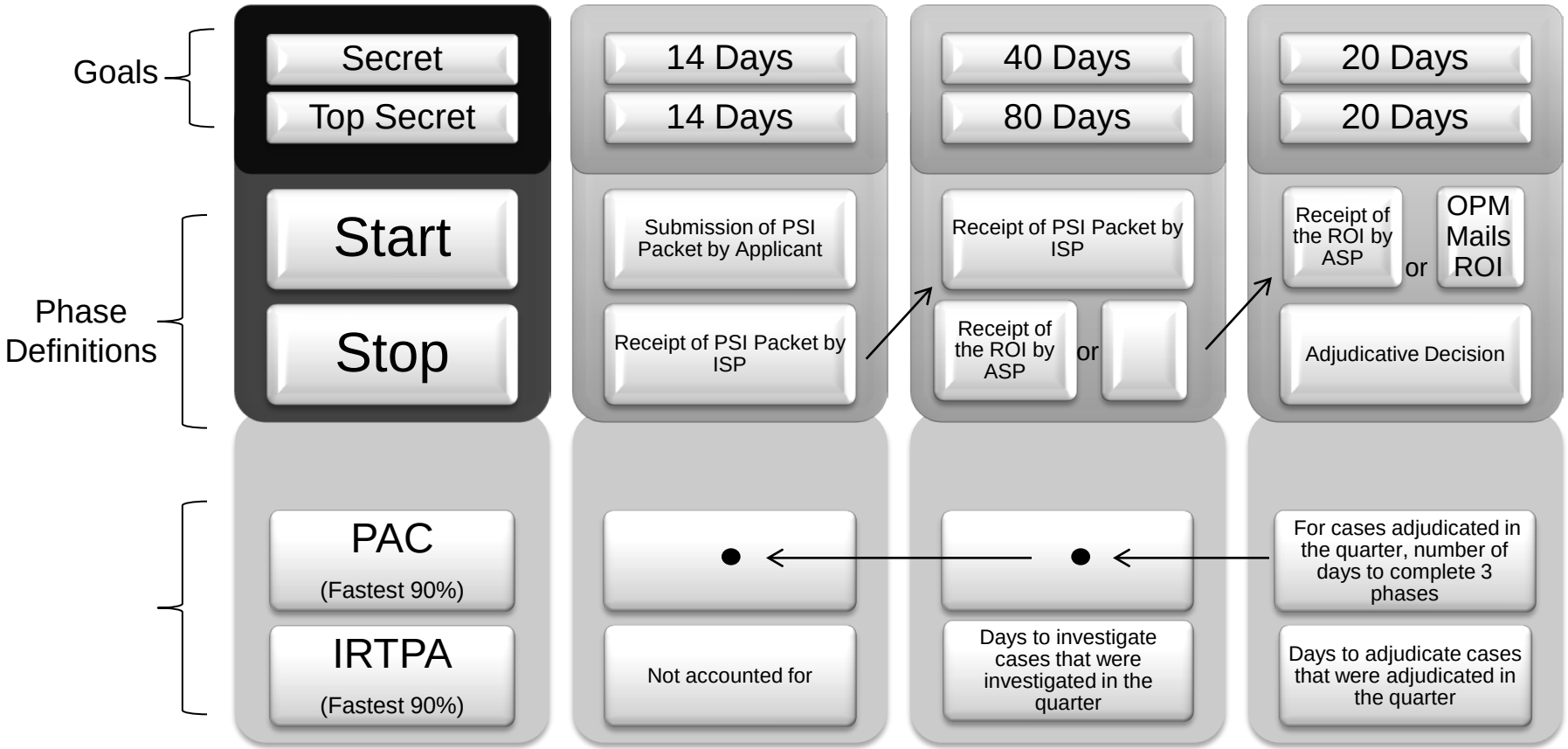
LEADING INTELLIGENCE INTEGRATION

NISPPAC
20 March 2013

Overall Volume by ISP



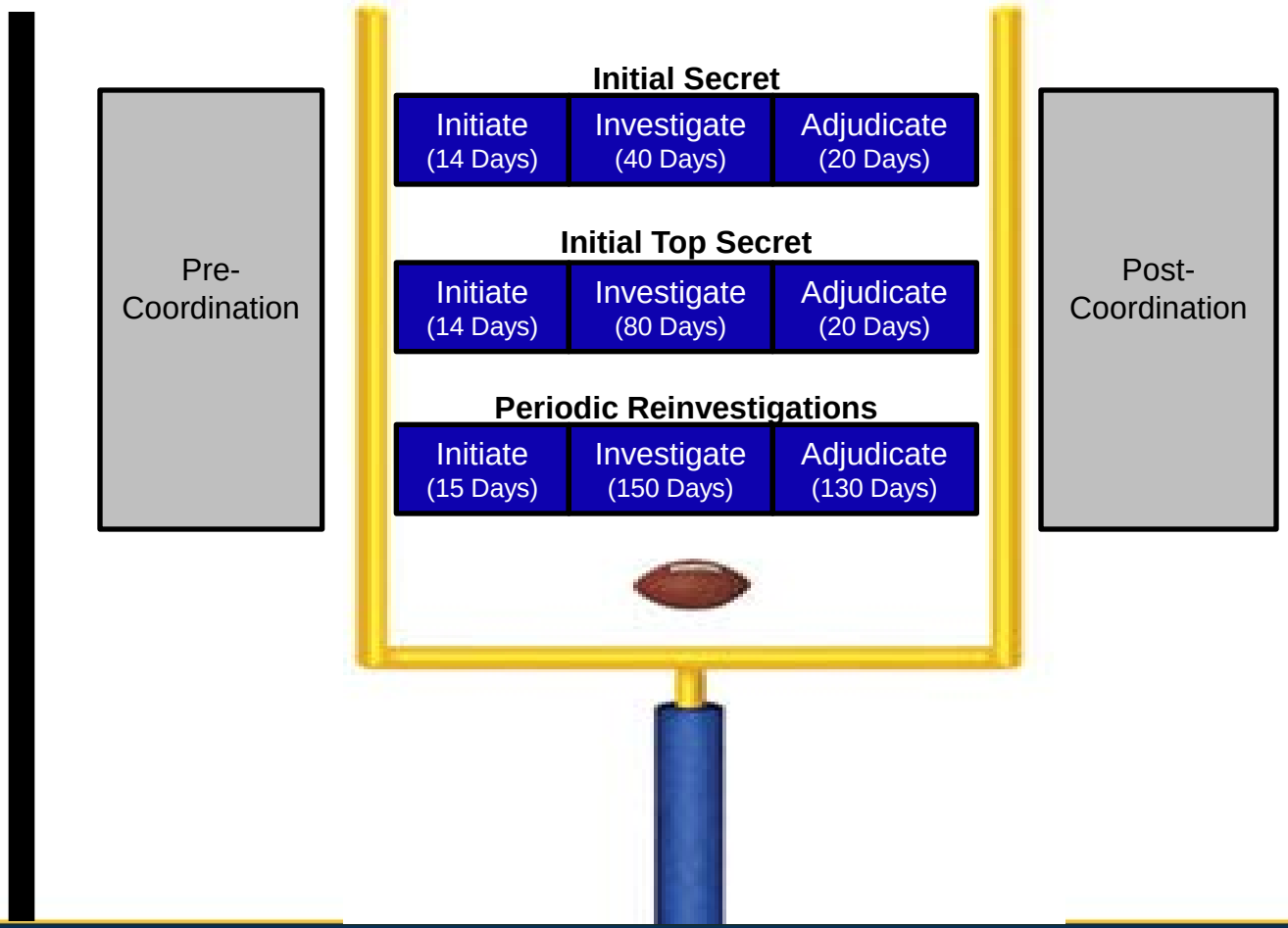
Performance Management & Collection



PSI Packet: Personnel Security Investigation Packet (PSI forms, releases, fingerprint cards, etc.) required to conduct an investigation by the investigative service provider
ISP: Investigative Service Provider
ASP: Adjudicative Service Provider
ROI: Report of Investigation
Adjudicative Decision: Either a decision by the adjudicator to approve or process to deny

PAC Security Clearance Methodology

- Timeliness data on the following slides reflects USG performance on Contractor cases
- Timeliness data is being provided to report how long contractor cases are taking- not contractor performance
- As shown in the diagram, 'Pre/Post' casework is not considered in the PAC Timeliness Methodology



Q1 FY2013 Timeliness for Industry

Intelligence Community Timeliness for Industry

There are 7 IC agencies that report metrics as delegated ISPs (4% of USG workload)

Effective 1 October 2012, a separate Top Secret timeliness goal was established

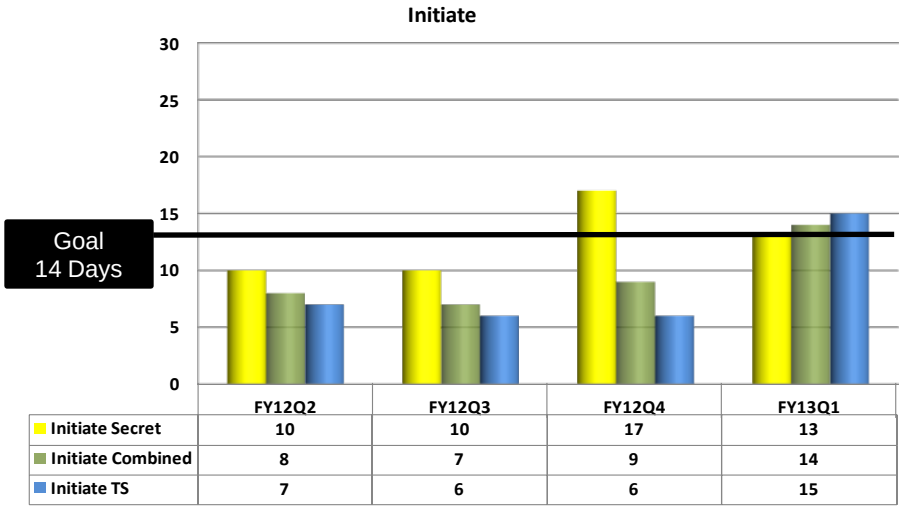
- Initials
  - Top Secret – Goal 114 days (14/80/20)
    - Industry End-to-End processing time decreased from 141 days in the 4th Quarter 2012 to 131 days in the 1st Quarter for the fastest 90% of Top Secret initial cases
  - Secret – Goal 74 days (14/40/20)
    - Industry End-to-End processing time increased from 89 days in the 4th Quarter 2012 to 95 days in the 1st Quarter for the fastest 90% of Secret initial cases
- Periodic Reinvestigations
  - Combined Performance – Goal 195 days (15/150/30 days)

    Industry End-to-End processing time increased from 181 days in the 4th Quarter 2012 to 228 days in the 1st Quarter for the fastest 90% of Periodic Reinvestigations

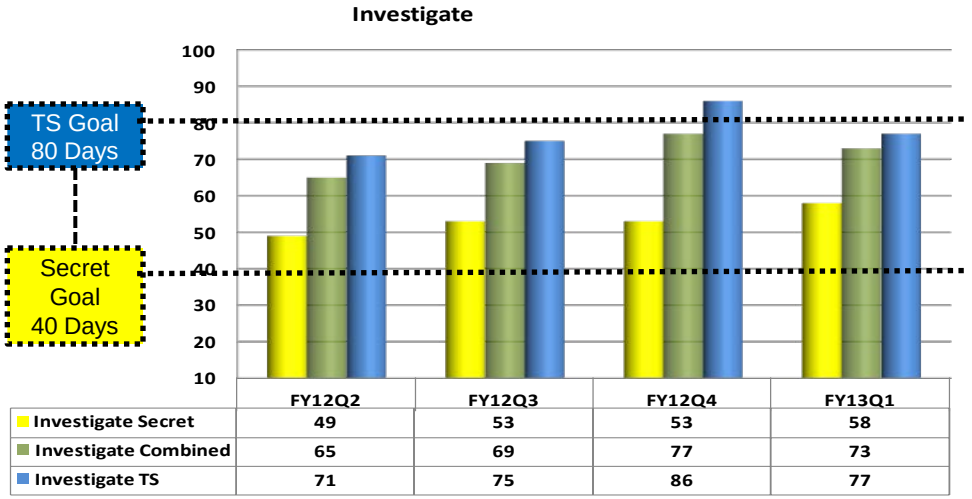
Other Delegated Investigative Service Provider's (ISP) Timeliness for Industry

- 3 of the 14 Delegated ISPs conducted initial investigations on contractors
- Only one agency conducted periodic reinvestigations on contractors
- As a result, meaningful data could not be derived from the limited number of investigations/adjudications

Intelligence Community
Secret/Top Secret and Combined Initials
(4% of USG Workload)



	FY12Q2	FY12Q3	FY12Q4	FY13Q1
Initiate Secret	10	10	17	13
Initiate Combined	8	7	9	14
Initiate TS	7	6	6	15

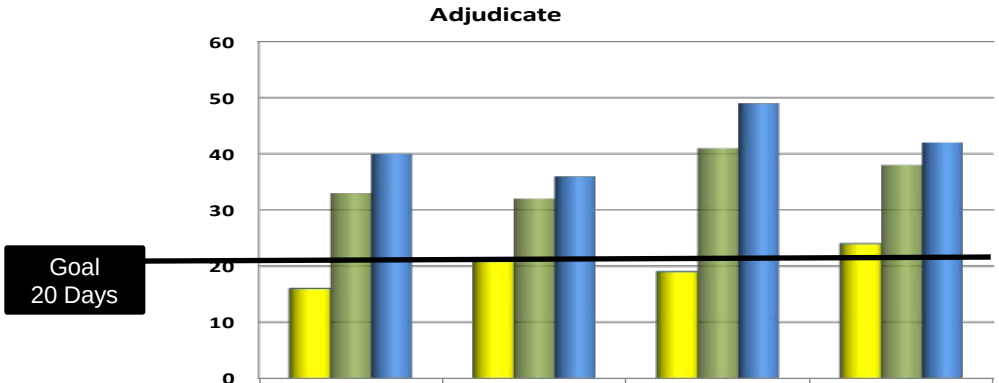


	FY12Q2	FY12Q3	FY12Q4	FY13Q1
Investigate Secret	49	53	53	58
Investigate Combined	65	69	77	73
Investigate TS	71	75	86	77

Timeliness:

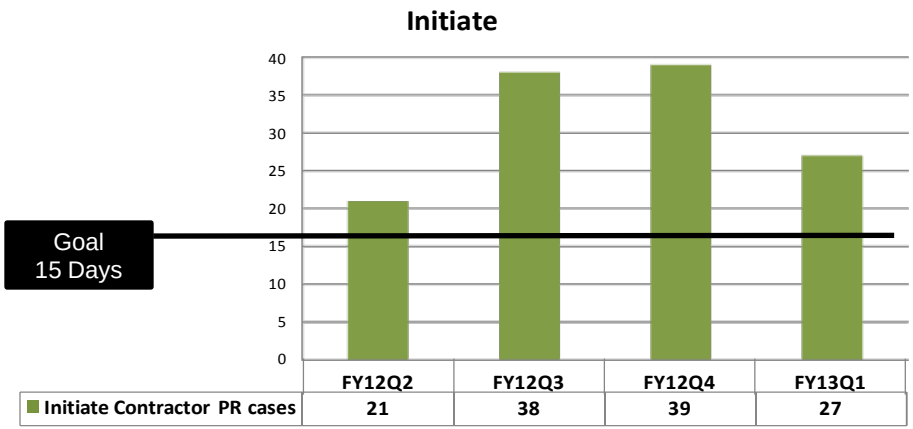
for Contractors

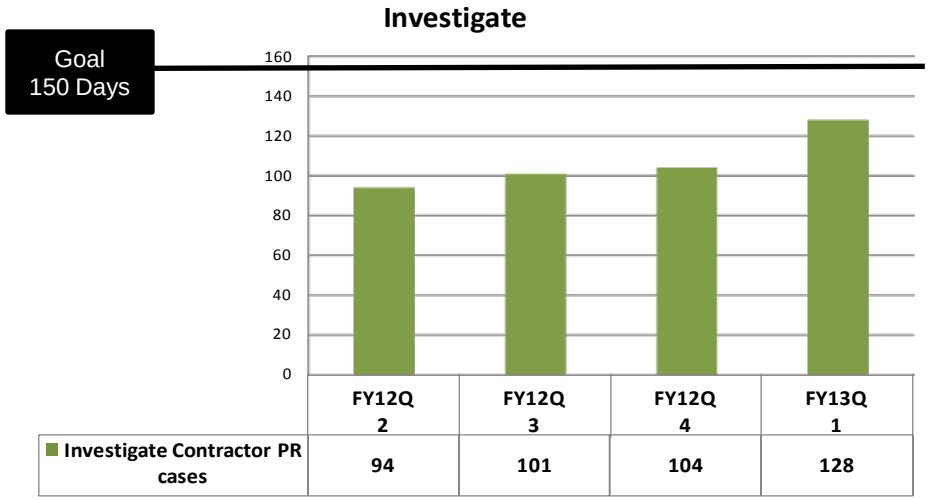
TS Goal: 114 days
Secret Goal: 74 days



	FY12Q2	FY12Q3	FY12Q4	FY13Q1
Adjudicate Secret	16	21	19	24
Adjudicate Combined	33	32	41	38
Adjudicate TS	40	36	49	42

Intelligence Community
Combined Periodic Reinvestigations
(4% of USG Workload)

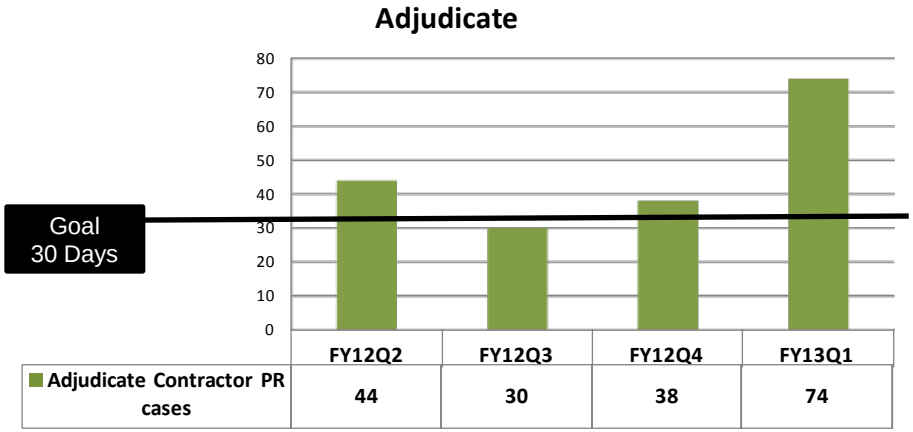




Timeliness:

for Contractors

Goal: 195 days



2012 Intelligence Authorization Act Report on Security Clearance Determinations

Number of Cleared individuals on 10/1/2012

Held a security clearance at such level:

Employee Type	As of 10/1/11:		As of 10/1/12:	
	Conf/Secret	Top Secret	Conf/Secret	Top Secret
Government	2,693,402	766,245	2,757,333	791,200
Contractor	598,006	478,835	582,524	483,263
Other	161,606	165,458	167,925	135,506
Sub-Total:	3,453,014	1,410,538	3,507,782	1,409,969

Total: 4,863,552 | 4,917,751

Number of Favorable determinations from 10/1/2011 to 9/30/2012

Approved for a security clearance at such level:

Employee Type	As of 10/1/11:		As of 10/1/12:	
	Conf/Secret	Top Secret	Conf/Secret	Top Secret
Government	400,490	178,926	364,498	140,016
Contractor	97,453	102,277	108,933	133,493
Other	42,546	29,702	38,045	13,633
Sub-Total:	540,489	310,905	511,476	287,142

Total: 851,394 | 798,618

- Includes all individuals in access, in addition to those deemed eligible to hold a clearance

- Could not distinguish between initial and PR determinations in Scattered Castles
- Does not take into account individuals that are debriefed or removed from access

Attachment #8- DOE PCL Presentation

U.S. Department of Energy

Personnel Security Brief

February 2013

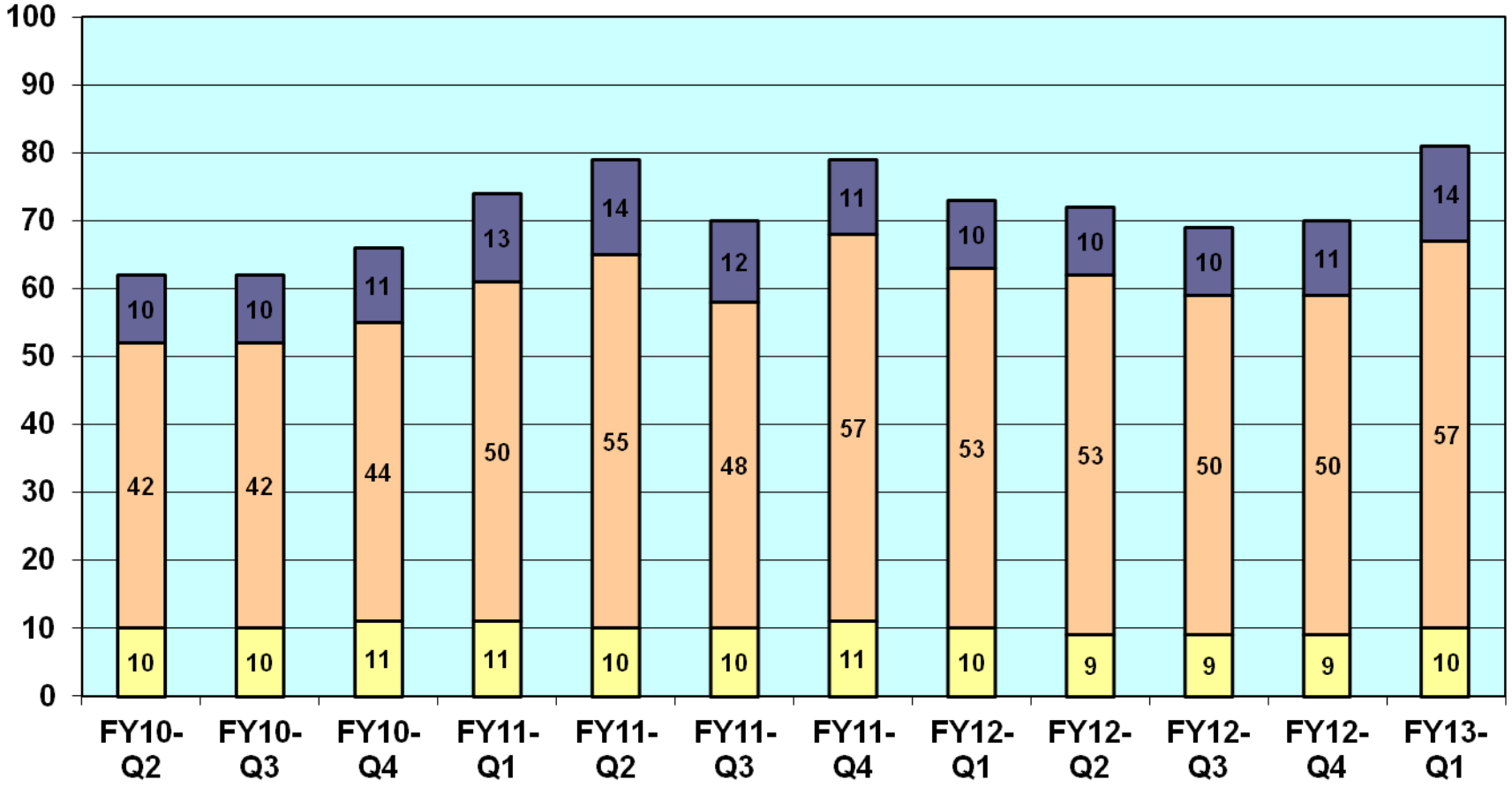
Personnel Security Overview

- DOE adjudicates both Federal and contractor staff
- Eight adjudicative facilities
- Policy, administrative review, and appeal functions centralized at Headquarters
- Cleared contractors, as of February 14, 2013:

  -61,387 Q access authorizations

  -23,158 L access authorizations
- Have met IRTPA initial security clearance adjudicative goals since April 2009

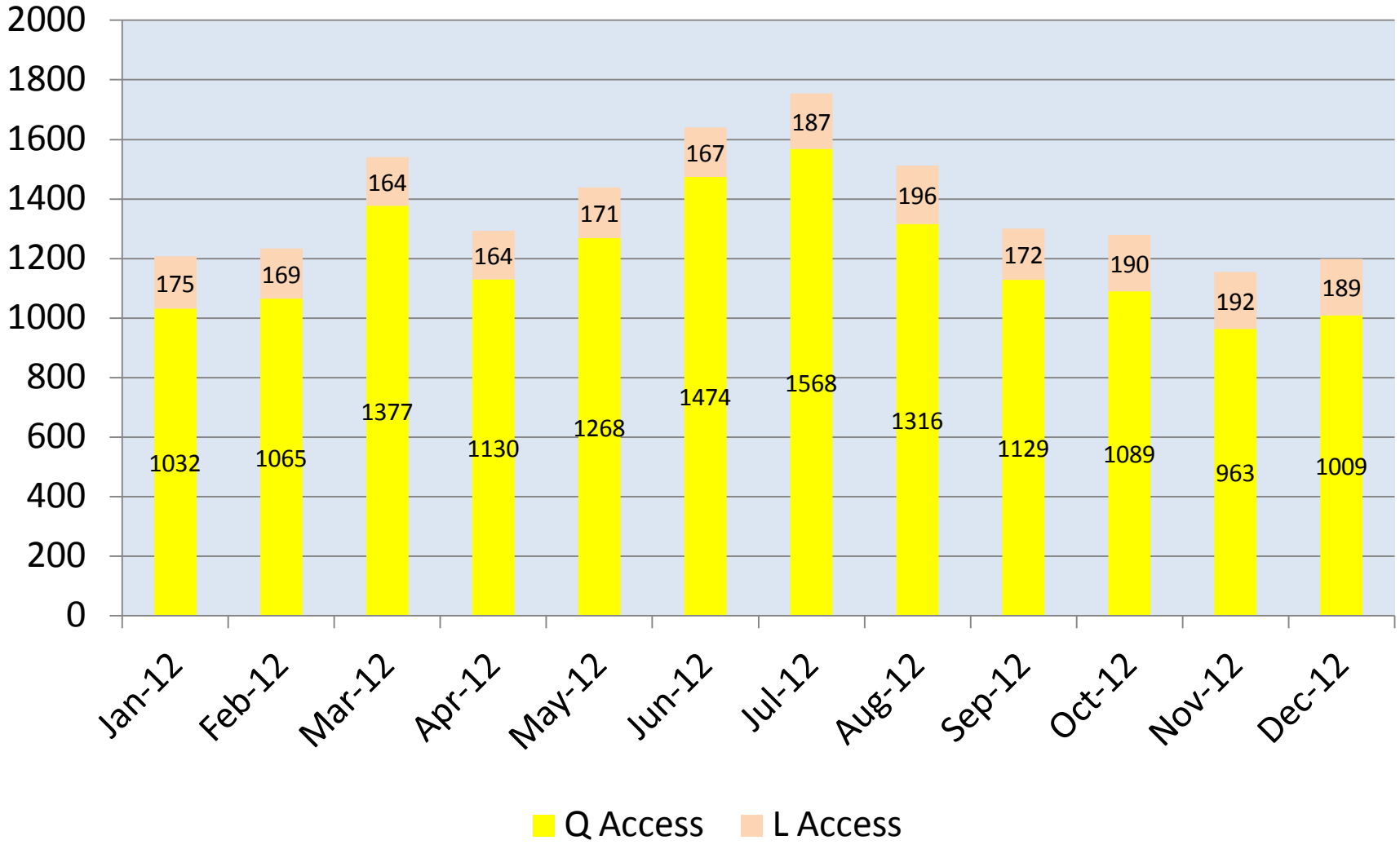
DOE's Average End-to-End Timeliness Trends for 90% Initial Q/TS and All L/S/C Security Clearances (Goal: 74 Days)



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 9- NRC PCL Presentation

U.S. NUCLEAR REGULATORY COMMISSION PERSONNEL SECURITY BRIEFING

Valerie Kerben, Chief
Personnel Security Branch
Division of Facilities & Security
Office of Administration
March 2013

PERSONNEL SECURITY PROGRAM OVERVIEW

•NRC employees are in sensitive positions and require access to national security information and be eligible for a security clearance.

•NRC requests all background investigations directly with the Office of Personnel Management (OPM).

•NRC is responsible to render adjudicative determinations for the Federal staff, Contractors, and Licensees.

•NRC has a Drug-Free Workplace Plan and tests all applicants, conducts employee random testing at 50% of FTE and tests contractors meeting specific criteria.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

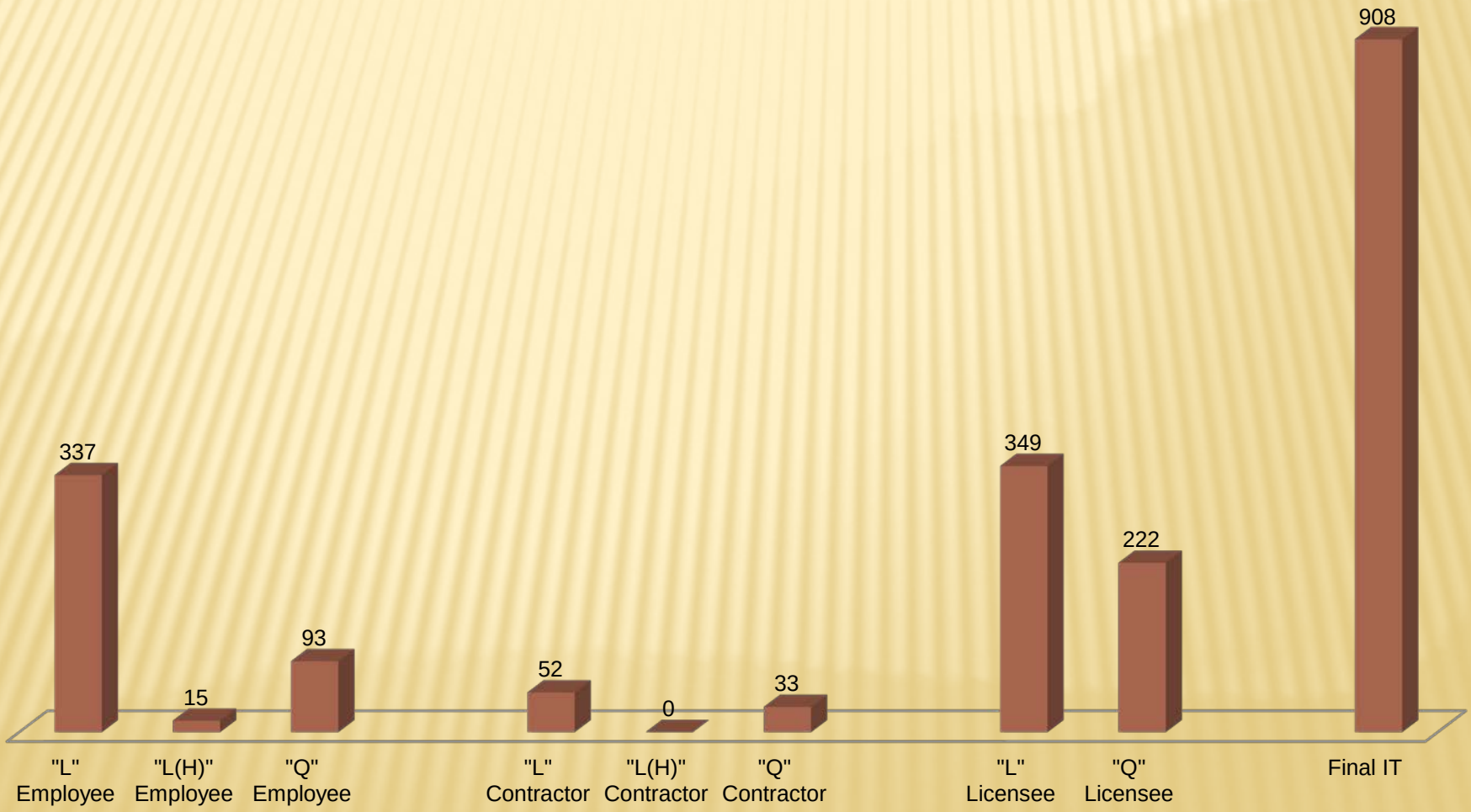
ACTIVE CLEARANCES

As of February 1, 2013 the following reflects active security clearances within the NRC:

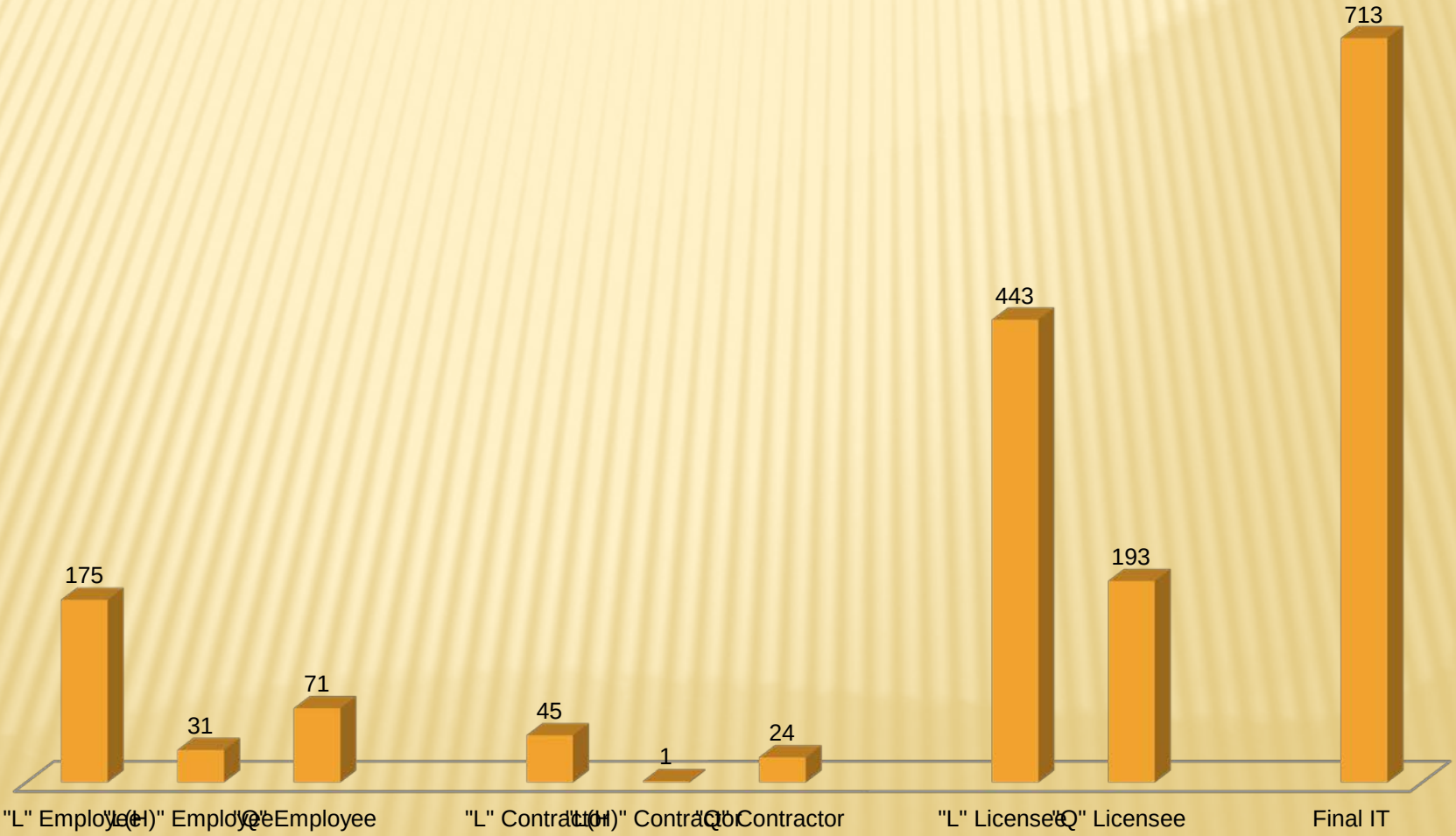
- 4,529 Federal employees
- 813 Contractors
- 4,505 Licensees

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

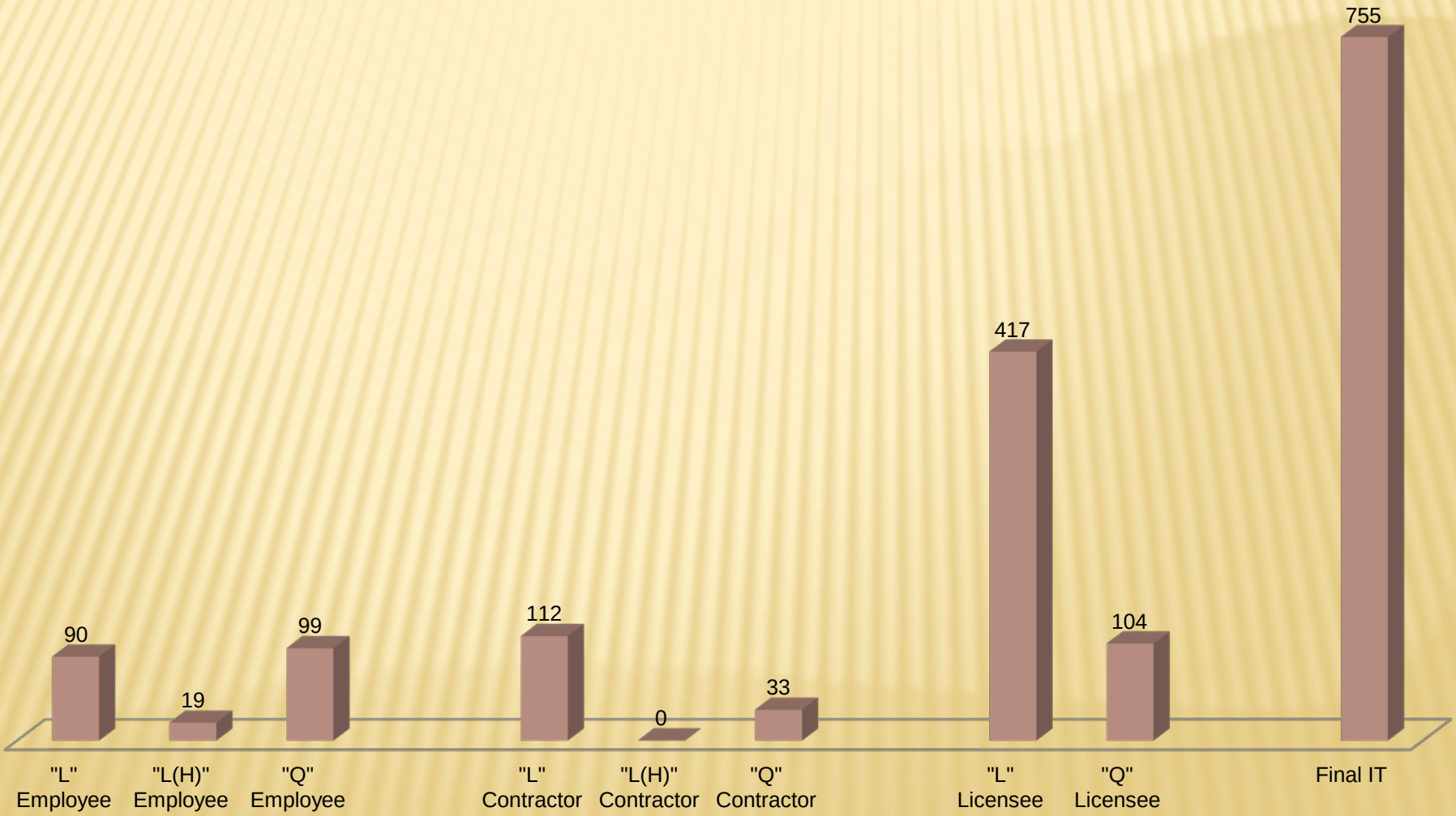
CLEARANCES/ACCESS GRANTED IN FY2010



CLEARANCES/ACCESS GRANTED IN FY2011



CLEARANCES/ACCESS GRANTED IN FY2012



Background Slides

APPLICABLE AUTHORITIES

•Executive Order 12968, as amended, “Access to Classified Information and Background Investigations Standards” (Employees, Contractors, Licensees)

•10 CFR Part 10, “Criteria and Procedures for Determining Eligibility for Access to Restricted Data or National Security Information or an Employment Clearance” (Employees, Contractors, Licensees)

•NRC Management Directive 12.3, “Personnel Security Program”

•10 CFR Part 11 , “Criteria and Procedures for Determining Eligibility for Access to or Control Over Special Nuclear Material” (Licensees)

•10 CFR Part 25, “Access Authorization” (Licensees)

CONTACTS OR QUESTIONS

Valerie Kerben, Branch Chief, (301) 492-3527
Valerie.Kerben@nrc.gov

Emily Robbins, Sr. Personnel Security Specialist, (301) 492-3524
Emily.Robbins@nrc.gov

Chris Heilig, Sr. Personnel Security Specialist, (301) 492-3544
Christoph.Heilig@nrc.gov

SECURITY CLEARANCES & ACCESS

- NRC “Q” clearance permits access with a need-to-know up to Top Secret and Restricted Data.
- NRC “L(H)” clearance permits access with a need-to-know up to Secret National Security Information and Confidential Restricted Data.
  - High Public Trust as Resident Inspectors.
- NRC “L” clearance permits access with a need-to-know up to Secret National Security Information and Confidential Restricted Data.
- NRC IT Access permits access to the NRC Local Area Network (LAN) and NRC facilities.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

TYPES OF CLEARANCES & INVESTIGATIONS

Security Clearances/ Access Types	Investigation Required
Q - Top Secret (TS)	Office of Personnel Management (OPM) Single-Scope Background Investigation (SSBI) with SSBI-Periodic Reinvestigation (SSBI-PR) every 5 years
L- High Public Trust (L(H)) (Secret)	OPM SSBI, with NACLC every 5 years
L - Secret (S)	Access National Agency Check with Inquiry (ANACI) and National Agency Check with law and credit (NACLC) for reinvestigations every 10 years
IT Level I Access	MBI, with NACLC reinvestigations every 10 years
IT Level II Access	NACLC with NACLC reinvestigations every 10 years
Atomic Energy Act, Section 145b, pre-appointment investigation waiver	SF-86 reviewed and FBI, credit, employment references, and education checks conducted

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Attachment 10- ODAA C&A Presentation

NISPPAC C&A Working Group Update for the Committee

February 2013

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

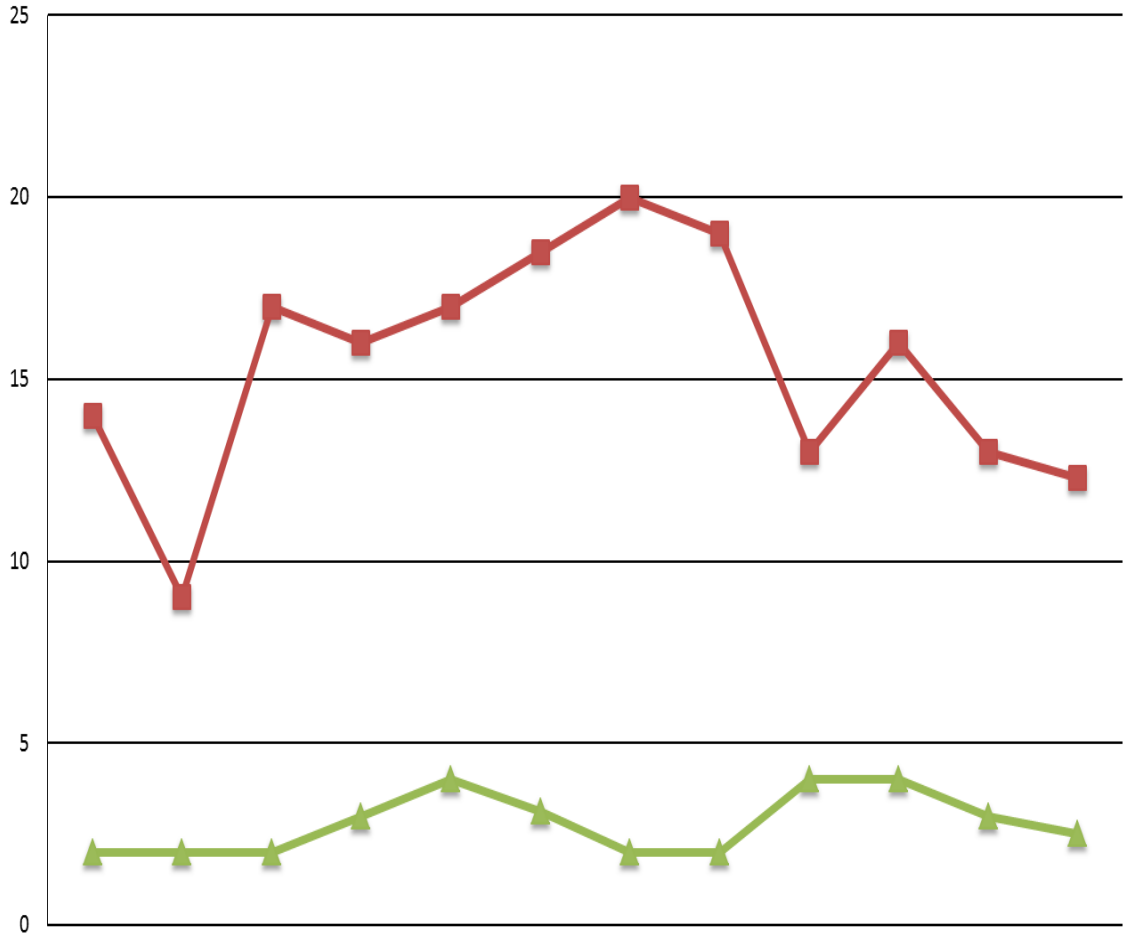
Certification & Accreditation

- 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.

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

Security Plan Review Results from Feb 2012- Jan 2013



	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12	Jan-13
Total IATOs	240	233	221	140	183	179	178	193	156	145	143	153
Time from DSS Receipt of plans to Granting of IATOs	14	9	17	16	17	18	20	19	13	16	13	12
Industry Response Time to DSS Questions, Comments	2	2	2	3	4	3	2	2	4	4	3	3
# Second IATOs	4	13	9	5	10	5	11	11	14	14	15	6

4227 SSPs Reviewed

2164 IATOs Issued

Avg. 15 Days to Issue IATOs

1621 SATOs Processed

16 Days to Issue SATO

1008 of the SSPs (24%) required some level of correction

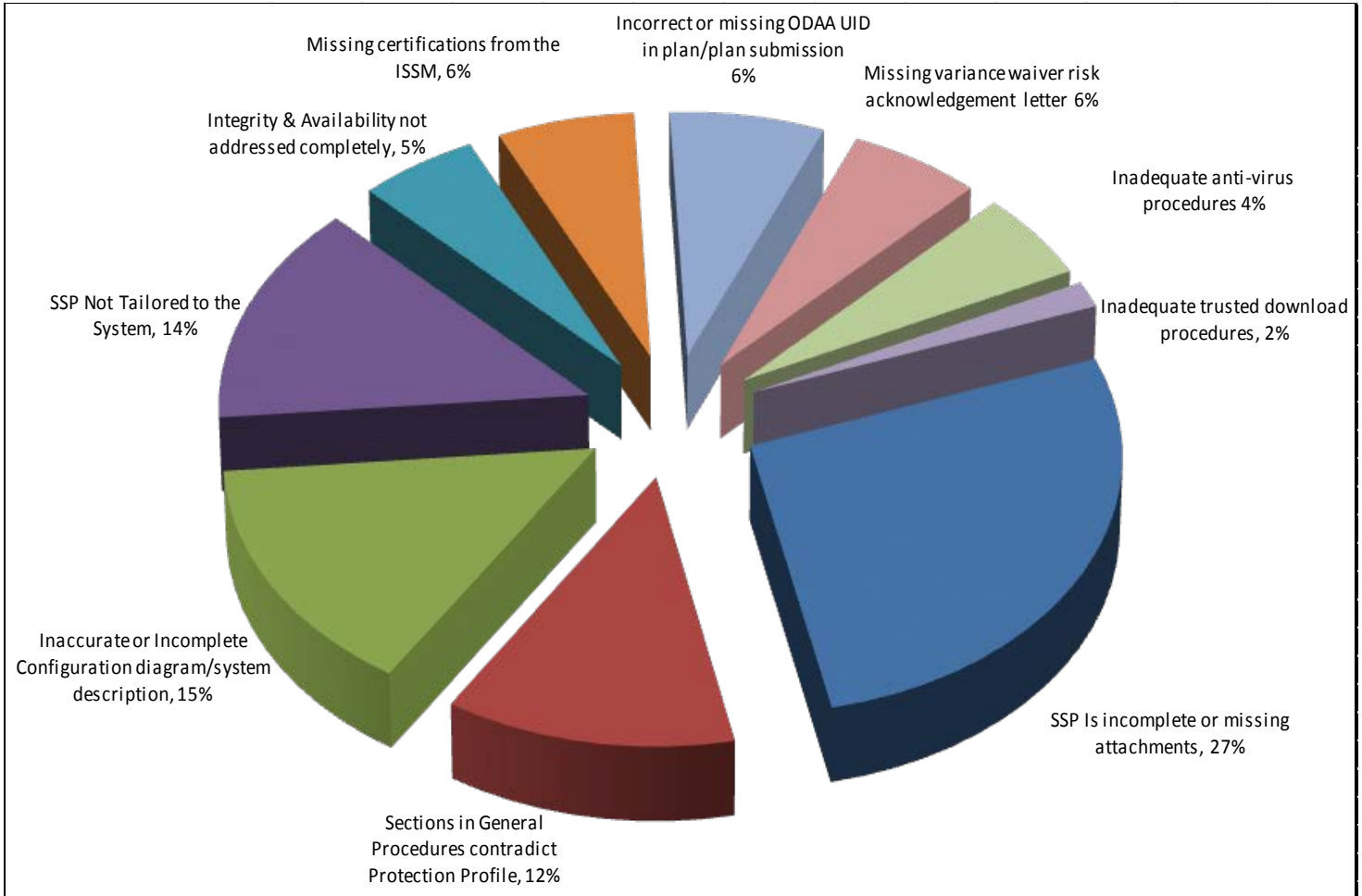
- 652 of the SSPs (15%) were granted IATO with corrections required

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

- 323 of the SSPs (8%) were reviewed and denied IATO (resubmitted after corrections)

- 119 of the SSPs (3%) were not submitted in accordance with requirements and were rejected. (resubmitted after corrections)

Common Deficiencies in Security Plans from Feb 2012- Jan 2013

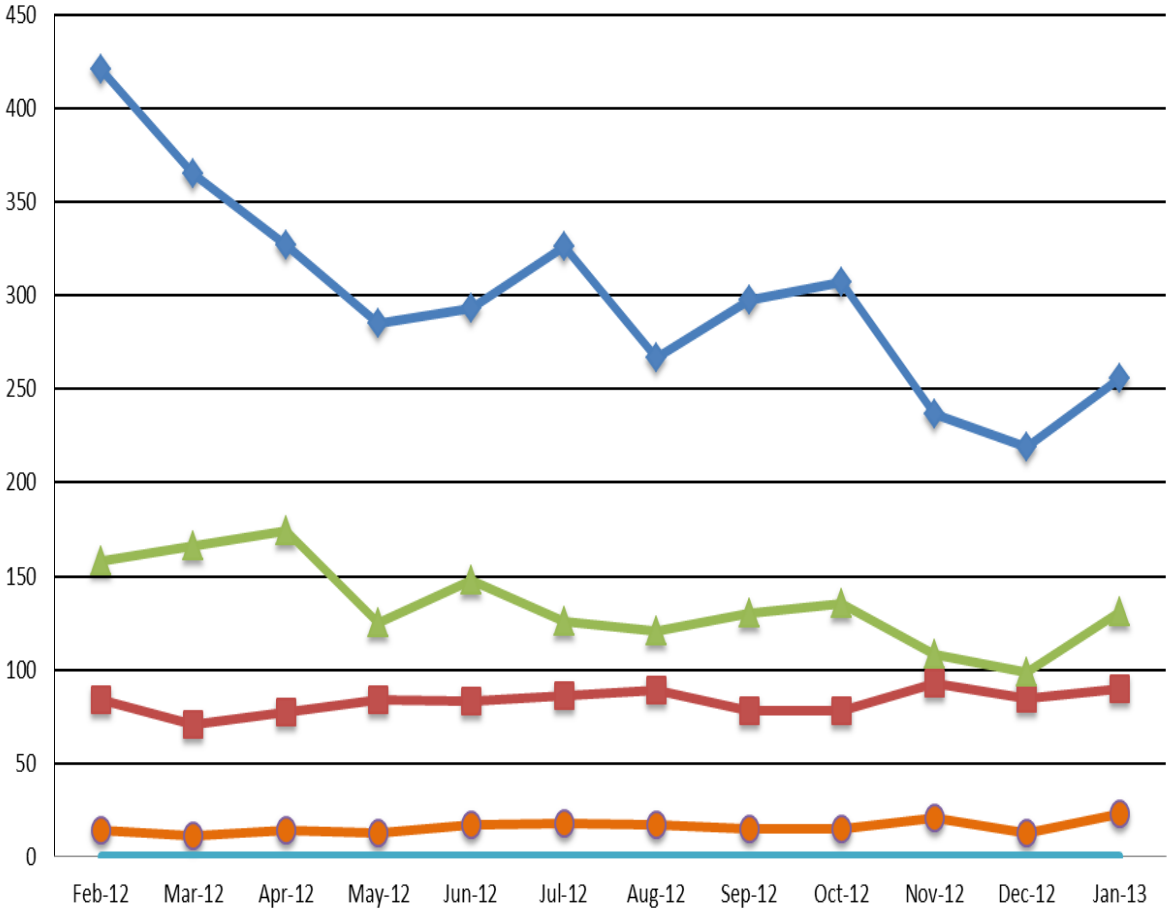


	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12	Jan-13
# Deficiencies	247	196	196	192	175	194	162	224	172	147	88	163
# Plans w/ Deficiencies	114	100	102	96	83	102	79	104	82	82	52	94
# Plans Reviewed	435	425	442	300	360	339	330	365	315	277	262	330
Avg Deficiency per Plan	0.57	0.46	0.44	0.64	0.49	0.57	0.49	0.61	0.55	0.53	0.34	0.49
Denials	37	26	47	34	24	25	25	34	19	9	15	28
Rejections	22	8	7	11	5	9	6	8	5	15	5	18

Top 10 Deficiencies

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

On Site Review Results from Feb 2012- Jan 2013



	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12	Jan-13
Total ATOs	421	365	327	285	293	326	267	298	307	237	219	256
Avg Days to Reg ATO	84	71	77	84	83	86	89	78	78	93	85	90
Total SATOs	158	166	174	125	148	126	121	130	135	108	99	131
Avg Days to SATO	14	11	14	13	17	18	17	15	15	21	13	23
% SATO's	38%	45%	53%	44%	51%	39%	45%	44%	44%	46%	45%	51%

During the Past 12 Months:

3601 ATOs

Avg 83 Days from IATO to ATO

1621 SATOs

Avg 16 days for SATOs

45% of all ATOs were SATO

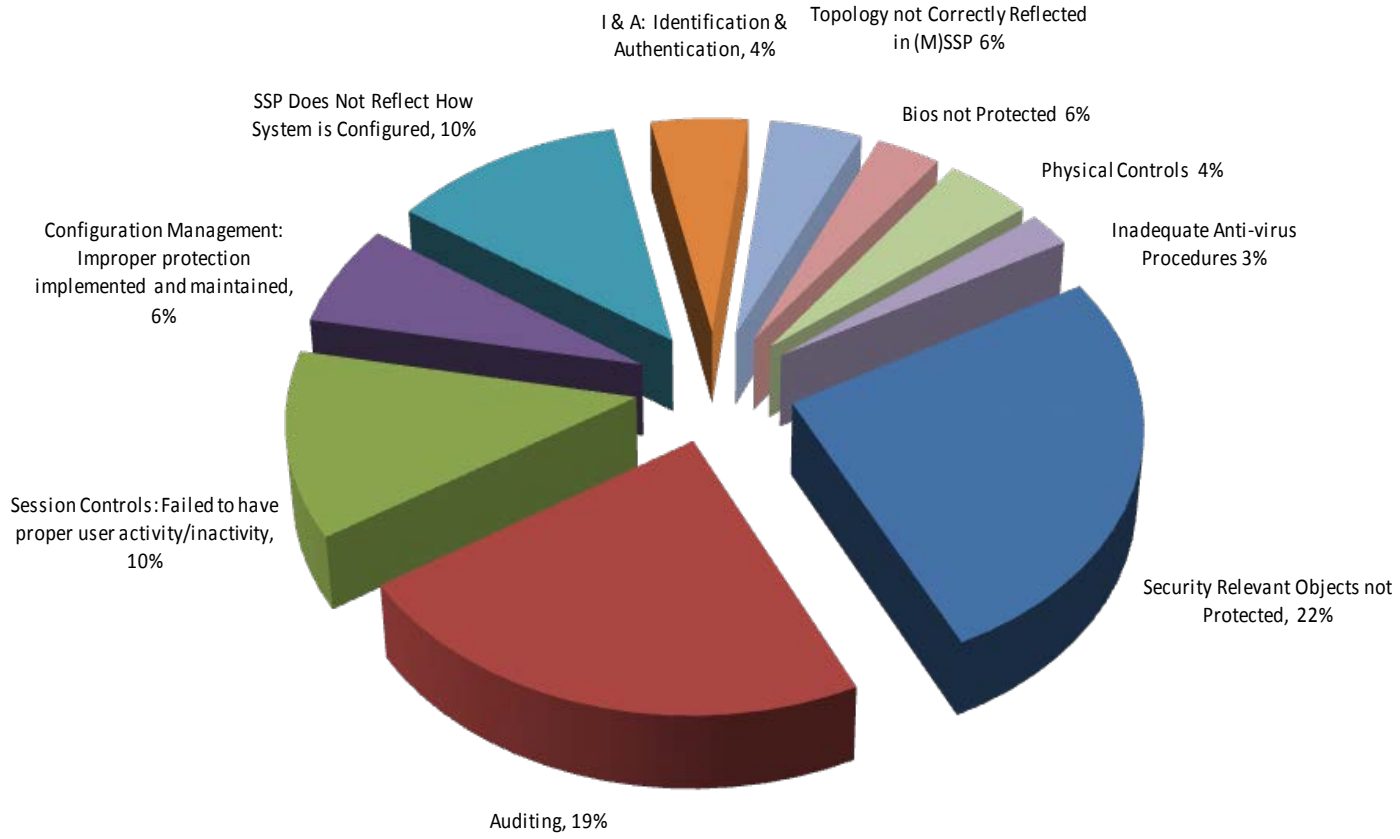
3481 ATO System Validations

- 2662 systems (76%) had no vulnerabilities identified.

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

- 56 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 Feb 2012- Jan 2013



	Feb-12	Mar-12	Apr-12	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12	Jan-13
# Vulnerabilities	163	166	119	94	124	94	96	95	104	67	92	128
# Onsites w/ vulnerabilities	78	67	71	62	73	68	51	63	62	45	59	78
# Onsites	427	372	315	278	284	305	256	286	285	219	207	247
Avg Vulnerability per Onsite	0.38	0.45	0.38	0.34	0.44	0.31	0.38	0.33	0.36	0.31	0.44	0.52

Top 10 Vulnerabilities

1. Security Relevant Objects not protected.
2. Inadequate auditing controls
3. Improper session controls: Failure to have proper user activity/inactivity, logon, system attempts enabled.
4. SSP does not reflect how the system is configured
5. Inadequate configuration management
6. Bios not protected
7. Topology not correctly reflected in (M)SSP
8. Identification & authentication controls
9. Physical security controls
10. Inadequate Anti-virus procedures

Summary and Takeaways:

- Security Plans are Being Processed and Reviewed in a Timely Manner
  - Most Common Deficiencies in SSPs Include Missing Attachments, Documentation Errors, Integrity and Availability Requirements
  - Need More Emphasis on Reducing Deficiencies
- Onsite Validations are Being Completed in a Timely Manner
  - Most Common Vulnerabilities Identified During System Validation Include Auditing Controls, Configuration Management, Not Protecting Security Relevant Objects
- More Straight to ATO (Where Practical) to Reduce Risk and Increase Efficiency
- Expect to see impact from DSS' Command Cyber Readiness Inspection (CCRI) Mission workload
- OBMS update

Questions?