NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

SUMMARY MINUTES OF THE MEETING

The NISPPAC held its 45th meeting on Wednesday, July 17, 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 August 21, 2013.

I. Welcome and Administrative Matters

Mr. Fitzpatrick welcomed the attendees, and after introductions, reminded everyone that NISPPAC meetings are recorded events. He acknowledged the service of Fred Riccardi and Shawn Daley, industry members whose terms expire on September 30th of this year, and presented each with Certificates of Appreciation for their service to the Committee, and a book about the National Archives building. He requested that Greg Pannoni, the NISPPAC Designated Federal Official (DFO), and Mr. Riccardi proceed with the process to select two new industry representatives. He then asked the DFO to review old business, to include a summary of the proposed changes to the NISPPAC bylaws and charter as required by the Federal Advisory Committee Act. (See Attachment 1 for a list of members and guests in attendance.)

II. Old Business

Mr. Pannoni reviewed the changes to the NISPPAC bylaws and charter that must be approved so the Committee's biennial renewal requirement can be completed by October 1, 2013. He noted the substantive changes as, (1) the provision for NISPPAC government representatives to provide annual financial disclosure information to the NARA Office of the General Council, (2) a certification from NISPPAC industry representatives that they are not registered lobbyists, and (3) a change updating the annual costs of NISPPAC activities. The Chair then asked for any further questions and/or comments relative to these requirements, and hearing none, received a unanimous vote of acceptance of the changes.

Mr. Pannoni then reviewed the action items from the March 20, 2013 meeting. He noted that the first item required ISOO to facilitate and monitor activities related to the update and automation of the Department of Defense (DoD) Form 254, and commented that the goal is to have an automated process in place by the end of this year. Further, he reported that the Personnel Security Clearance Working Group (PCLWG) had several actions, including a review of measures to lessen the impact of delayed periodic reinvestigations (PRs) on the overall timeliness of industry clearance submissions, investigations, and adjudications; tracking the overall performance timeliness for industry investigations using the Intelligence Reform and Terrorism Prevention Act (IRTPA) reporting criteria; and utilizing standardized performance metrics criteria developed by the Office of the Director of National Intelligence's (ODNI) Security Executive Agent (SEA) in their presentations to the Committee. (Action items for this meeting are provided at Attachment 2.)

III. Reports

(A) DoD Update

Valerie Heil, Office of the Under Secretary of Defense for Intelligence (OUSD(I)), informed the Committee that in June 2013, the National Defense Industrial Association hosted a meeting to discuss proposed changes to the National Industrial Security Program Operating Manual (NISPOM) on insider threat and implementation of section 941 of the fiscal year (FY) 2013 National Defense Authorization Act. She noted that based on recommendations from that meeting, the National Security Staff (NSS) concurred that a second conforming change to the NISPOM was needed, which would incorporate both the minimum standards for insider threat and the cyber intrusion reporting requirements. Furthermore, she reported that DoD is working its' internal processes to proceed with the development of this change and that they would coordinate with the other Cognizant Security Authorities (CSA) as well as ISOO and the NISPPAC for their review and concurrence.

(B) Defense Security Service (DSS) Update

Stan Sims, DSS Director, reported that both the government and industry stakeholder's meetings engaged in productive discussions regarding the recently reported unauthorized disclosures, and the challenges faced in light of the Snowden event. He noted that important progress was being made towards informing and educating each other on information pertinent to perceived or actual systemic threats. In addition, he noted that industry stakeholders continued to discuss military base access issues, as well as the December 2013 deadline for total electronic fingerprint submissions. He recommended that industry stakeholders who have not yet transitioned to electronic fingerprint submissions should visit the DSS website to view the five methods from which they might choose the solution that best fits their needs. He commented that the timeline for ongoing efforts at automating the DD Form 254 may have to be extended into next year, due to budget constraints. However, the requirements generation process is proceeding, and DSS has received excellent inputs from all involved.

Concerning Top Secret (TS) PRs for industry, he noted most were suspended on the 14th of June 2013, but the high risk TS PRs, such as those linked to Sensitive Compartmented Information (SCI) programs or those which are a part of the personnel reliability program, continue to be processed. He assured the Committee that DSS is working with Facility Security Officers (FSO) to ensure that these requirements are being validated as they are submitted, and that no one is incurring unnecessary risk. Finally, he reiterated that DSS understands the negative effects on the industrial security program that furloughs have caused, but reminded everyone that although some program delays are unavoidable, ultimately all will be accomplished.

(C) Combined Industry Presentation (See Attachment 3)

Mr. Riccardi, Industry Spokesperson, began by recognizing Leonard Moss as the new president of the National Classification Management Society (NCMS). He then updated the NISPPAC on industry efforts to meet the requirements of Executive Order (E.O.) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." He postulated that one must view insider threat hand-in-hand with counterintelligence measures, personnel security issues, and safeguarding initiatives, regardless of any chosen risk analysis equation, and by so doing, we can construct the appropriate workforce training and awareness programs. He also noted that this newest insider threat

training requirement for security professionals would only require about one and one half hours, and that industry is looking forward to working with the Center for Development of Security Excellence to leverage our programs and best practices.

Next, he expressed industry's appreciation to the Executive Agent (EA) for Controlled Unclassified Information (CUI) for the progress made to date on the establishment of standards for protecting unclassified but sensitive information, and voiced enthusiasm for future meetings on this subject. However, he cautioned against the premature issuance of Requests for Proposals that specify CUI requirements, and explained that industry cannot afford to make hasty and possibly inflated investment commitments without the official sanction of the EA for CUI. He agreed that the recent DSS stakeholder's meeting resulted in a good understanding of the need for greater emphasis on network security, information technology (IT) incident reporting, and the sharing of threats and vulnerabilities within the Defense Industrial Base. However, he reiterated industry's ongoing desire that we establish single standards and avoid a piecemeal approach in the deployment of new IT systems. In addition, he noted that while we are fully aware that budgets will continue to shrink, industry welcomes any interactions that define the consequences of change and how we may best implement those changes to reach the desired objectives.

Mr. Riccardi spoke to some of industry's personnel security concerns, and of the ongoing efforts of the Intelligence and National Security Alliance. He explained how they are studying the probable impacts on the suspension of PRs, and noted how this initiative could result in some form of an enhanced program or initiative that describes risk resulting from the lack of investigations, regardless of the timeline. He then reiterated industry's emphasis on the imperative for reciprocity, in that without renewed clearances an employee will be unable to move to another task when their clearance investigation is beyond the five-year mark. He reminded the Committee that some of these investigations are not conducted through DoD and therefore some companies face burdens they cannot contractually mitigate. He expressed concerns with the lack of consistency in the RAPIDGate program, and noted that as a result of recent consultations with key government personnel, industry will provide a white paper that summarizes the issues, findings, and concerns regarding resource utilization and the duplication of processes. He noted that industry was on track with changes to the Office of Designated Approval Authority (ODAA) Process Manual, and submitted comments for inclusion into the revision. He acknowledged industry's satisfaction with the progress of the automation of the DD Form 254, and is pleased to participate in the requirements definition process and assist with product standardization. He recognized the efforts of the Special Access Program Working Group, and noted that the recently approved nomination process should result in better reciprocity, and that they look forward to its implementation. He concluded, noting that industry's goal is to leverage existing training and experience with new training requirements in as cost effective manner as possible.

(D) PCLWG Update Report (See Attachments 4 through 9)

Colleen Crowley, Office of Personnel Management (OPM), updated timeliness performance metrics for industry personnel clearance submissions, investigations, and adjudications (see Attachment 4). She explained that the working group continues to examine the implications to investigative and adjudicative performance in the context of workload shifts, specifically in light of the PR surge of the past year. She noted that the overall goals for all categories of

investigations and adjudications are being met. She explained that OPM has managed all performance examinations as a combined initiative, with the ODNI and can now measure and establish goals for each type of investigation. She described the TS portion as having reached an investigation inventory high point of 24,000 cases and continues to shrink, due to a shift in focus because of a limited fieldwork capacity. With regard to Secret and Confidential investigations, she noted the inventory continues to decrease, and achieve a timeliness that permits OPM to continue to improve effectiveness and approach. With regard to TS PRs, she stated that while the overall TS inventory decreased the TS PR inventory increased for the reasons already cited. Also, she reminded the Committee that every case that proceeds through the investigative pipeline automatically becomes an adjudication responsibility, and that all these numbers are reflective of an ongoing workload moving through that process. The Chair asked if the adjudicative time recorded in the Central Verification System reflected only the end-to-end efficiency of completed cases. Ms. Crowley confirmed that was the case, and reiterated that the pending workload on hand is indeed not being counted in these metrics and that we must measure the length of both investigative and adjudicative stages to calculate the overall timeliness of a case. The Chair encouraged the government partners in the NISPPAC to seek ways to report information that would help to improve the accuracy of the numbers noting that the best numbers ensure the best picture, which in turn helps us manage expectations among our industry partners and monitor accountability among our government partners.

Ned Fish, Director of the DoD Consolidation Facility (CAF) continued the PCLWG's report by providing industry adjudication metrics (See Attachment 5). He explained that, due to the large backlog of industrial cases, the CAF is in the process of blending the work of the adjudicators from the former Defense Industrial Security Clearance Office and the Defense Office of Hearings and Appeals (DOHA) into a single division. He noted that the goal is to have a significant reduction in the adjudication backlog over the next two years. He detailed that the backlog was caused in part by a disparity with how the workload was shared, and suggested that the problem would exist until we achieve a single case management system, which is planned for FY 2014. He stated that the size of the backlog since the last NISPPAC meeting has decreased by roughly 12.5%. He noted that the most immediate challenges were caused by fiscal constraints that caused the cessation of overtime, and from the affects of sequestration, which he estimated would stall any improvements in the elimination or reduction of the backlog. He commented that previous estimates that the backlog would be eliminated by May of 2014 are now unrealistic, and that based on current budget constraints, the complete elimination of the backlog will take approximately two years. He remarked that one of his challenges is meeting the IRTPA goal of no backlogs, so his top priority is to achieve a balance between continued reductions of the backlog while at the same time maintaining IRTPA mandates. He acknowledged that until that backlog is gone, there will be a higher IRTPA number than what has been seen in the past. In response to a comment from Rosalind Baybutt, industry, regarding whether DOHA cases were included in the case count, Mr. Fish confirmed that cases that are either at the Personnel Security Appeals Board or DOHA are not reflected in this report. J.C. Dodson, industry, asked if, due to the discrepancies between OPM's metrics and those of the CAF, there was any pressure to meet IRTPA expectations, and if the CAF has determined a need to acknowledge that some of the established guidelines may be exceeded. Ms. Crowley remarked that they've managed to make sure to have the correct emphasis on the work that has a legal mandate for timeliness, and that the automated part of the process was achievable under IRTPA, but to grow fieldwork capacity to get the leads that are required for a PR or for a Single

Scope Background Investigation (SSBI) takes time, resources, and money that isn't presently available. Mr. Dodson then asked if even with the initial investigations moving along the correct path, if we will reach a point where the backlog has increased to where the people who require clearances will not have them. In response, Mr. Fish noted that even with additional funds and their best efforts it will take one to two more years to get any new hires certified to adjudicate cases in accordance with DoD regulations. Further, he noted that the follow-up question depended on which report card is being referenced, because if it is industry only, then those pressures will be more evident, but if we look across the board at DoD as a whole, we don't suffer the same challenges. Mr. Dodson repeated his challenge that our community should set its expectations based on the data that's available and cautioned that there will be pressure points regardless, and opined that industry will lag behind the government agencies simply due to the way the process is structured. He commented that while we are hearing that the root cause of the problem is predominantly manpower and furlough related, another cause of the problem could actually be a more complex investigative process coupled with a much broader scope. Mr. Fish noted that the backlog did not occur overnight, but rather grew over a long period of time, and that although it is actually still growing by about 500 cases a month, the hemorrhaging has stopped and that steady progress is being made. The Chair repeated his desire that we always recognize the numbers that we have for what they are, and while we can speculate about what might happen, we want to come back here again in four months and see the numbers again as they really are, and for us to be cognizant of the fact that this particular part of this meeting is really intended to make sure that everybody has available all the data that any of us maintains so we share the same picture of what is going on. He noted that the attention on PRs will remain high, and that we have talked for a number of years in this forum about how to get our hands around those cases that should have been submitted, and that this is a problem that senior government officials continue to recognize as one that must be addressed.

Ms. Baybutt asked if any government colleagues were seeing any push from Congress on clearance reduction, that is, is there any concern that there are perhaps too many people holding clearances. The Chair responded that there is attention from at least two branches of government on what it means to have this many people with clearances, and how to reinvestigate that population in the most prudent way. He added there have been many discussions about procedural improvements that might be available and whether we are recording the numbers properly. In addition, the Chair explained that from the point of view of the NISP, ISOO represents industry's concerns at various forums, such as the Performance Accountability Council, and the White House steering committee and that he routinely calls for discussions to consider the concerns and interests of industry. Finally, he assured the Committee that ISOO will continue to speak up wherever there is something substantive being discussed on this issue, and whenever some decision is forthcoming we will be there to put it on the record for everybody involved in the NISPPAC. Joseph Mahaley, National Aeronautics and Space Administration (NASA), asked in view of the present climate wherein we have suspended most TS PRs, was he to waive the in-scope requirement in order to keep these clearances active, and if this was indeed government policy, and if all agencies are going to follow this formula so that contractors will be able to continue to complete their work.. Mr. Pannoni explained that such a decision is an acceptable posture so long it remains under NASA's control, and that this condition is especially important for the contracted community, where there are multiple contracts involving multiple government agencies. Teresa Nankivill, ODNI, responded that

under current policy, investigations are to be conducted between the five- and seven-year marks, and that an agency has the discretion to reciprocally accept this posture. Further, she explained that beyond the seven-year mark there is still some discretion, but that at that point it has really become a risk management decision. She noted that both Intelligence Community Policy Guidance (ICPG) 704.2 and 704.4 offer this guidance. Shawn Daley, industry, asked if insider threat considerations were in any way a part of the clearance adjudication process, whether at the initial or PR level. Mr. Fish responded that while insider threat is always a concern, that for the sake of the requirements inherent in this process, it is not a part of this specific initiative.

Laura Hickman, DSS Personnel Security Management Office (PSMO) continued the report, reminding 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 causes for rejection (see Attachment 6). She noted that the submission of e-QIP continues to improve in quality, and that the goal of achieving a combined rejection rate of no more than 5% by the end of 2013 is possible. She noted the number one cause for rejection at PSMO continues to be missing employment information, and that the number one cause of rejects from OPM continues to be the missing fingerprint cards. She reminded the Committee that failure to meet the 14-day deadline will automatically cause OPM to reject the e-QIP back to PSMO. She cautioned that these rejects come back to PSMO via mail, and it can take up to two-weeks to notify the submitter of a case rejection. She noted that the second most frequent cause for rejection is when certification and release forms, which include fingerprint cards, have not been properly signed or submitted. She stated that the number of electronic fingerprint submissions rose to 28% as of the end of May, and reminded the Committee that all companies, contractors, and subcontractors who might need assistance in meeting the December 2013 requirement for electronic fingerprint submission, should contact the PSMO for assistance. With regard to the impact of sequestration and the resulting furlough on e-Qip submission, she noted that the PSMO expects only a modest increase in required processing time of perhaps one day per week over the furlough period. Mr. Sims acknowledged that the percentage of electronic fingerprint submissions was increasing, but cautioned that the rate is still well below the 100% requirement, with just over five months for all to comply. Tony Ingenito, industry, asked if the CAGE Code, which does appear on the Standard Form 86, might suffice as the missing employment information, thus substantially reducing the e-Qip rejection rate. Ms. Hickman acknowledged that the PSMO has submitted some applications to OPM without the current employment information, and that we are tracking those through the system to see what issues, if any, impact OPM's process. Mr. Ingenito then inquired, regarding electronic fingerprint submission, if it was possible to identify which class of facilities is having the most difficulties complying with this requirement, and suggested that the Committee might develop a marketing strategy to address compliance across all facility categories. Ms. Hickman replied that every known strategy has and is being offered, but should anyone think of another the government would be pleased to entertain it.

Ms. Nankivill, ODNI continued the working group report by presenting the performance metrics for the intelligence community (IC) (see Attachment 7). She described the SEA as being responsible for the oversight of investigations and the eligibility determinations for access to classified information made by any agency, as well as for developing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of national security investigations and adjudications. She reviewed the timeliness goals set for completing

each phase of the clearance process and noted they are the same for all agencies, and noted that anything that occurs prior to submission, or post adjudication or due process, is not included in the end-to-end measurements. She reminded the Committee that the working group's objective was to measure government performance on industry cases, and that while 95% of all their investigations are conducted by OPM, about five percent of the investigations and adjudications are conducted for the IC, with less than one percent of those conducted by one of the designated Investigative Service Providers (ISP). Regarding performance metrics, Ms. Nankivell reported that the timeliness for both initial TS and S investigations decreased from 58 to 55 days and from 129 to 119 respectively, while PRs experienced an increase from 194 to 208 days, thus exceeding the IRTPA goal by 13 days. She noted that the figures included in the PR backlog, which the Chair had asked be added to the overall metrics picture, include investigations that have already been submitted and investigated, and are in the process of being adjudicated. She explained that these are actually out-of-scope reinvestigations, or those representing TS/SCI individuals who already have a SSBI and that may be due for a PR. She reminded the Committee that industry cases constitute almost half of all TS-SCI clearances, and that the data represents all the IC and DoD community. The Chair suggested that a helpful measurement would be to know how many of these cases have been submitted and whether the responsible official knows how many pending cases are in the pipeline. Ms. Nankivill responded that while Scattered Castles is not a case management system, the Joint Personnel Adjudication System (JPAS) is and could satisfy such needs. Mr. Sims reminded the Committee that last year, to address budgetary constraints and to achieve greater speed, DSS changed the requirement for 180-day submission to 90 days, and further reduced it to 30 days, so as not to eliminate them, but push them out to FY 2014. Mr. Riccardi added that some IC contractors are simply not being allowed to submit PRs, thus creating a situation where a company cannot move its personnel between programs, which put them at a competitive disadvantage, especially in teaming arrangements, when clearance investigations cannot exceed the five year mark. Ms. Nankivill clarified that there is no IC moratorium on industry PRs, and noted that some agencies, using a risk management approach, have identified high-risk populations that they continue to submit for PRs. The Chair clarified that there is no IC-wide policy prohibiting the submission of PRs and noted that there is increased attention on the status of people who have been submitted for a PR, and that this condition is being driven by the headlines. He thanked both the ODNI team and the PCLWG for working this issue and trying to accomplish whatever visibility can be achieved. He reiterated that the NISPPAC will continue to put the industry impact picture into the mix, and declared that in the future we must be able to propose sound alternative approaches. Ms. Nankivill commented that this all supports the larger picture of the continuous evaluation programs that are being explored, piloted, and developed, alongside the insider threat programs. Finally, she briefly summarized the IC performance data for industry, noting that initial Secret timelines increased by six days to 101, initial TS timelines decreased by 11 days to 123, and PR timelines increased by 16 days to 245, which is 50 days over the 195-day goal.

Mark Pekrul continued the PCLWG report with the performance metrics for the Department of Energy (DOE). He presented a review of DOE's personnel security posture (see Attachment 8) in which he reported that their cleared industry population, which as of June 1, 2013, was approximately 61,000 Q (TS equivalency) and approximately 23,000 L (S equivalency). He reported no substantive changes from the previous NISPPAC meeting, and reaffirmed that DOE's performance continues to remain within the IRTPA guidelines. With regard the L population, the September 2012 initial case timelines increased to 15 days, but subsequently

recovered and reached IRTPA mandates by April 2013. Finally, in terms of Q PRs, the agency is averaging 10-11day adjudication time, initials are significantly lower, and the agency has thus far not needed to suspend or otherwise delay its PR schedule.

Valerie Kerben continued the PCLWG report with a presentation of metrics from the Nuclear Regulatory Commission (NRC). She offered 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 reported that at present there are 877 contractors who work for NRC, approximately 800 of whom have been granted either the Q or L clearance. With regard to both Q and L investigations the agency continues to achieve better than acceptable timelines and their PRs remain well within the goal. She noted that NRC has a very robust prescreening process, and thus reviewing e-QIP products and other process elements prior to submitting them to OPM increases timeliness metrics on the front end, and that adjudications were presently stable. The Chair expressed appreciation for the excellent work of the PCLWG, as it continues to evolve to address our needs through a growing partnership, which is especially evident when we see all of the CSAs talking about their particular perspective, as well as the common ground, on the matter of security clearance processing. He noted that there are important distinctions from one community to another, and that one really does get an opportunity to admire the breadth of the NISP in terms of the CSA partnership that is necessary to effectively manage this clearance process. Finally, he recognized OPM's thorough contribution in providing the bulk of the production workload for the working group report.

(E) Certification & Accreditation Working Group (C&AWG) Report (See Attachment 10)

Tracy Brown, DSS, provided the C&AWG report and reminded the Committee that DSS is the primary government entity responsible for approving contractor information systems to process classified information, and that they work with industry partners to ensure that system security controls are in place to limit the risks of compromising national security information, and to ensure adherence to national industrial security standards. She explained that the working group's current initiatives included: the development of Windows 7 and 8 server baseline standards, defining how continuous monitoring concepts will ultimately be applied to security systems, and the updating of Industrial Security Field Operations (ISFO) process manual. She noted that the initial ISFO draft has already been submitted to our industry partners, and that their comments are in the process of being incorporated, and that the ODAA is currently reviewing the Security Content Automation Protocol in order to determine how it might be leveraged into their assessments process. She reviewed the results of metrics gathered from review of the 4,767 system security plans (SPP) submitted between May 2012 and April 2013. She noted that the average processing time required for issuing an Interim Authority to Operate (IATO) or a Straight to ATO (SATO) was 17 days, and that approximately 24% of plans contained errors that had to be addressed by industry. She indicated that the most common deficiency revealed during the desktop reviews remains incomplete or missing attachments, and that the second is the presence of incomplete configuration diagrams or system descriptions. With regard to on-site review metrics during the same 12-month cycle, she noted that the ODAA issued 3,173 ATOs, with 77% requiring no on-site system corrections, and that 22% required minor adjustments, followed by the issue of final accreditation once the corrections were made.

Ms. Brown reviewed the common vulnerabilities found during on-site visits, and noted that the discovery of unprotected security-relevant objects, inadequate security auditing controls, and improper session controls accounted for the bulk of the discrepancies. She noted that occasionally, a system's configuration documentation did not agree with what was actually found during the on-site review. She remarked that in the future the ODAA will issue SATOs wherever practical, and expects to begin assessing the impacts of our Cyber Command Readiness Inspection mission on our workload. She noted that the ODAA is also affected by sequestration and the furlough programs, and that they too expect to see some decreased timeliness and efficiency. Finally, she reminded the Committee that the ODAA is still in the process of building its Office Business Management System which will be online some time in FY 2014. She explained that its objective is to streamline and automate C&A processing, as well as to track the details in each step of the accreditation life cycle. The Chair applauded the C&AWG's accreditation metrics standardization efforts, as well as their focus on process and quality control issues that accurately illustrate inputs, outputs, and timeline improvements.

(F) E.O. 13587 Update (See Attachment 11)

The Chair then provided a brief overview of the Classified Information Sharing and Safeguarding Office (CISSO), which was created as part of E.O. 13587. He explained that CISSO is housed within the ODNI's Program Manager for the Information Sharing Environment (PM-ISE), and supports the Senior Information Sharing and Safeguarding Steering Committee (SISSSC), a White House steering committee established in the post WikiLeaks environment. He introduced Ray Sexton, Chief of the Management and Oversight Division of the PM-ISE to provide an update on the implementation of E.O. 13587. Mr. Saxon described his present duties as providing support for both the SISSSC and the Information Sharing and Access Interagency Policy Committee (ISAIPC), which are White House level senior policy bodies presently engaged in dealing with the recent incidences of unauthorized disclosure, making this a timely opportunity to update the Committee on the progress related to the E.O. 13587 elements. He explained that the E.O. was issued shortly after WikiLeaks, and that there were a number of structures and processes created as a result of some of the lessons learned and issues identified. He noted that the ISAIPC identified five priority areas that required immediate attention which were then converted from conditions of operations to inclusion into the programmatic and implementation guidance in the budget cycle. He stated that definitions of both for Initial Operational Capacity (IOC) and Full Operational Capacity (FOC) were forged for each of these five priorities and were followed by implementation timelines developed by the Office of Management and Budget. He explained that one of our most important goals was to ensure that the timelines fall within the scope of the present administration, and described the difficulty in assailing the kinds of activities that need to be accomplished, such as enhancing control of removable media, building a more robust insider threat program, and improving enterprise audit capabilities. He noted that the ISE is not just a federal problem, but also a state, local, tribal, private industry, and even international problem in both scope and complexity. He explained that while we are now just focusing on these issues as a completely federal-centric effort, we need to acknowledge that our industry partners must play a major role in effecting solutions. He stated that the immediate priority is to have the federal government identify the actual circumstances that led to this most recent unauthorized disclosure, and what federal-centric actions will be taken to correct it. He continued, adding that we must address the enormous number of personnel with clearances, the elimination of the backlog, as well as a more vigilant

selection of personnel approved for a clearance. He noted that the White House is fully aware that the focus can no longer be only federal-centric, and that our industrial partners will have to become an integral player in these discussions. The Chair responded that we are on track and making progress in the evolution of formal standards and guidance, such as that from the Committee on National Security Systems, or the National Insider Threat Task Force (NITTF), and how they are to be implemented through the NISPOM. He stated that he hoped to have a more definitive answer to industry's involvement in the on-going dialogue at our next NISPPAC meeting, and noted that industry has been involved in activities such as the previously mentioned NISPOM revisions, and the development of conforming change number two, which embrace the elements of these requirements, and are then filtered through the CSAs in the NISP structure. The Chair further noted that the NITTF has been instrumental in integrating insider threat guidelines into the NISP policy process. Mr. Sexton agreed that the implementation of insider threat initiatives is prominent in the policy arena and noted that as we examine the recent unauthorized disclosures of sensitive information, realizing that we have a long-established system for dealing with espionage, and that with the creation of E.O. 13587, we now have an improved mechanism to deal with leaks. He opined that while we still have more to learn, we understand that the central challenge is to devise a strategy that makes it as difficult as possible for those who would leak sensitive information to be able to do so, and also for us to gain enough knowledge to expeditiously recover whenever the inevitable leaks occur. He concluded by noting that one side of the equation must deal with becoming better at checking on people, that is, making sure they are reliable, tracking their performance, and creating all the right circumstances to prevent them from being able to leak; and the other side of the equation, which is driven by the NSS, is an historical examination of the totality of the event, that is, how did the individual find the cracks in the systems that enabled him to take advantage of systemic vulnerabilities, and what then are the actions that can be put in place to prevent duplication of those intrusions, and finally, what must be done afterwards to expedite damage control and minimize the volume of compromised information.

IV. Closing Remarks and Adjournment

The Chair reminded everyone that the next NISPPAC meeting is scheduled for November 14, 2013, and that it would be available in a virtual format. He noted that the first meeting in 2014, is tentatively planned for March 19, and that the second will be held in mid June in conjunction with the NCMS annual seminar. Mr. Pannoni reviewed the two action items that emerged from this meeting: (1) ISOO will work with NISPPAC industry representatives to ensure nominees for the 2013-2017 term are approved and in place at the November 2013 meeting, and (2). the PM-ISE will update the Committee on the status of E.O. 13587 implementation and its impact on industry. There being no further business, the meeting adjourned at 12:15 p.m.

Attachment #1- NISPPAC Attendees

Attachment 1

NISPPAC MEETING ATTENDEES/ABSENTEES

The following individuals were present at the July 17, 2013, NISPPAC meeting:

• John Fitzpatrick,	Information Security Oversight Office	Chairman
• Greg Pannoni,	Information Security Oversight Office	Designated Federal Officer
• Stan Sims	Defense Security Service	Member/Presenter
• Kim Baugher	Department of State	Member
• Ryan McCausland	Department of the Air Force	Member
• Dennis Hanratty	National Security Agency	Member
• Anna Harrison	Department of Justice	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/ MOU Representative	Member
• Drew Winneberger	Defense Security Service	Alternate
• Jeff Jones	Department of the Navy	Alternate
• Kesha Braxton,	Department of Commerce	Alternate
• Christal Fulton	Department of Homeland Security	Alternate
• Lisa Desmond	Department of the Army	Alternate
• Mark Pekrul	Department of Energy	Alternate/Presenter
• Valerie Heil	Department of Defense	Alternate/Presenter
• Valerie Kerben	Nuclear Regulatory Commission	Alternate/Presenter
• Kathleen Branch	Defense Security Service	Alternate
• George Ladner	Central Intelligence Agency	Alternate
• Kathy Healey	National Aeronautics & Space Administration	Alternate
• Neal Duckworth	Office of the Director of National Intelligence	Alternate
• Derrick Broussard	Department of the Navy	Alternate
• Colleen Crowley	Office of Personnel Management	Presenter
• Ned Fish	Department of Defense	Presenter
• Teresa Nankivill	Office of the Director of National Intelligence	Presenter
• Laura Hickman	Defense Security Service	Presenter
• Tracey Brown	Defense Security Service	Presenter
• Ray Sexton,	ODNI, PM-ISE.	Presenter
• Karen Duprey	MOU Representative	Attendee
• Mark Rush	MOU Representative	Attendee
• Kirk Poulsen	MOU Representative	Attendee
• Robert Harney	MOU Representative	Attendee
• Leonard Moss, Jr.	MOU Representative	Attendee
• James Shamess	MOU Representative	Attendee

• James O'Heron	Department of Defense	Attendee
• David Fries	Office of the Director of National Intelligence	Attendee
• Joseph Mahaley	National Aeronautics & Space Administration	Alternate
• Kathy Branch	Defense Security Service	Attendee
• John Haberkern	Defense Security Service	Attendee
• Andrea Jones	Department of State	Attendee
• Robert Orlosky	Central intelligence Agency	Attendee
• Kimberly Lew	Department of Homeland Security	Attendee
• Lisa Loss	Office of Personnel Management	Attendee
• Derrick Broussard	Department of Navy	Attendee
• Jay Buffington	Defense Security Service	Attendee
• Anthony Lougee	National Security Agency	Attendee
• Mitch Lawrence	Industry	Attendee
• William Davidson	Industry	Attendee
• Doug Hudson	Industry	Attendee
• Rhonda Peyton	Industry	Attendee
• Dennis Arriaga	Industry	Attendee
• Jim Euton	Industry	Attendee
• Tabetha Chandler	Industry	Attendee
• Debbie Young	Industry	Attendee
• Scott Conway	Industry	Attendee
• Kevin Stroop	Industry	Attendee
• Dorothy Rader	Industry	Attendee
• Marcus Carpenter	Industry	Attendee
• David Best	Information Security Oversight Office	Staff
• Robert Tringali	Information Security Oversight Office	Staff
• Joseph Taylor	Information Security Oversight Office	Staff

Attachment 2- NISPPAC Action Items

Attachment 2

Action Items - 7/17/2013 NISPPAC Meeting

1. ISOO will work with NISPPAC industry representatives to ensure nominees for the 2013-2017 term are approved and in place at the November 2013 meeting

2. The PM-ISE will update the Committee on the status of E.O. 13587 implementation and its impact on industry.

Attachment #3- Combined Industry Presentation

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

17 JULY 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
Roslind 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

National Industrial Security Program

Industry MOU Members

AIA	J.C. Dodson
ASIS	Jim Shamess
CSSWG	Mark Rush
ISWG	Karen Duprey
NCMS	Leonard Moss
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 and 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

Security Policy Update

Executive Order #13587

EO # 13587

Structural Reforms to improve security of classified networks

7 OCT 2011

Office of Management and Budget and National Security Staff - Co-Chairs

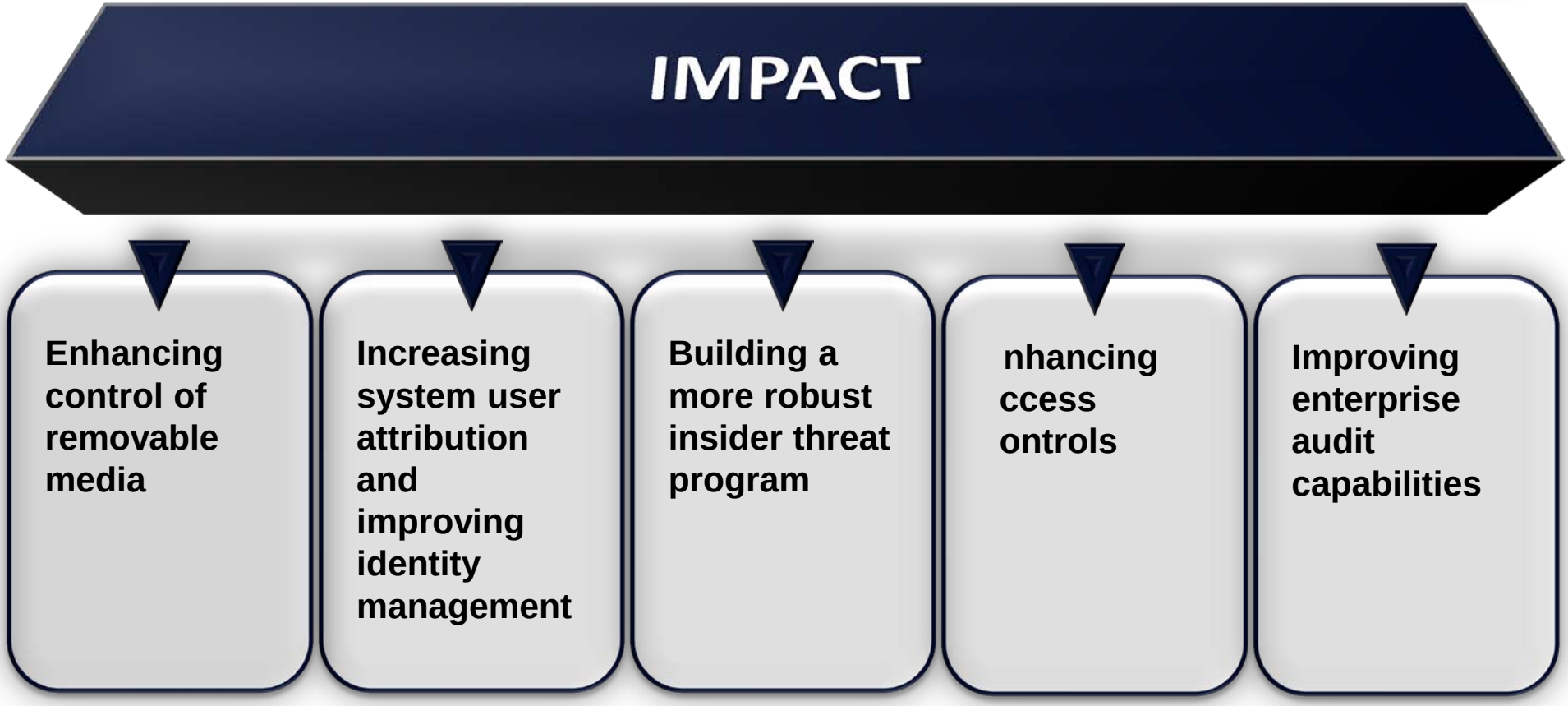
- Steering Committee comprised of Dept. of State, Defense, Justice, Energy, Homeland Security, Office of the Director of National Intelligence, Central Intelligence Agency, and the Information Security Oversight Office

INSIDER THREAT

- **Directing structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks**
- **Integrating Information Security, Personnel Security and System Security**
  - Internal and external threats and vulnerabilities
- **Developing policies and minimum standards for sharing classified information**
  - Primary focus on classified computer networks

Security Policy Update

Executive Order #13587 (cont.)



Security Policy Update

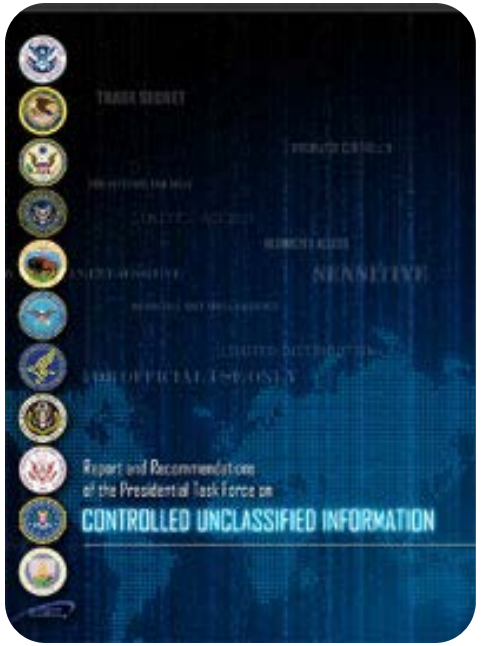
Executive Order #13556

EO # 13556

Controlled Unclassified Information (CUI)

4 NOV 2010

- **National Archives and Records Administration Executive Agent (NARA)**
- **Establish standards for protecting unclassified sensitive information**



- **Federal government Registry established**
  - 16 major categories and 70 sub-categories
- **Next Steps**
  - Develop marking, safeguarding, dissemination, IT Security policy
  - Standard definitions to be published by NARA via CUI registry

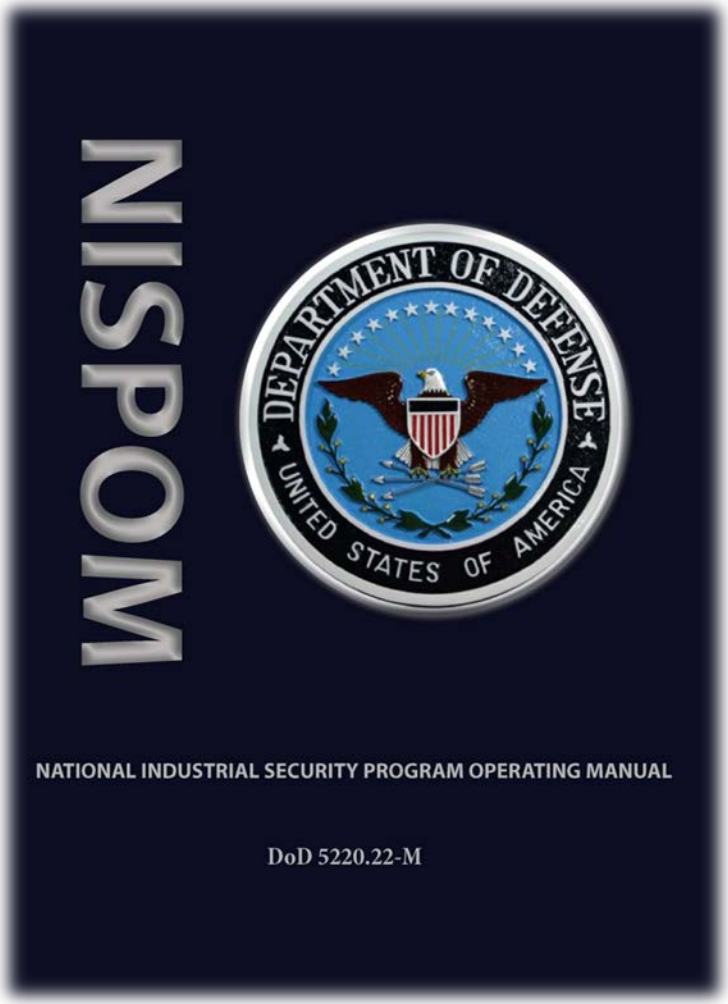
Security Policy Update

IT Security

- **Defense Federal Acquisition Regulation Supplement (DFARS) Unclassified IT Security**
  - Establishes security measures for IT across the Defense Industrial Base (DIB)
  - Greater emphasis on network security and IT incident reporting
  - Share threats and vulnerabilities throughout DIB
- **DoD established an IT Security Framework Agreement**
  - 30+ companies have signed on
  - Program expansion planned
- **IMPACT**
  - Other government agencies moving forward with imposing IT Security measures and requirements
    - Missile Defense Agency
    - Air Force
    - Defense Information Systems Agency (DISA)

Security Policy Update

Industrial Security Policy Modernization



- **National Industrial Security Program Operating Manual revision and update**
- **Department of Defense Special Access Program Manual development**
- **Industrial Security Regulation, Volume II update**
- **Special Access Program (SAP) Supplement being eliminated**
  - Planning to convert to an Appendix
- **IMPACT**
  - Some movement forward towards reassessing Special Access Program security requirements

National Industrial Security Program
Policy Advisory Committee Working Groups

- **Personnel Security**
  - Continued effects of Government Sequestration on clearance processing
    - Planning for transmission of TS PRs
  - Plans for DoD CAF to reduce significant backlog (both age and quantity) of industry adjudications
  - USN's RapidGate Program and Air Force Base access criteria challenges
- **Automated Information System Certification and Accreditation**
  - Industry reviewed and submitted comments for revised ODAA Process Manual Draft v6
  - Government policy change from 3-yr accreditation to continuous monitoring
    - Implementation in progress

National Industrial Security Program
Policy Advisory Committee Working Groups (cont.)

- **Ad-hoc**
  - NISPOM Rewrite Working Group
    - Government/Industry meeting to discuss Government response to industry comments on Conforming Change 2 to NISPOM
  - Potential DD254 revision
    - Industry attended DSS/Army Demo and participated in the requirements definition
- **ISOO sponsored Ad-hoc SAP Working Group**
  - Meetings continued in 2013
    - SAP draft volumes to be shared with NISP signatories and industry
  - Volume 2, Personnel Security on Dr. Vickers desk for approval
  - Other volumes expected to be published by end of FY13
  - New SAP Nomination Process Implementation Guidance signed by Dr. Vickers, USD(I) 20 May 2013
    - Implementation targeted for August/September
    - Expected to improve reciprocity

Additional Significant Activities

- **Controlled Unclassified Information**
  - Meeting with ISOO and CUI Executive Agent Team on 20 March 2013
  - Excellent exchange on Industry Implementation efficiency options
    - Comments to draft implementation submitted
- **Insider Threat**
  - Leverage collective experience and benchmark practices to
    - Support Government policy and tools development for successful operational implementation
    - Meet National Security Insider Threat objectives
      - Provide support to public policy development (e.g., NISPOM Conforming Change #2)
      - Liaison with MOUs, NISPPAC, other ASIS Councils, Government and Commercial Entities (e.g., financial, gaming, medical, and chemical) “Best Practices”

THANK YOU

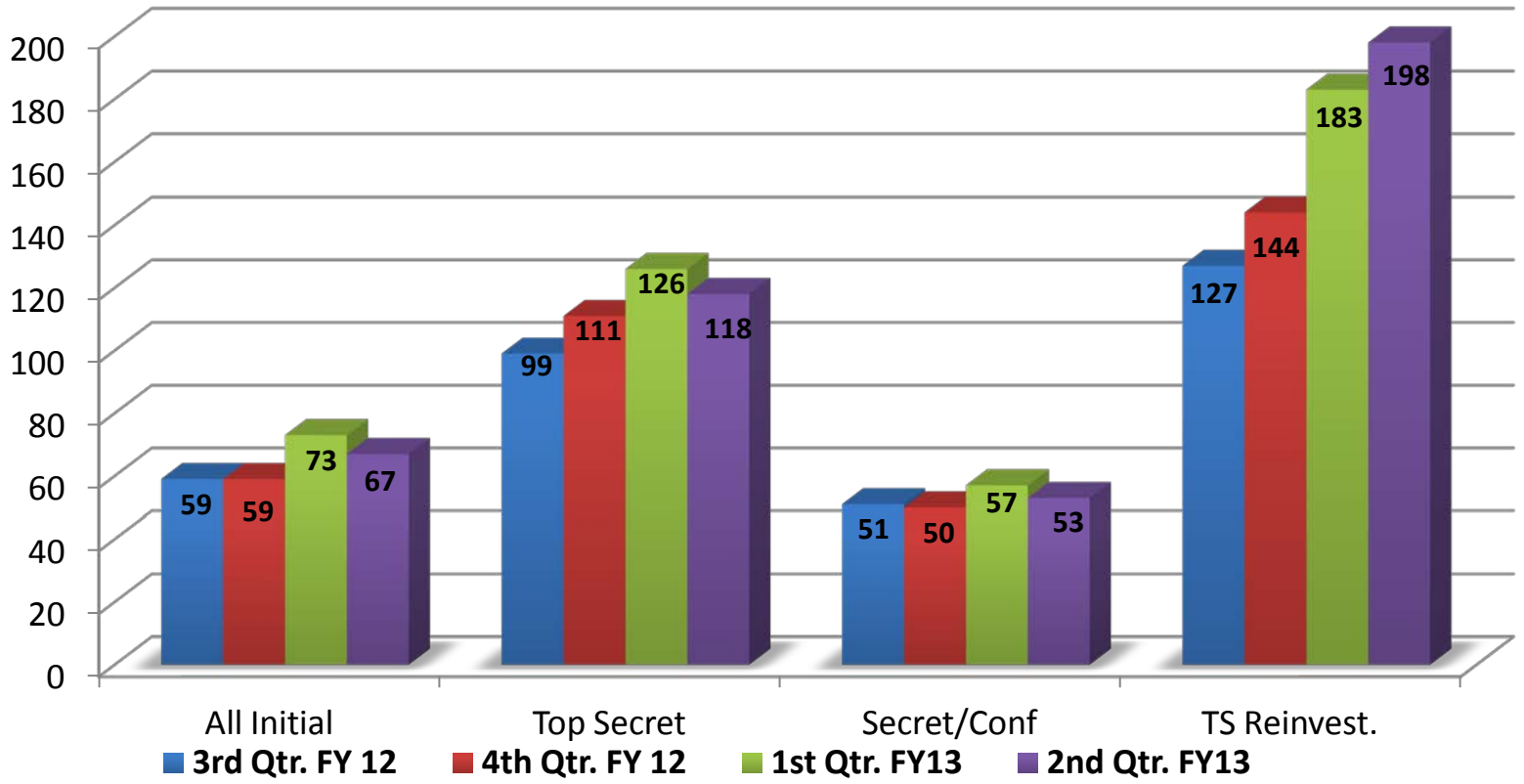
Attachment #4- OPM PCL Presentation

a New Day for Federal Service

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

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

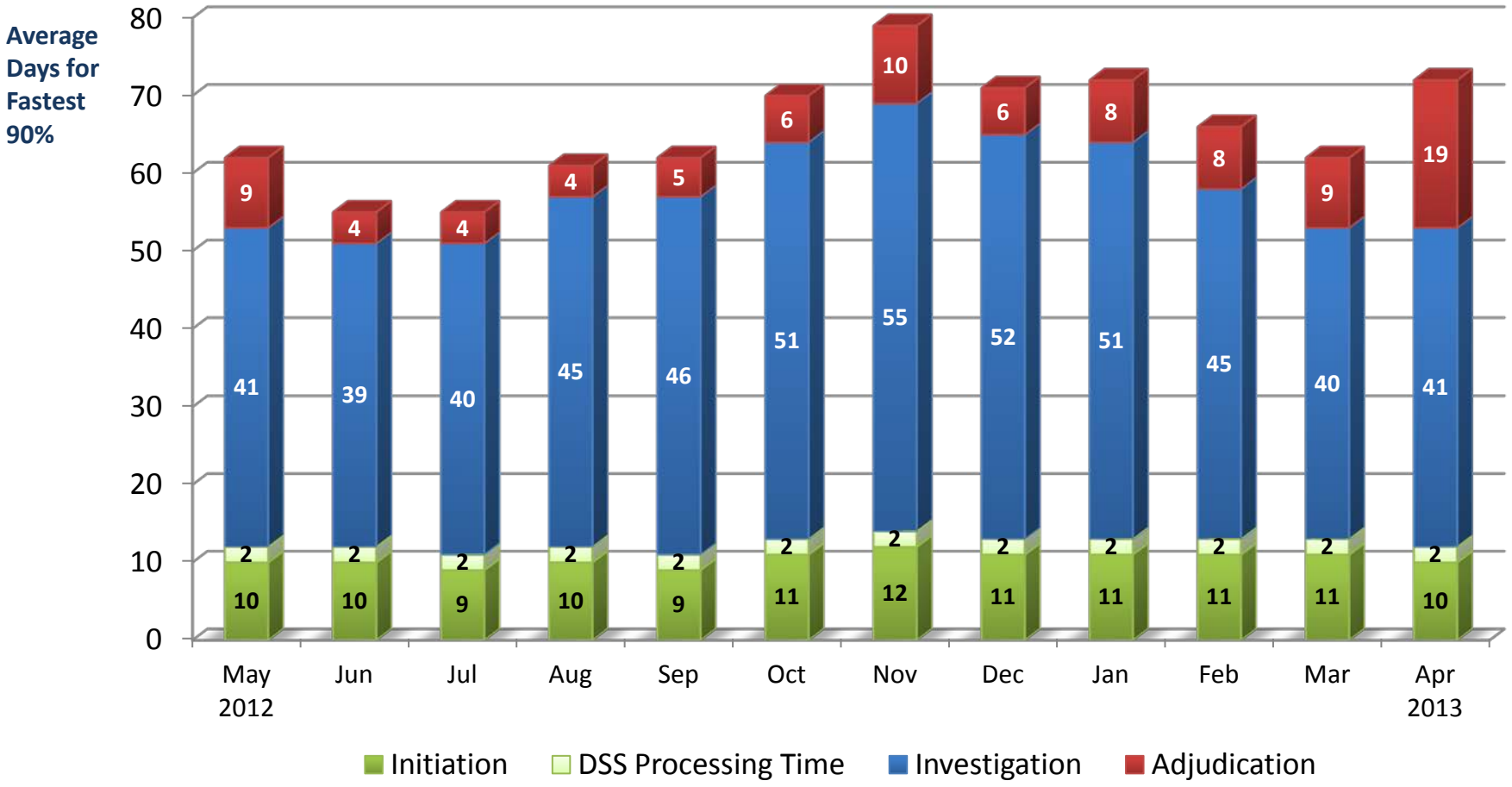
Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 3rd Q 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
Adjudication actions taken – 2nd Q FY13	26,136	5,782	20,354	8,655

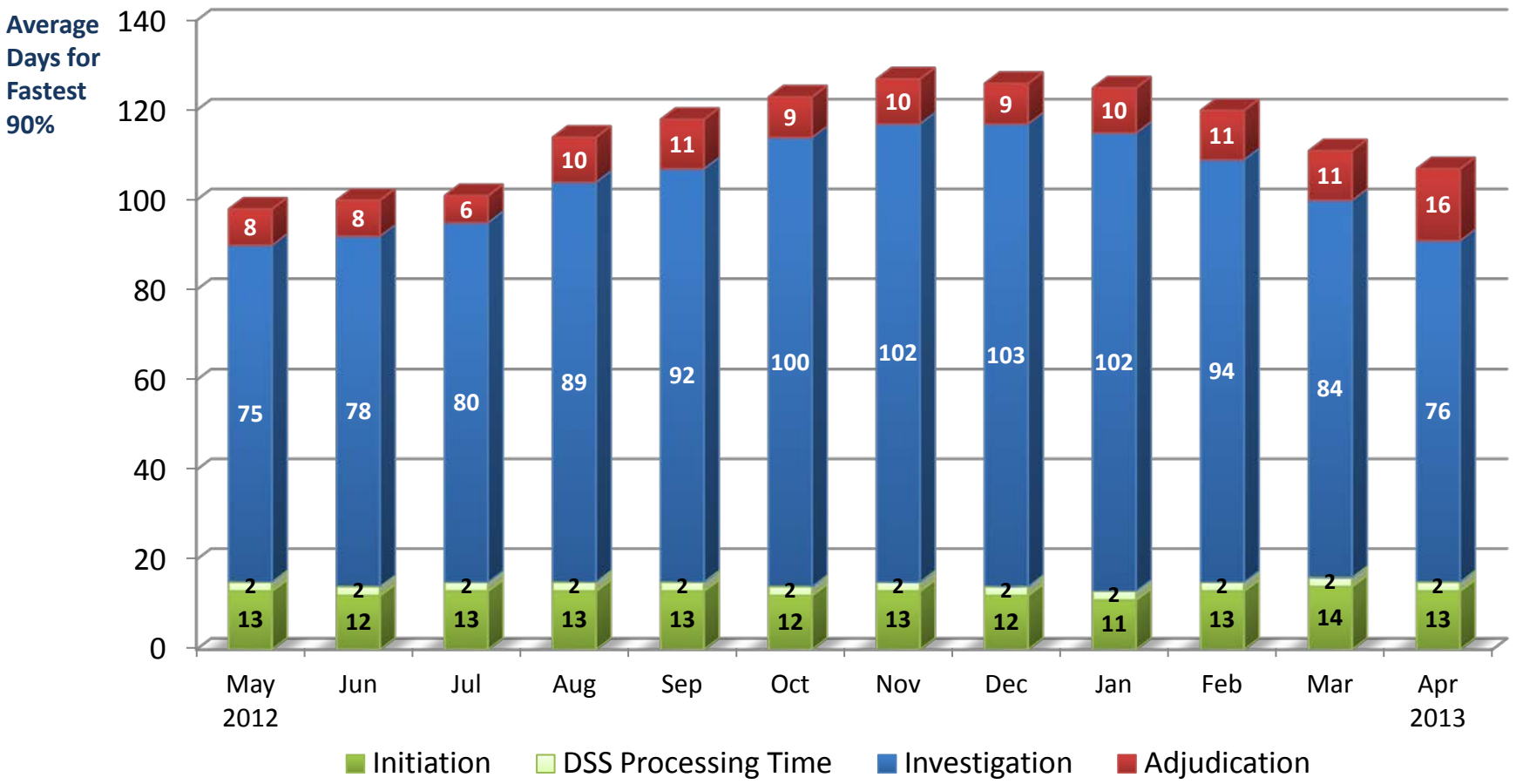
*The adjudication timeliness include collateral adjudication by DISCO and SCI adjudication by other DoD adjudication facilities

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



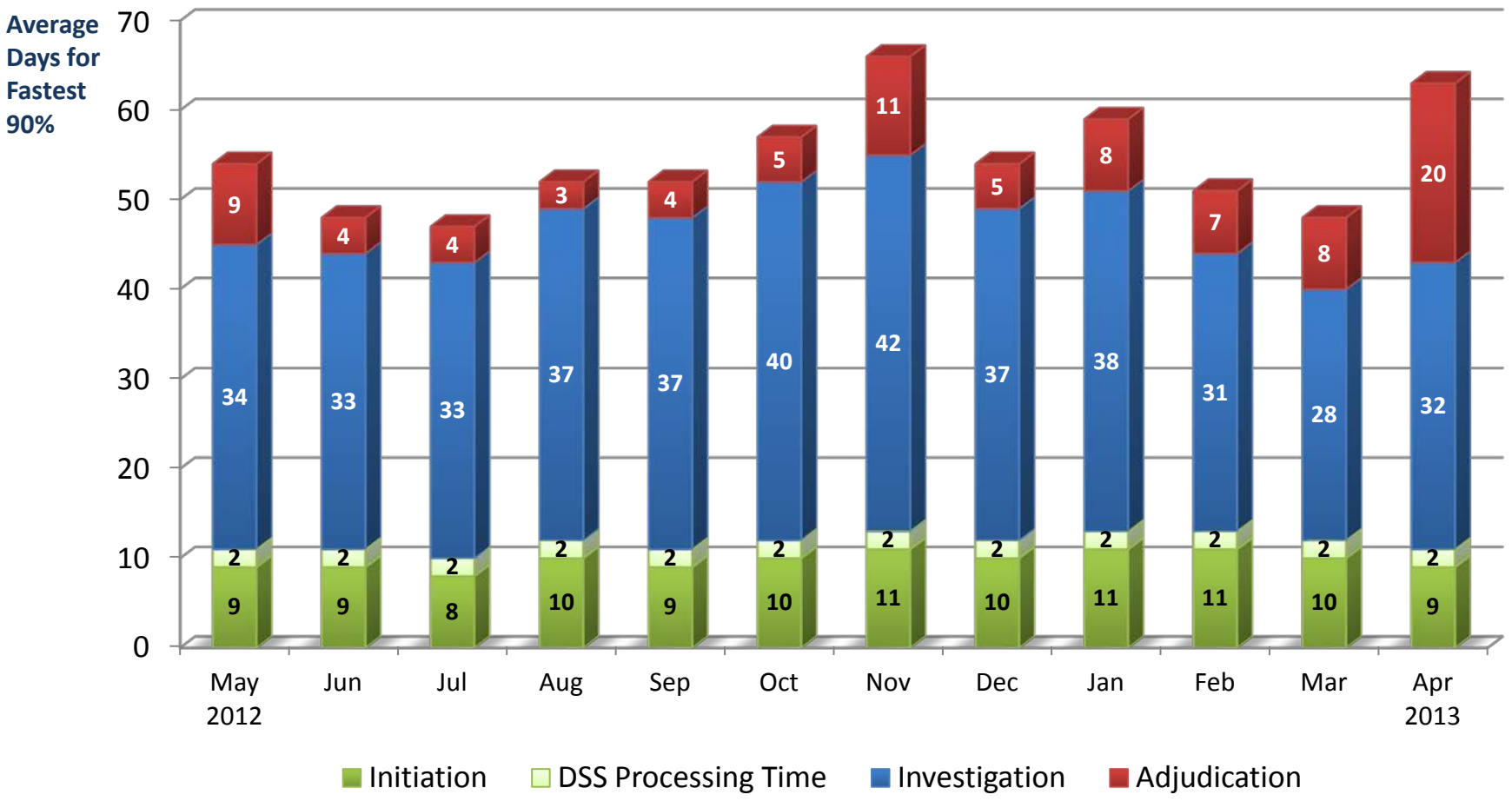
	May 2012	Jun 2012	Jul 2012	Aug 2012	Sep 2012	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013
100% of Reported Adjudications	10,633	10,980	4,013	10,333	8,054	3,745	3,343	7,901	8,710	8,392	9,056	7,964
Average Days for Fastest 90%	62 days	55 days	55 days	61 days	62 days	70 days	79 days	71 days	72 days	66 days	62 days	72 days

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



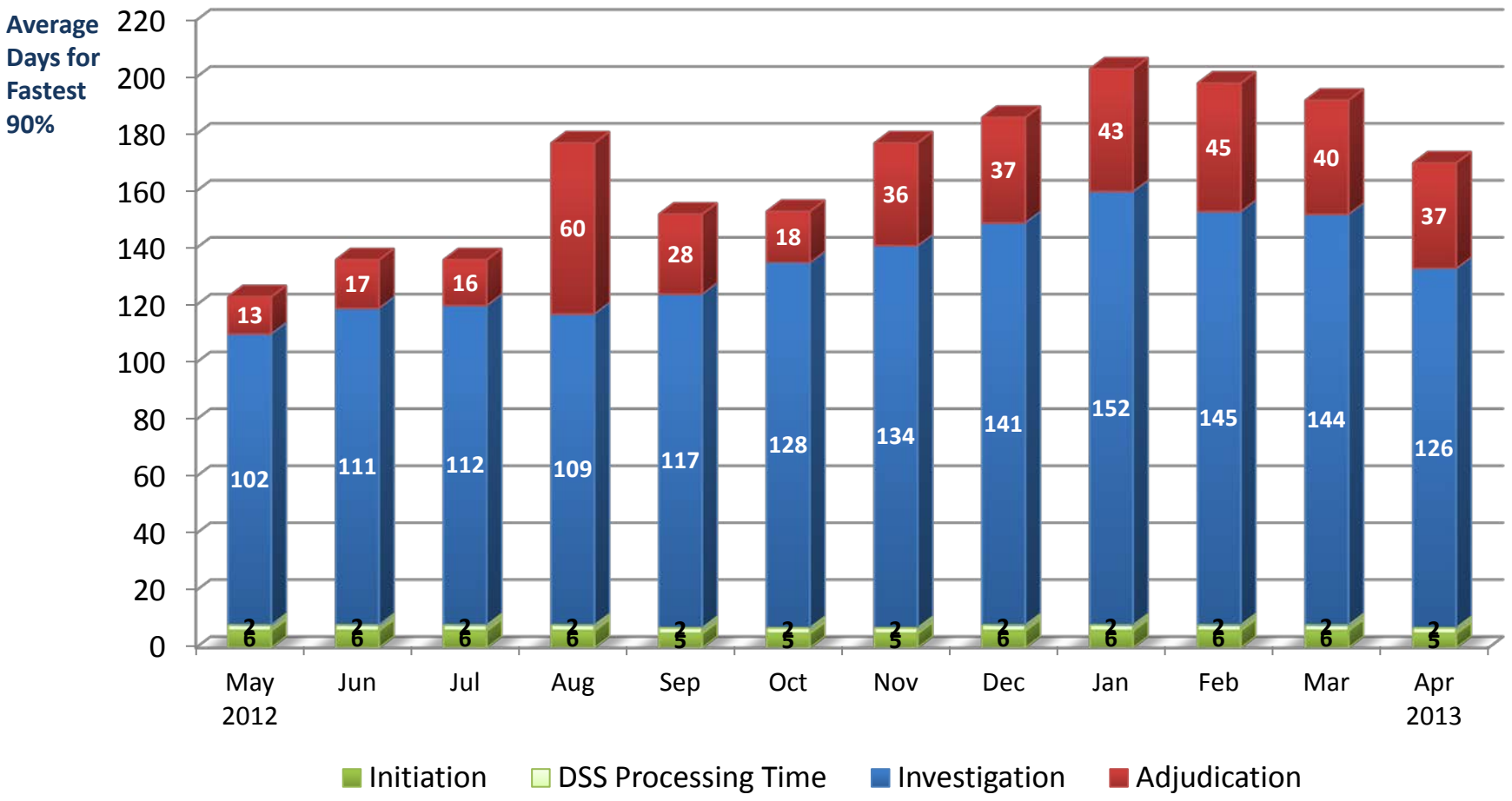
	May 2012	Jun 2012	Jul 2012	Aug 2012	Sep 2012	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013
100% of Reported Adjudications	2,023	1,625	595	1,573	1,420	740	718	1,945	1,805	1,910	2,073	1,637
Average Days for fastest 90%	98 days	100 days	101 days	114 days	118 days	123 days	127 days	126 days	125 days	120 days	111 days	107 days

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



	May 2012	Jun 2012	Jul 2012	Aug 2012	Sep 2012	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013
100% of Reported Adjudications	8,610	9,355	3,418	8,760	6,634	3,005	2,625	5,956	6,905	6,482	6,983	6,327
Average Days for fastest 90%	54 days	48 days	47 days	52 days	52 days	57 days	66 days	54 days	59 days	51 days	48 days	63 days

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



	May 2012	Jun 2012	Jul 2012	Aug 2012	Sep 2012	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013
100% of Reported Adjudications	3,841	3,988	3,053	4,678	3,024	1,317	1,783	3,443	3,125	3,122	2,380	4,114
Average Days for fastest 90%	123 days	136 days	136 days	177 days	152 days	153 days	177 days	186 days	203 days	198 days	192 days	170 days

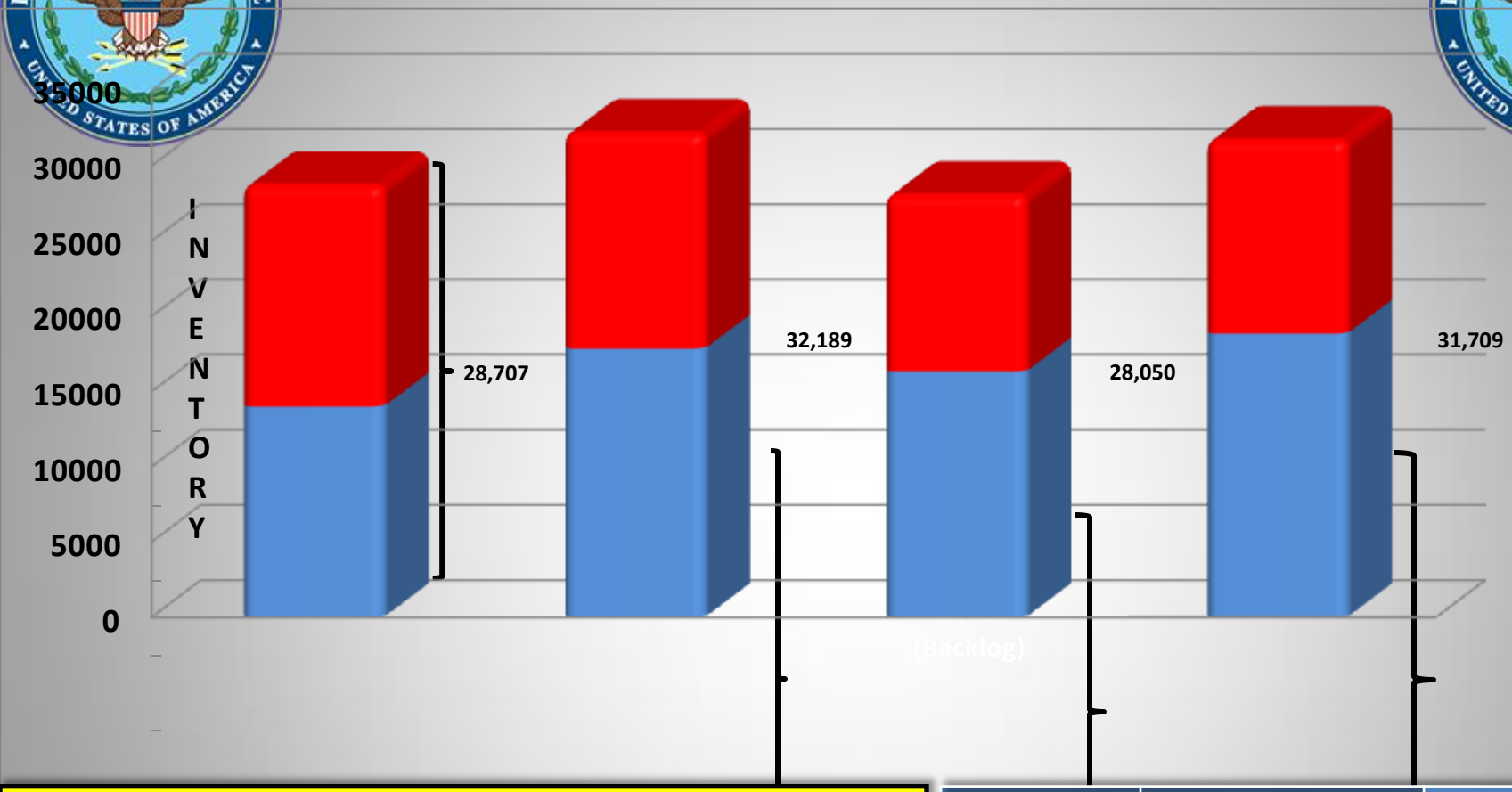
Attachment #5- DoD CAF PCL Presentation

Department of Defense
Consolidated Adjudications Facility

Brief to National Industrial Security Program Policy Advisory Committee

17 July 2013

DoD CAF Industry Workload



- **Workload Changes Since APR 13:**
  - Overall WIP increased by **3,002** cases **(10.4%)**
  - NISP Backlog decreased by **1,843** cases **(12.5%)**
  - Better cross-CAF balance with inherited portfolios
  - Reduction of NISP backlog stalled with cessation of OT

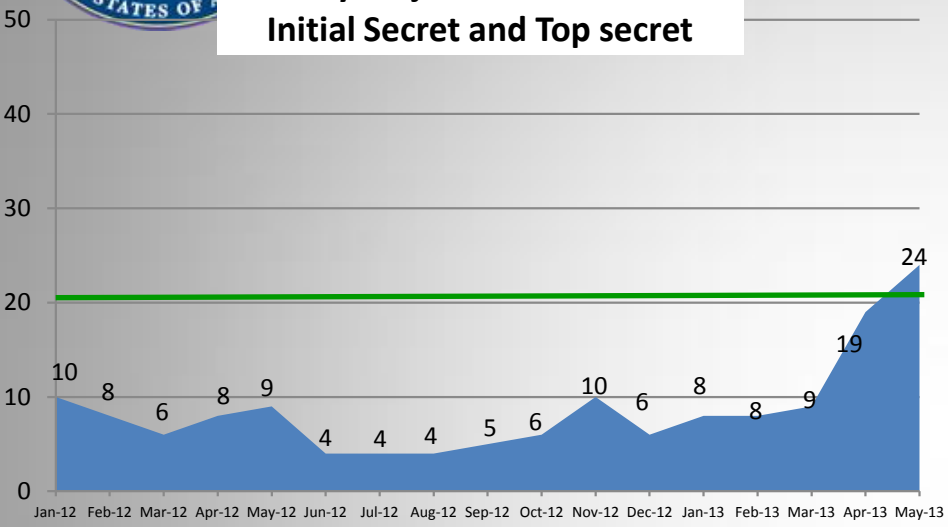
17,851
Steady State

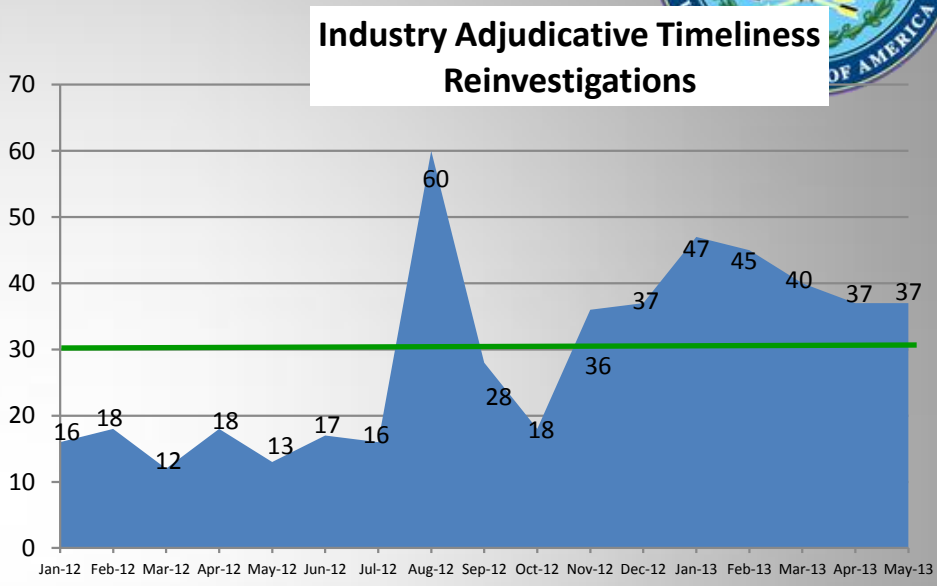
Month	Total NISP Workload	otal CAF Inventory
April	28,707	37.9%
	(+3,482)	40.5% (+2.6%)
June	28,050 (-4,139)	35% (-5.5%)
	31,709 (+3,659)	39% (+4%)

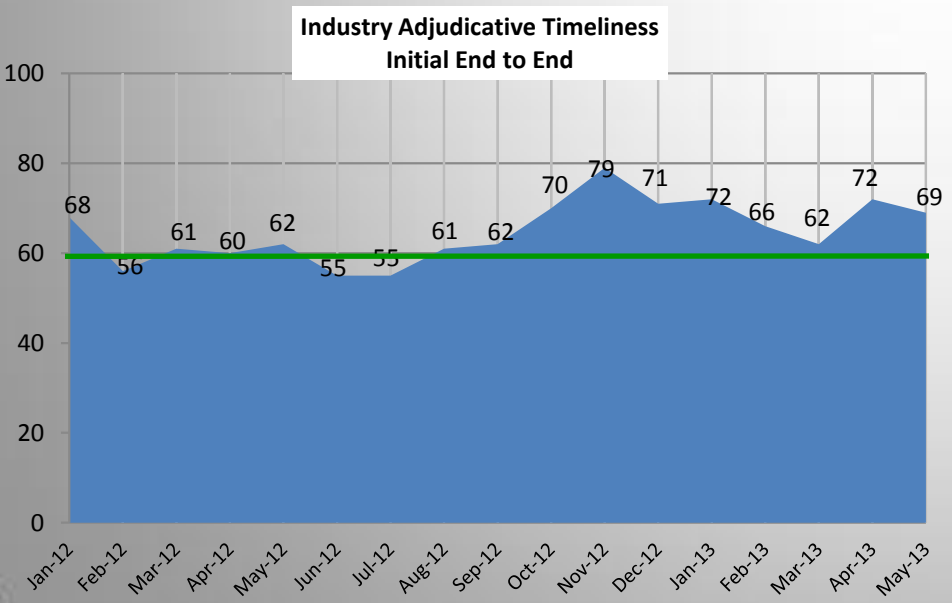
5-Apr-13 3-May-13 1-Jun-13 1-Jul-13

y Backlog

Industry IRTPA Timelines







ASSESSMENT

- Industry "Initial PSI" timelines:
  - Climb as more old/backlog cases closed
  - Trend stays negative until backlogs eliminated
- Sustainment of positive Reinvestigation trend is good; this will be <u>tough to maintain</u>

DoD Consolidated Adjudications Facility (CAF) Summary and Takeaways:

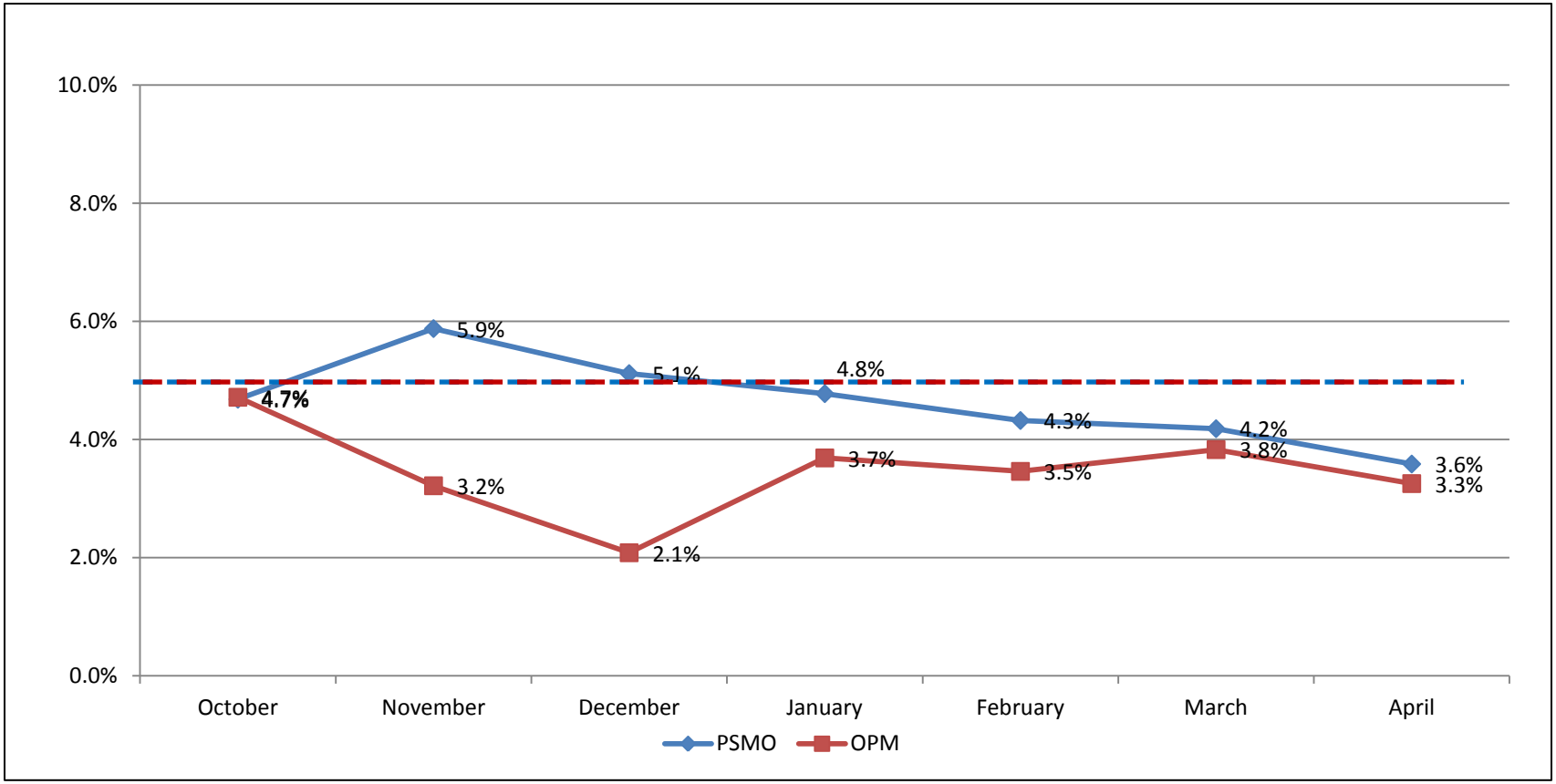
- **IRTPA**
  - Initials (SSBI & NACLC) edged above the established IRTPA standard in May due to the cessation of OT and the ongoing industry merger.
  - SSBI-PR's & PPR's are above the established USDI standard of 30 days
  - DoD CAF requested OPM to provide separate DoD CAF IRTPA reporting
- **DoD CAF Caseload Inventory**
  - Industrial caseload WIP standard not 100% defined….yet!
  - DoD CAF to improve timeliness and eliminate backlog via:
    - Improved Processes
    - New Efficiencies

    } On-going merger of former DISCO and DOHA; reducing "touch time"
    - Reallocation of adjudicator manpower to NISP cases
- **DoD CAF Director Assessment:**
  - On-going reduction of Industry backlog will stall due to planned furloughs
  - 1-2 years to fully eliminate Industrial case backlog
  - Timeliness for "Initials" to increase as we adjudicate more & older backlog cases
  - Merger of former DISCO & DOHA to enhance overall efficiency and effectiveness

Attachment #6- PSMO PCL Presentation

FY 13 PSMO-I and OPM Reject Rates

Initial and Periodic Reinvestigation Clearance Requests



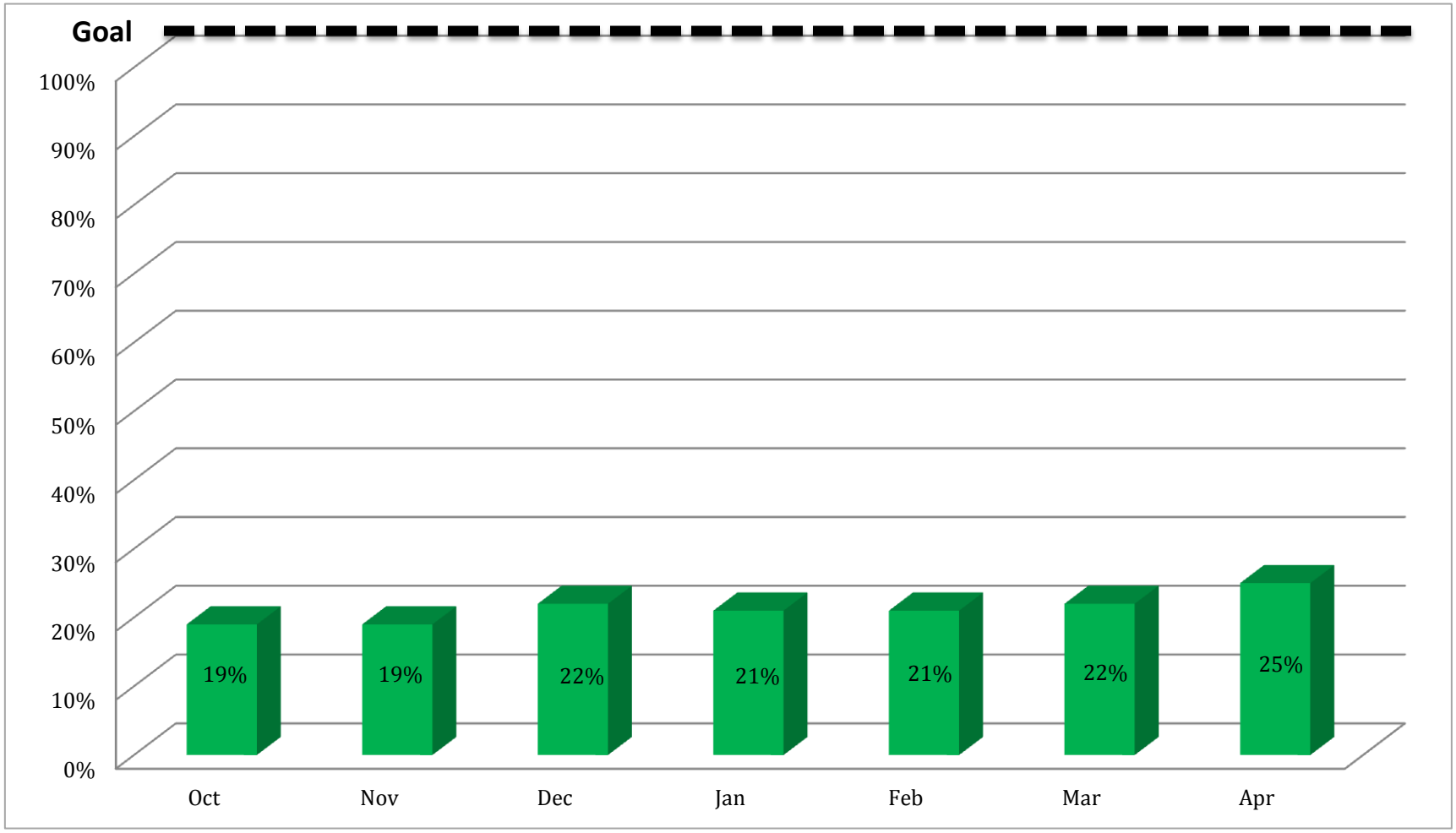
Defense Security Service (DSS)
Reasons for Case Rejection by PSMO-I
(Feb – Apr)

Top Five DSS Rejection Reasons	Count	Percent
Missing Employment Information (Submitting Organization)	810	50%
Missing Relative Information	309	19%
Missing Selective Service registration information	209	13%
Missing social security number of spouse or co-habitant	158	10%
Missing School Reference information	139	9%
Top Five Grand Total	**1625**	**100%**

Defense Security Service (DSS)
Reasons for Case Rejection by OPM
(Feb – Apr)

Top Five OPM Rejection Reasons	Count	Percent
Missing Fingerprint Cards not submitted with SF 86	805	49%
Certification and Release Forms not signed or submitted	659	40%
Discrepancy with applicant's place of birth and date of birth	114	7%
Missing or Discrepant Reference information	50	3%
Missing SSN for spouse/cohabitant	23	1%
Top Five Grand Total	**1656**	**100%**

Industry Electronic Fingerprint Submissions – FY13



Attachment #7- ODNI PCL Presentation

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Industry Performance Metrics

ONCIX/Special Security Directorate

LEADING INTELLIGENCE INTEGRATION

NISPPAC
17 July 2013

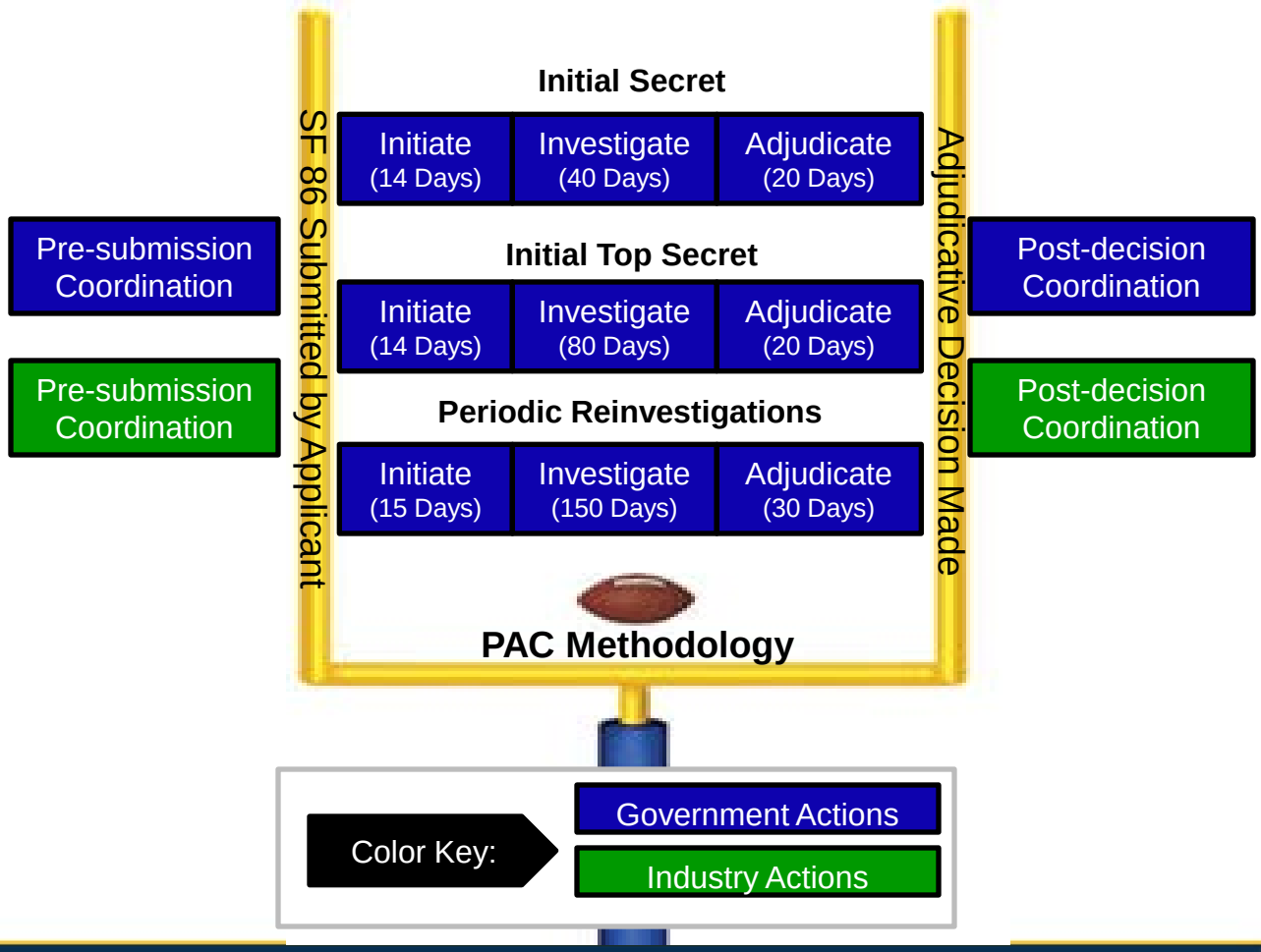
Security Executive Agent

- The DNI, as Security Executive Agent, is responsible for:
  - "the oversight of investigations and determinations of eligibility for access to classified information or eligibility to hold a sensitive position made by any agency"
  - "developing uniform and consistent policies and procedures" to ensure the effective, efficient, and timely completion of national security investigations and adjudications

- E.O. 13467

Who is responsible for the timelines?

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



Who is Getting Cleared?
… and how Fast?

Overall U.S. Government

Workload by ISP
- 95% OPM
- 4% IC Agencies
- <1% Other

Government Employees

Overall Industry (DoD + IC)

Timeliness:
- Secret Initials (slide 6)
- TS Initials (slide 7)
- PRs (slide 8)

Backlog:
- PRs (slide 9)

Intelligence Community Industry Cases

Timeliness:
- Secret Initials (slide 11)
- TS Initials (slide 12)
- PRs (slide 13)

DoD Industry Cases

OPM / DoD briefing this section

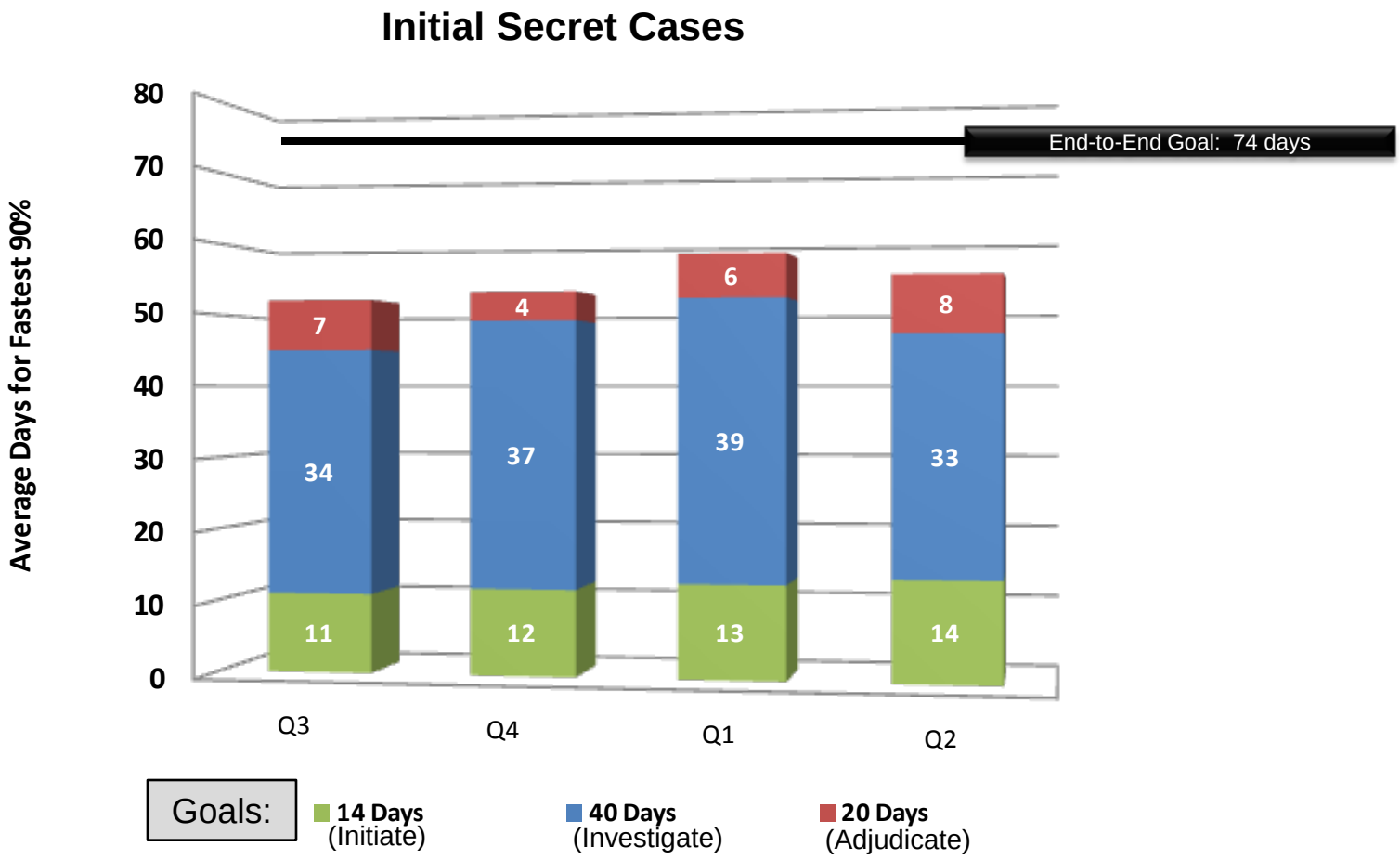
Overall Industry* FY13 Q2

Qtr 1 to Qtr 2 Analysis

- Initials
  - Secret – Goal 74 days (End-to-end)
    - Decreased 3 days (58 days to 55 days)
  - Top Secret – Goal 114 days (End-to-end)
    - Decreased 10 days (129 days to 119 days)
- Periodic Reinvestigations
  - Combined Performance – Goal 195 days (End-to-end)
    - Increased 14 days (194 days to 208 days)

*Based on IC and DoD Industry data

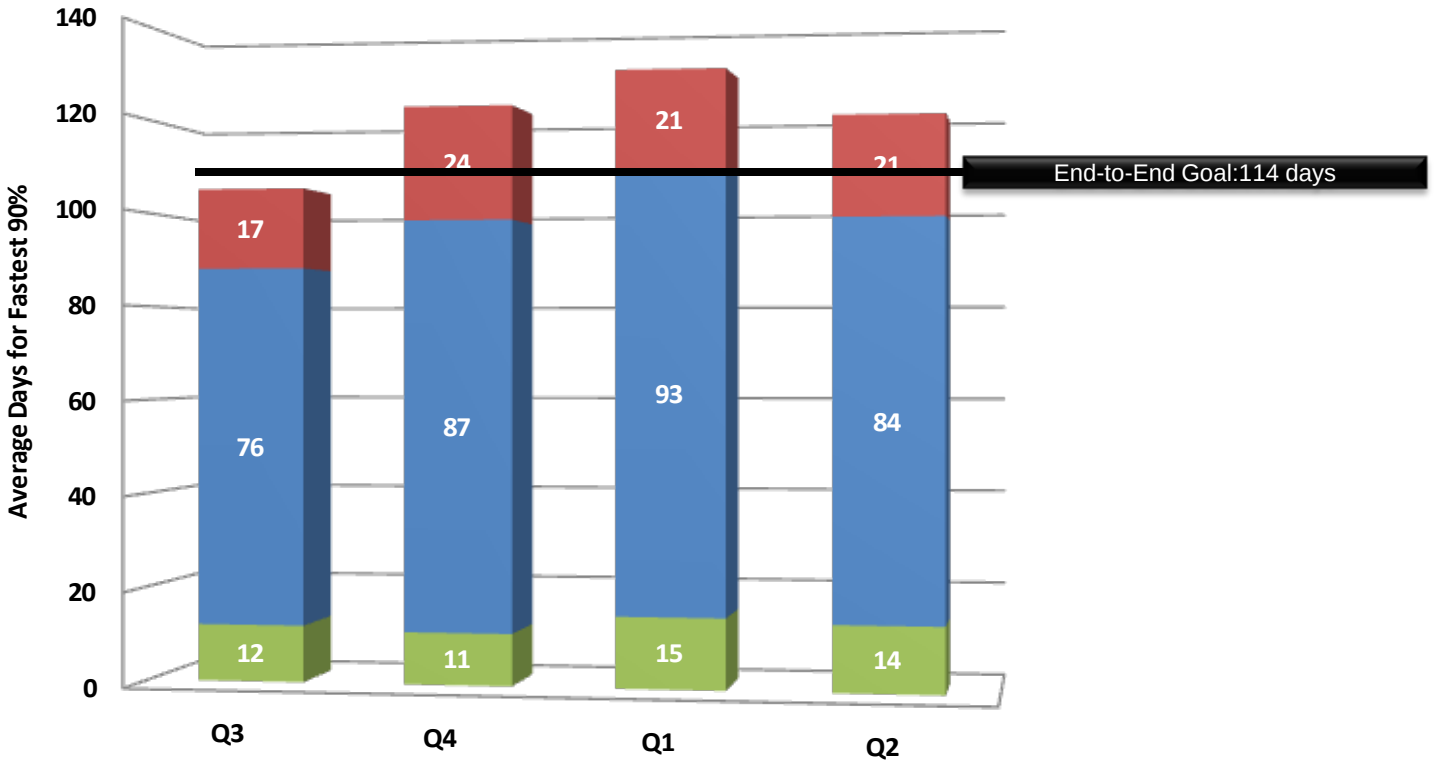
Overall Industry*



*Based on IC and DoD Industry data

Overall Industry*

Initial Top Secret Cases



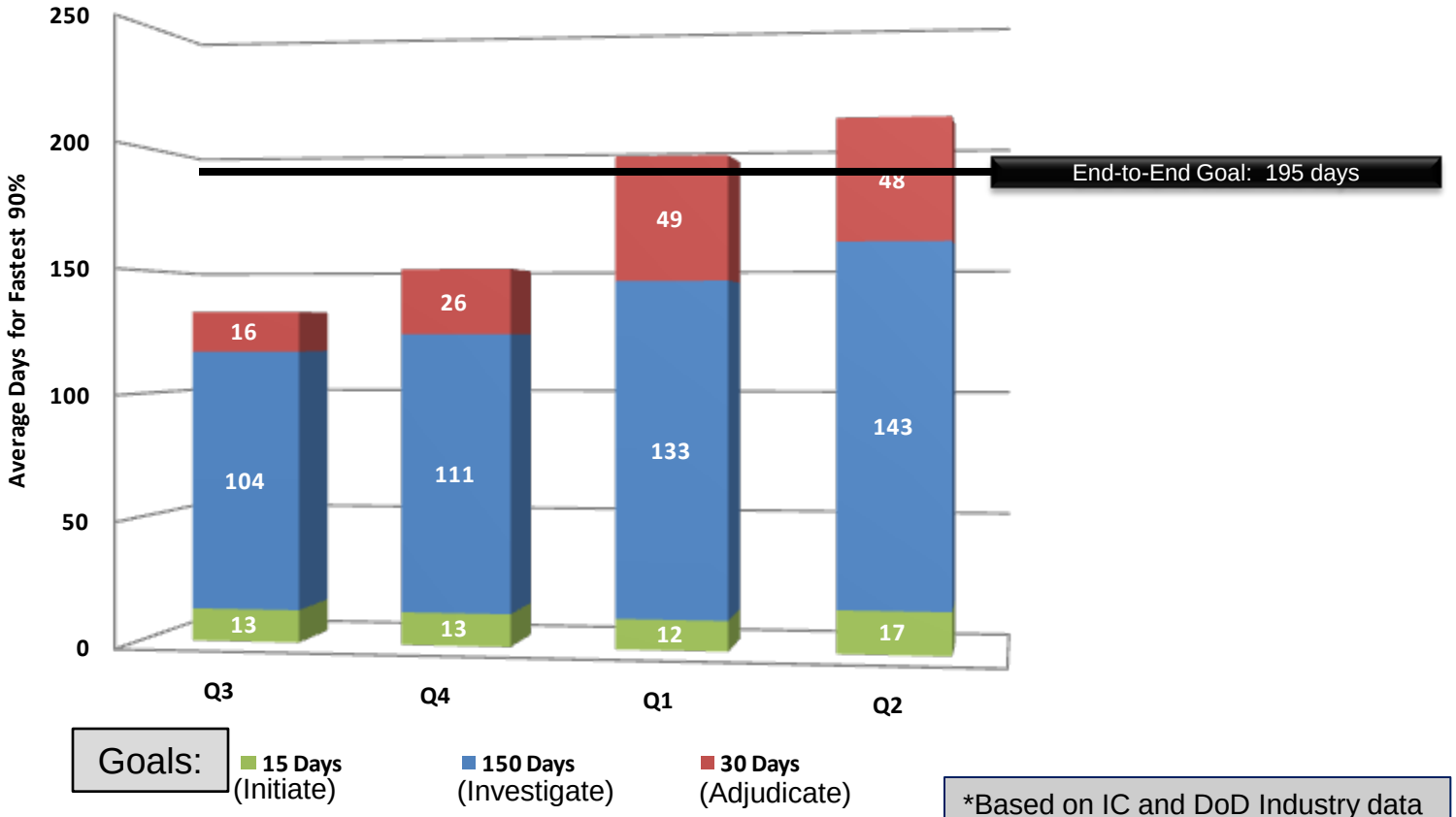
Goals:

- 14 Days (Initiate)
- 80 Days (Investigate)
- 20 Days (Adjudicate)

*Based on IC and DoD Industry data

Overall Industry*

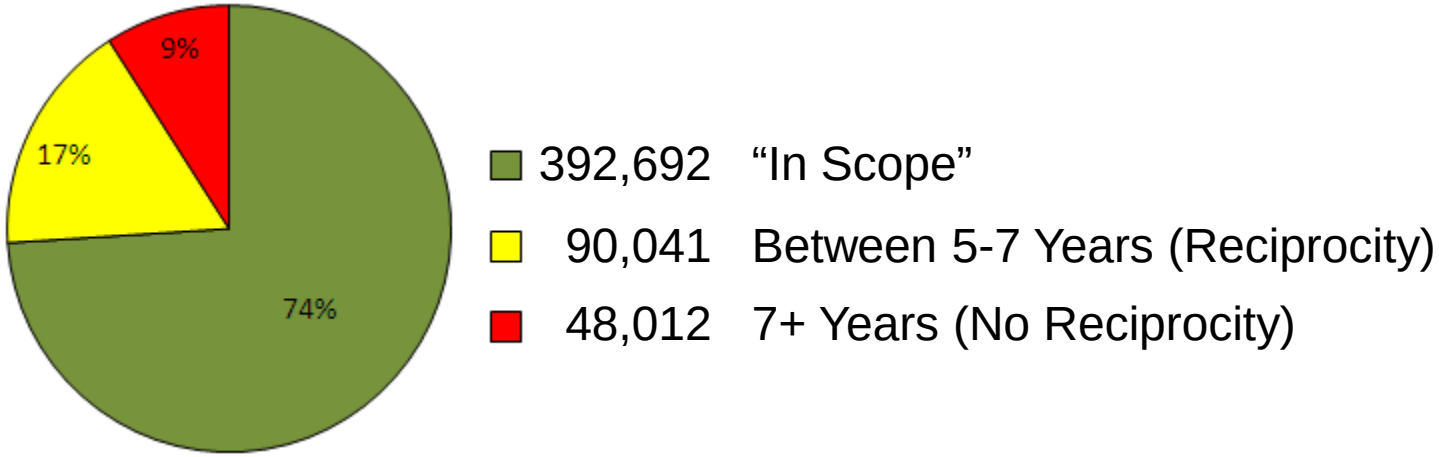
Periodic Reinvestigations



*Based on IC and DoD Industry data

Periodic Reinvestigation Backlog

- Overall Industry
  - Industry makes up almost half of all TS/SCI clearances in the USG
  - Data below: Scattered Castles + JPAS Query as of June 2013:



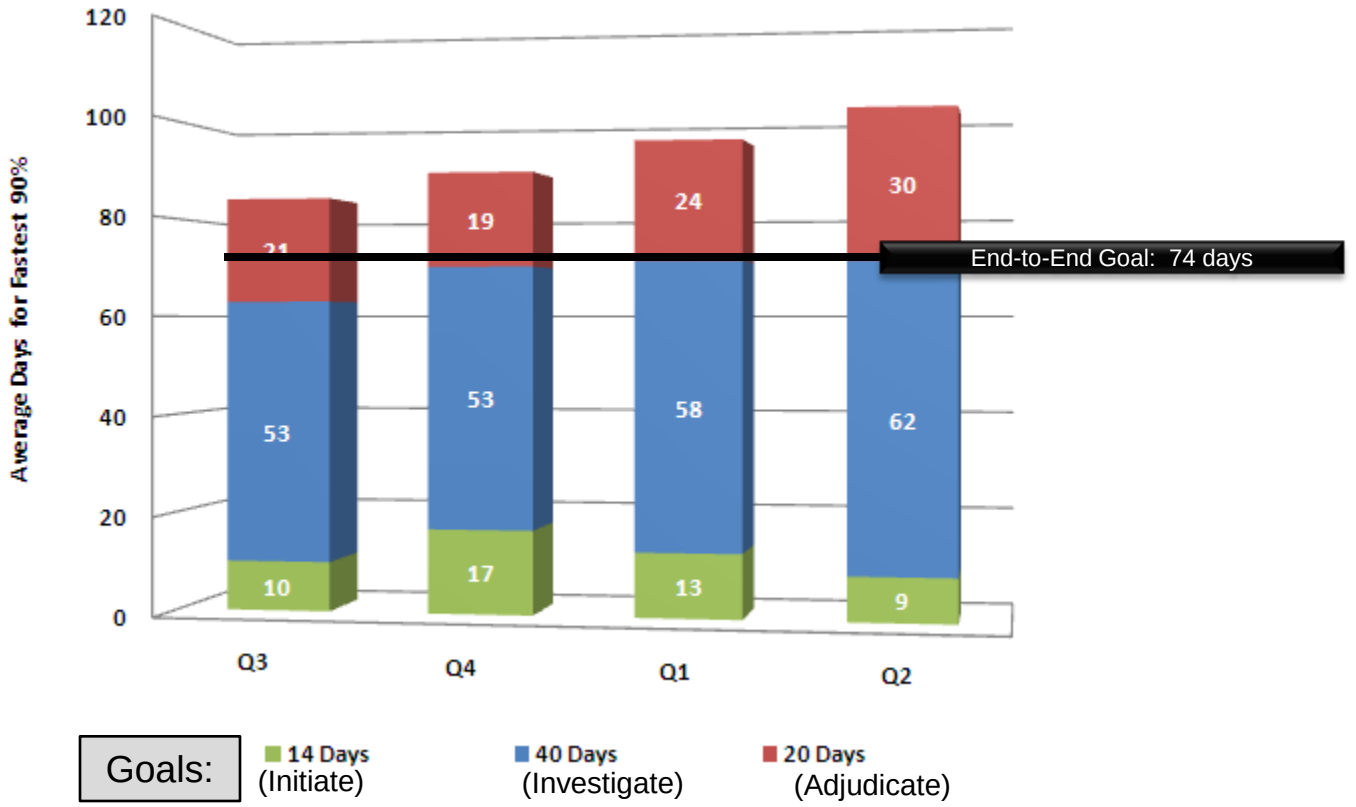
Intelligence Community Industry

Qtr 1 to Qtr 2 Analysis

- Initials
  - Secret – Goal 74 days
    - Increased 6 days (95 days to 101 days)
  - Top Secret – Goal 114 days
    - Decreased 11 days (134 days to 123 days)
- Periodic Reinvestigations
  - Combined Performance – Goal 195 days
    - Increased 16 days (229 days to 245 days)

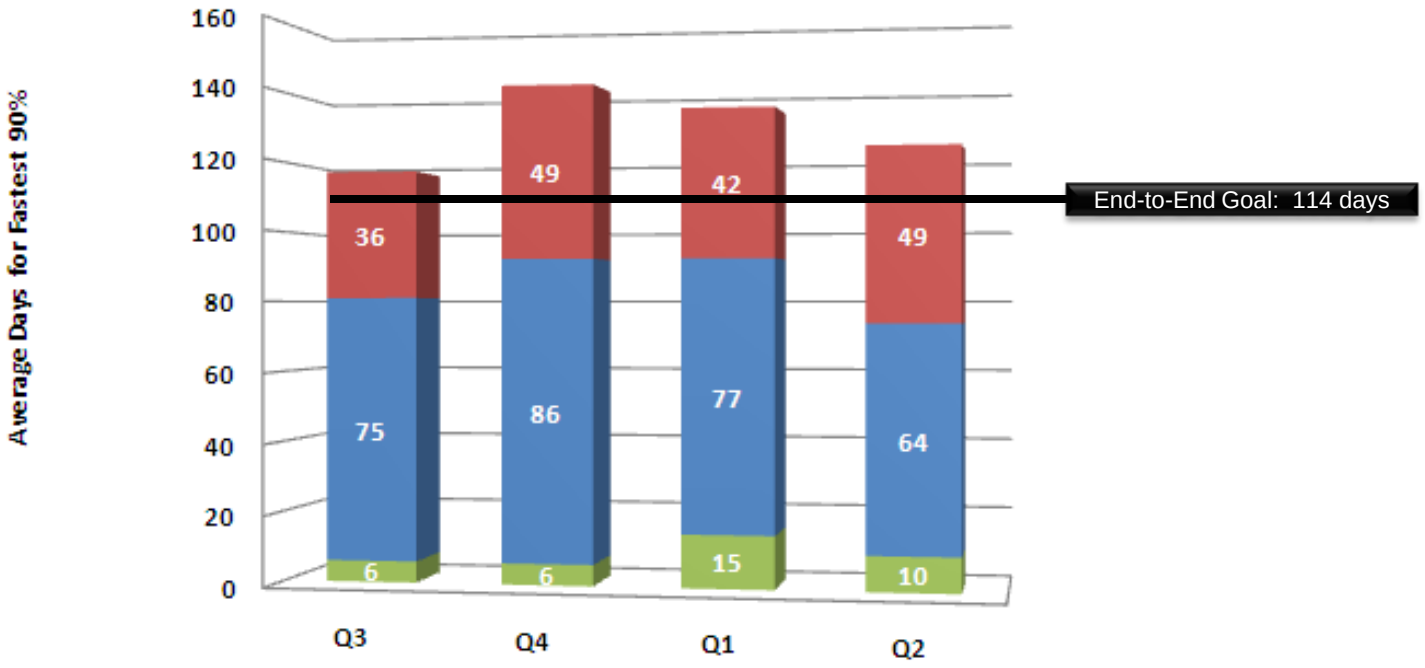
Intelligence Community Industry

Initial Secret Cases



Intelligence Community Industry

Initial Top Secret Cases

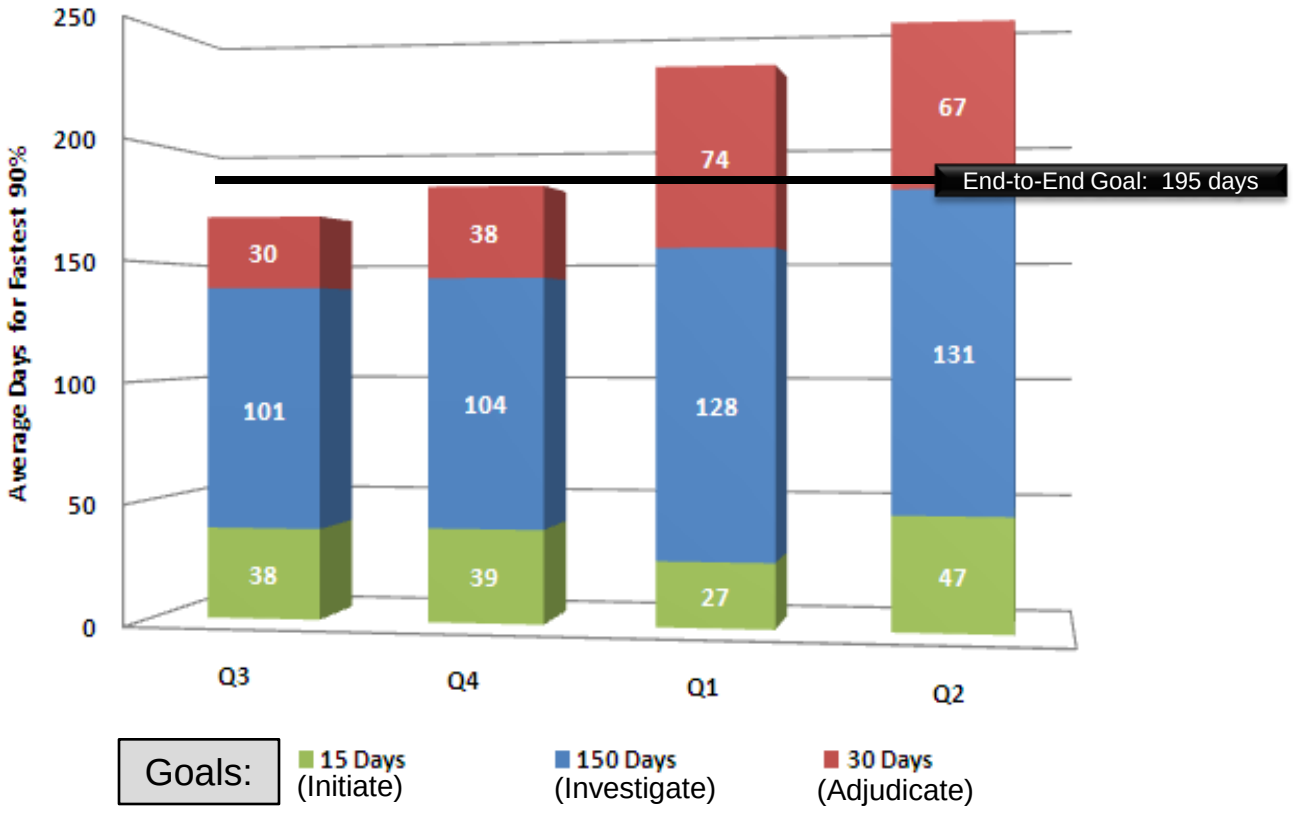


Goals:

- 14 Days (Initiate)
- 80 Days (Investigate)
- 20 Days (Adjudicate)

Intelligence Community Industry

Periodic Reinvestigations



Attachment #8- DOE PCL Presentation

U.S. Department of Energy

Personnel Security Brief

June 2013

Personnel Security Overview

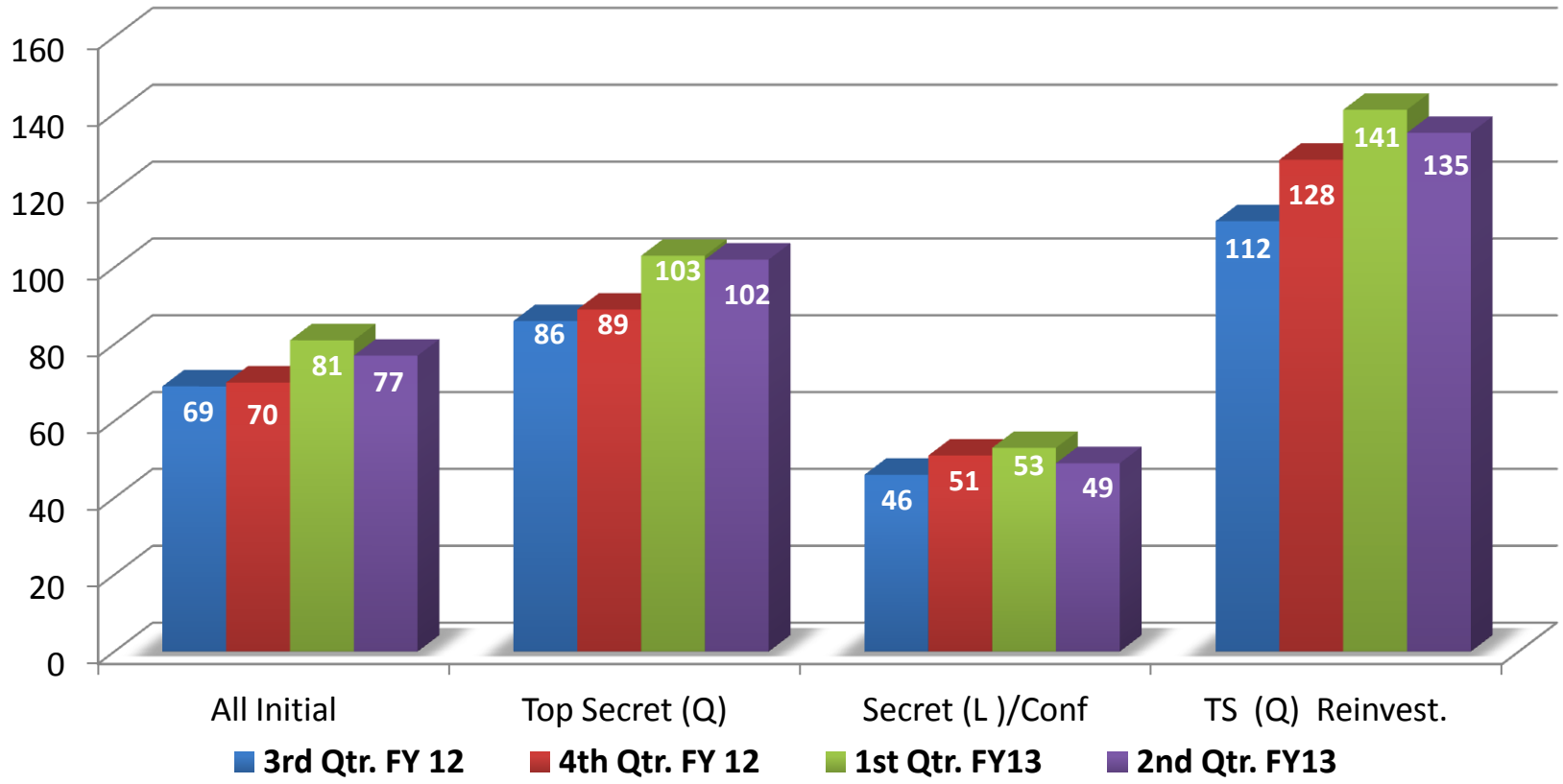
- DOE adjudicates both Federal and contractor staff
- Eight adjudicative facilities
- Policy, administrative review, and appeal functions centralized at Headquarters
- Cleared contractors, as of June 1, 2013:

  -61,072 Q access authorizations

  -22,958 L access authorizations
- Have met IRTPA initial security clearance adjudicative goals since April 2009

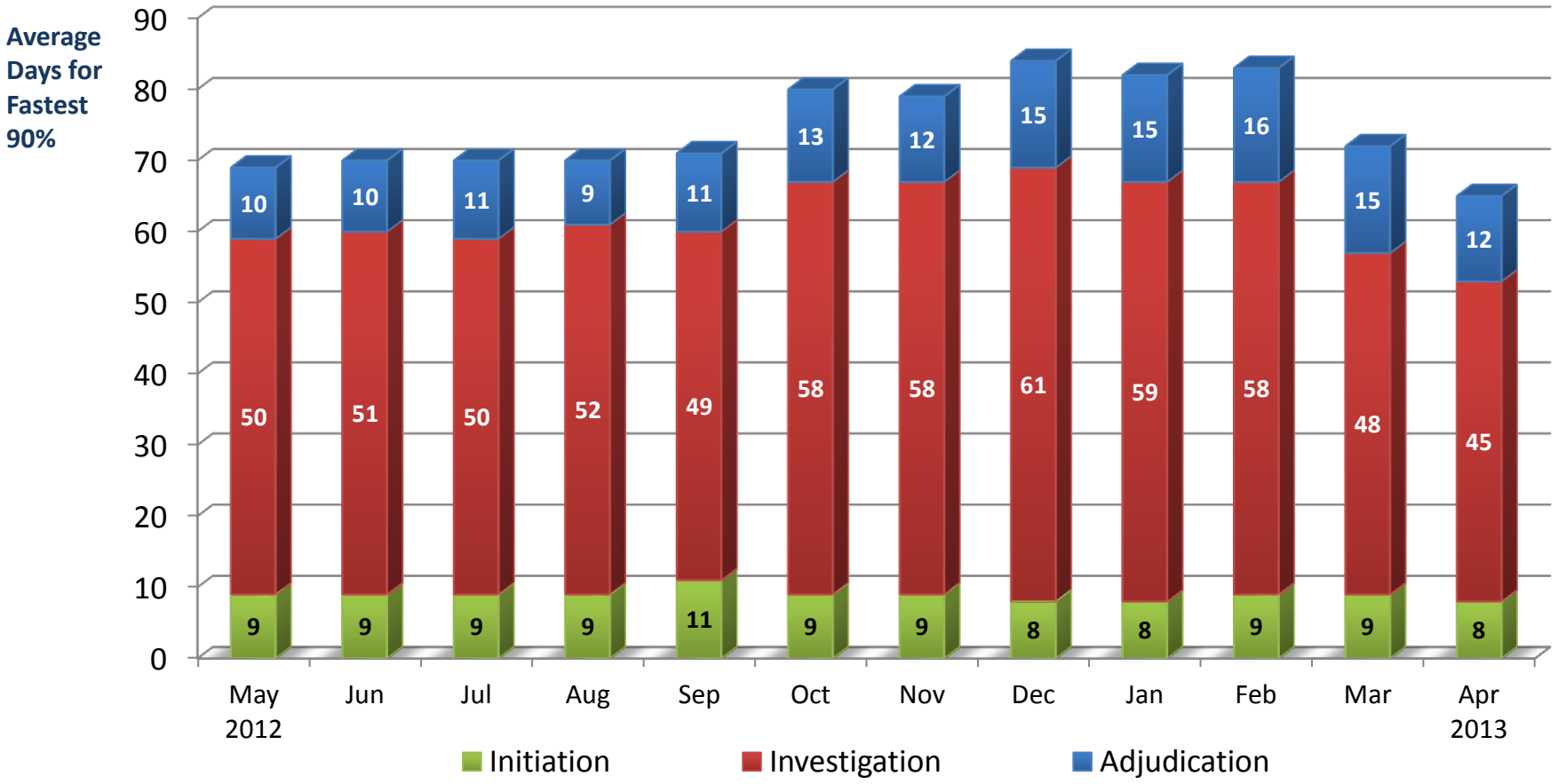
Timeliness Performance Metrics for DOE's Personnel Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made



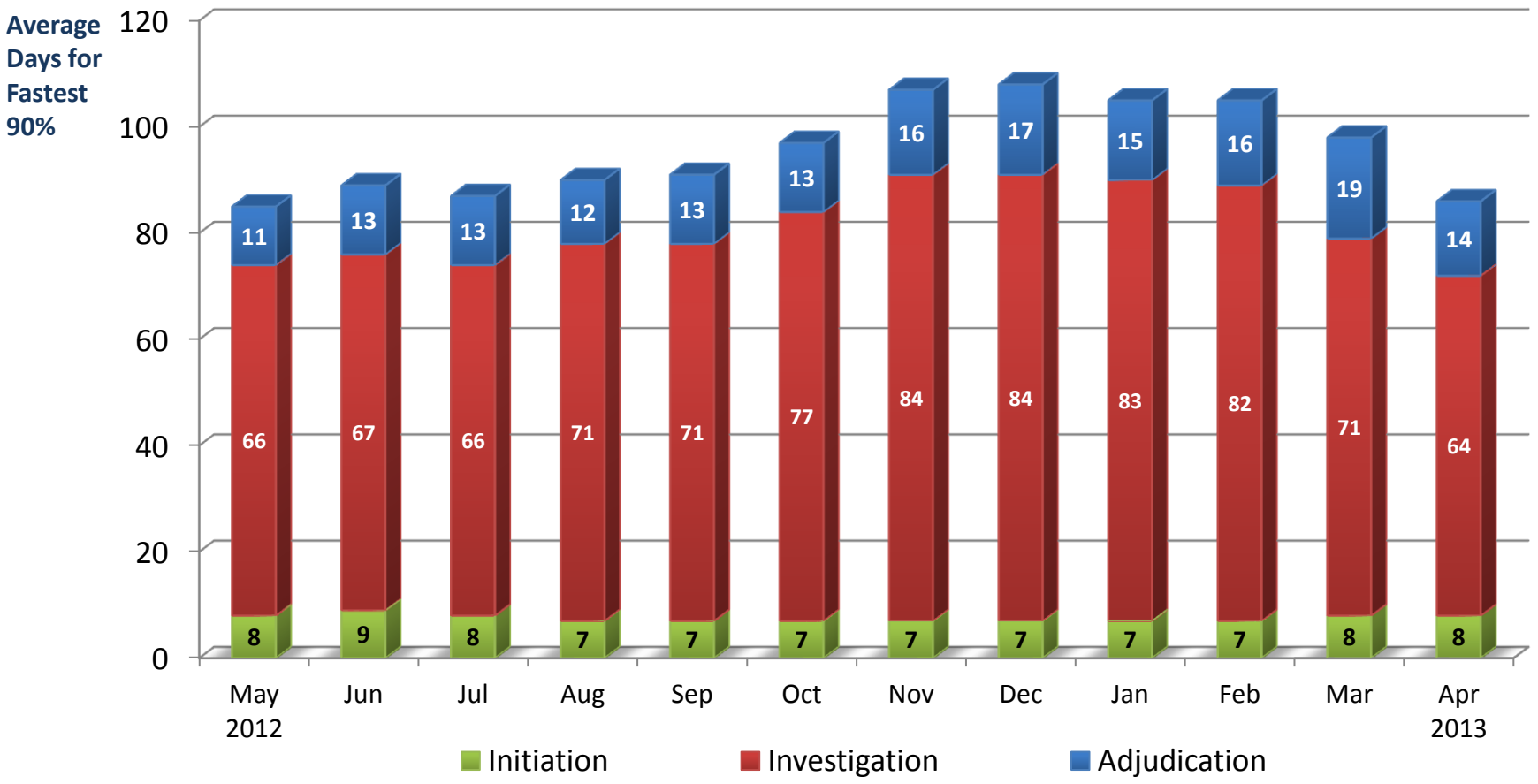
	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 3rd Q FY12	1,614	919	695	2,883
Adjudication actions taken – 4th Q FY12	1,424	735	689	3,495
Adjudication actions taken – 1st Q FY13	1,362	770	592	1,895
Adjudication actions taken – 2nd Q FY13	1,679	914	765	1,971

DOE's Average Timeliness Trends for 90% Initial Top Secret(Q) and All Secret (L)/Confidential Security Clearance Decisions



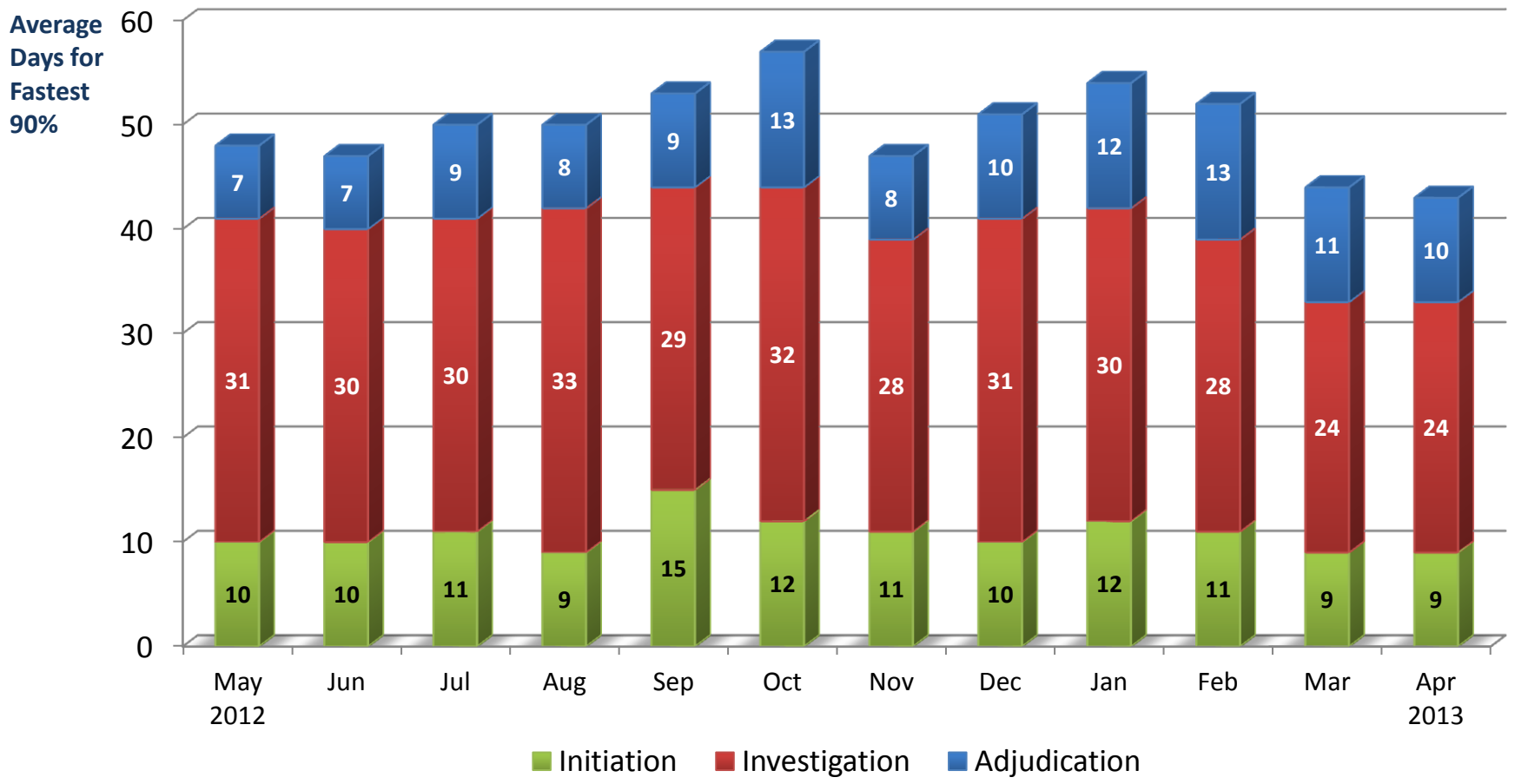
	May 2012	Jun 2012	Jul 2012	Aug 2012	Sep 2012	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013
100% of Reported Adjudications	534	504	523	465	411	447	415	409	523	494	596	719
Average Days for Fastest 90%	69 days	70 days	70 days	70 days	71 days	80 days	79 days	84 days	82 days	83 days	72 days	65 days

DOE's Average Timeliness Trends for 90% Initial Top Secret(Q) Security Clearance Decisions



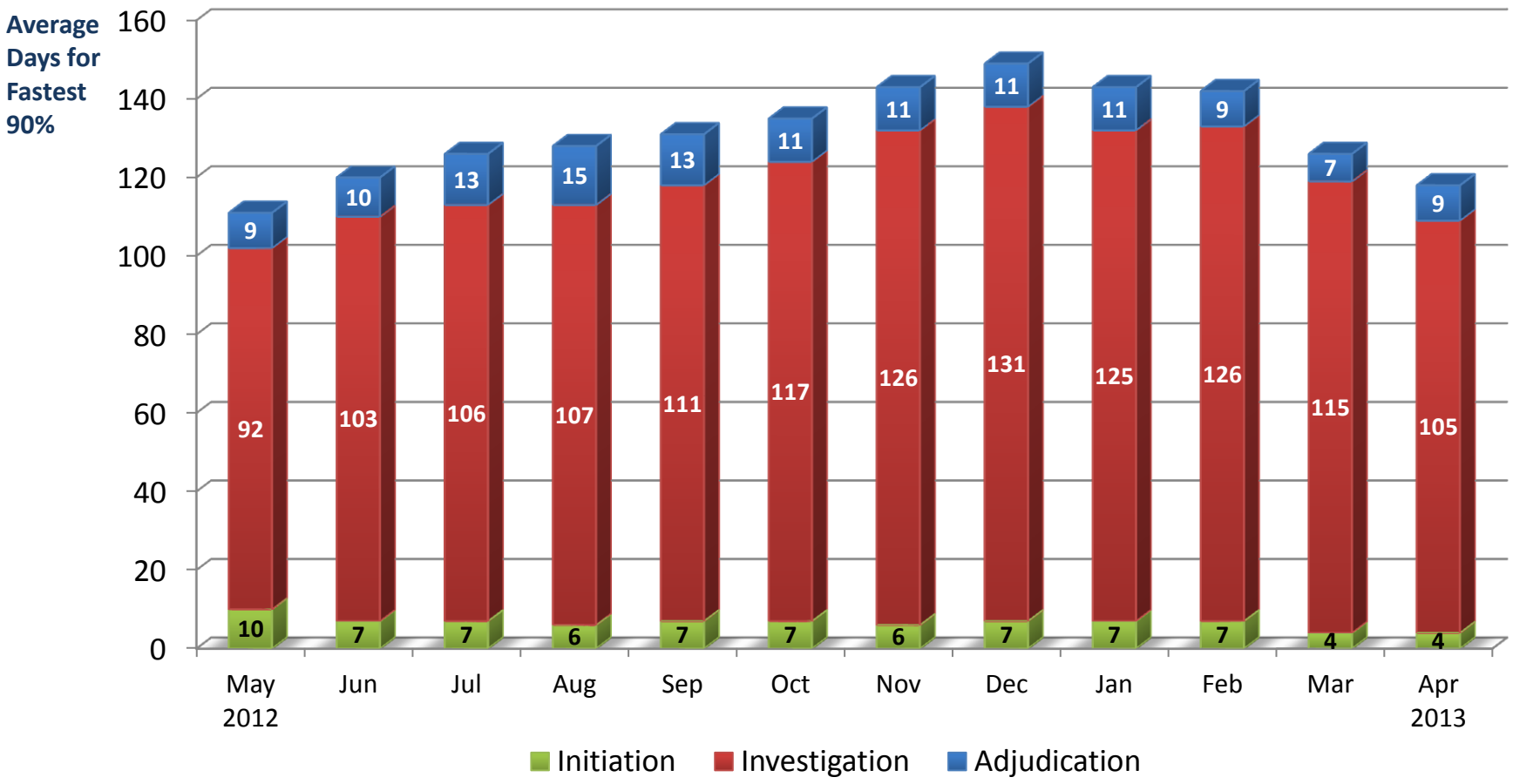
	May 2012	Jun 2012	Jul 2012	Aug 2012	Sep 2012	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013
100% of Reported Adjudications	311	293	290	235	202	263	232	244	302	285	311	381
Average Days for fastest 90%	85 days	89 days	87 days	90 days	91 days	97 days	107 days	108 days	105 days	105 days	98 days	86 days

DOE's Average Timeliness Trends for 90% Secret (L)/Confidential Security Clearance Decisions



	May 2012	Jun 2012	Jul 2012	Aug 2012	Sep 2012	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013
100% of Reported Adjudications	223	211	233	230	209	184	183	165	221	209	285	338
Average Days for fastest 90%	48 days	47 days	50 days	50 days	53 days	57 days	47 days	51 days	54 days	52 days	44 days	43 days

DOE's Average Timeliness Trends for 90%
Top Secret (Q) Reinvestigation Security Clearance Decisions



	May 2012	Jun 2012	Jul 2012	Aug 2012	Sep 2012	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013
100% of Reported Adjudications	850	1,077	1,281	1,268	911	831	540	479	500	580	860	1,159
Average Days for fastest 90%	111 days	120 days	126 days	128 days	131 days	135 days	143 days	149 days	143 days	142 days	126 days	118 days

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
June 2013

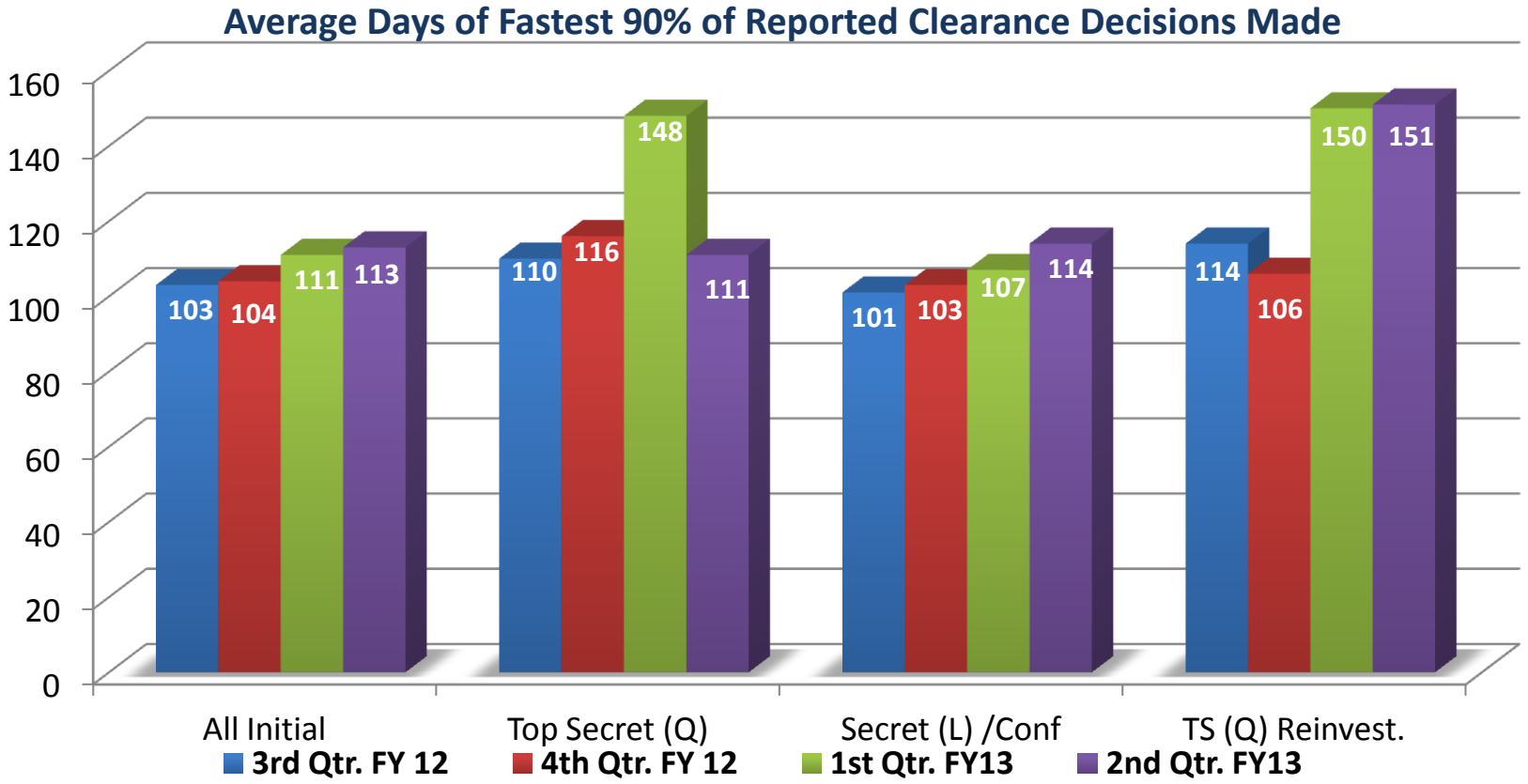
Active Clearances

As of June 4, 2013 the following reflects current active security clearances for the NRC:

- 4,611 Federal employees
- 4,540 Licensees
- 877 Contractors

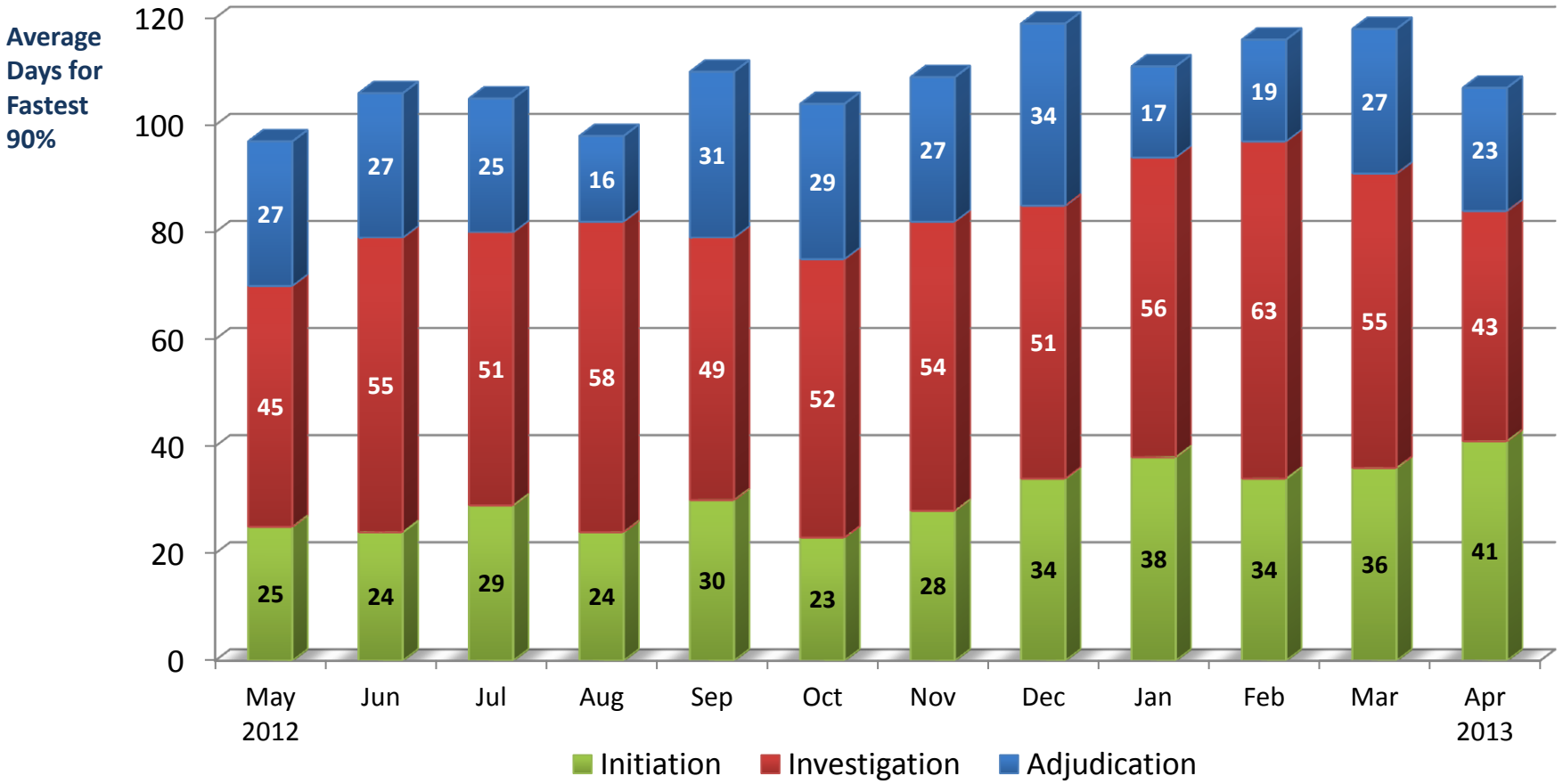
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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



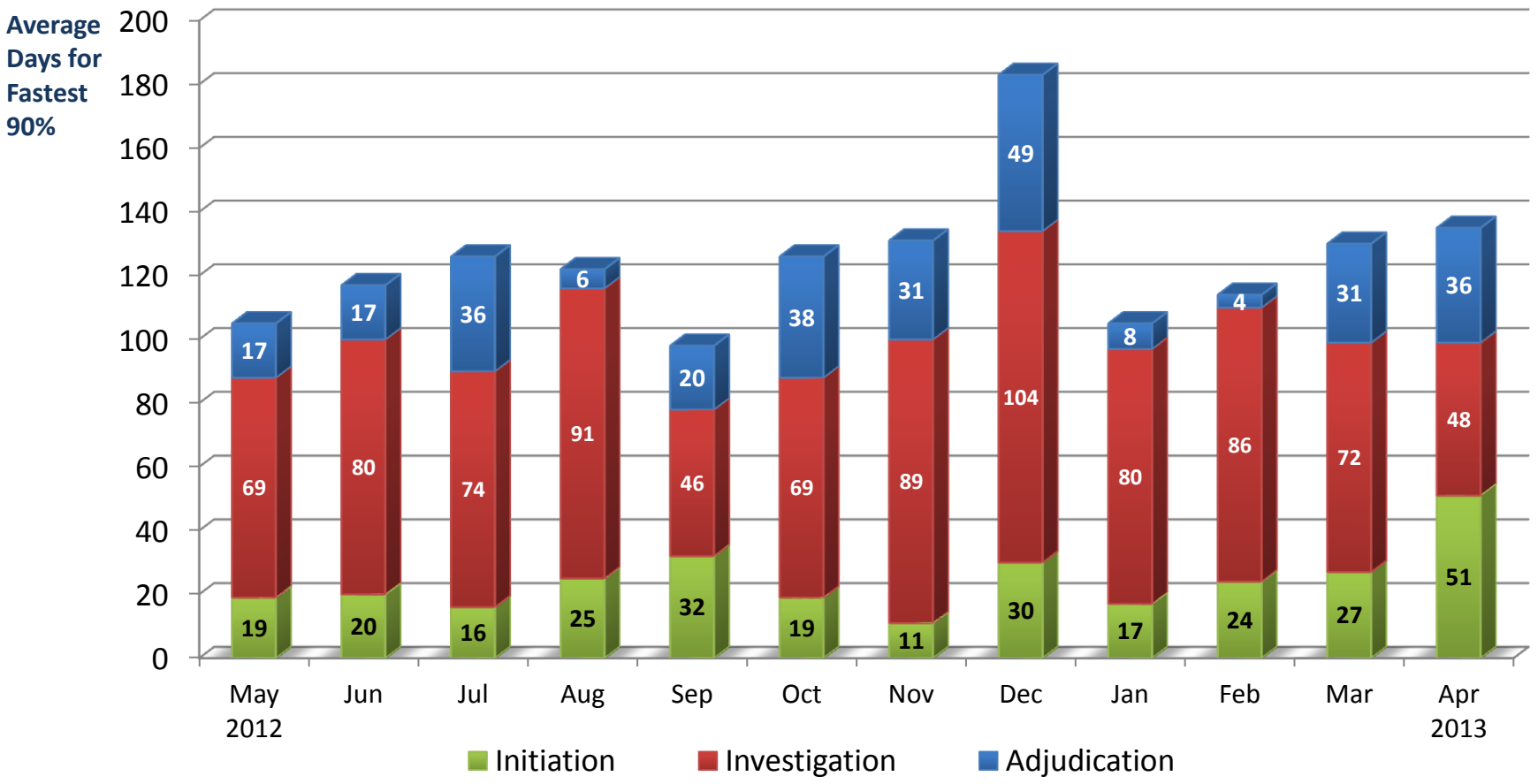
	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 3rd Q FY12	222	39	183	39
Adjudication actions taken – 4th Q FY12	245	21	224	47
Adjudication actions taken – 1st Q FY13	201	22	179	31
Adjudication actions taken – 2nd Q FY13	227	59	168	25

NRC's Average Timeliness Trends for 90% Initial Top Secret (Q) and All Secret (L) /Confidential Security Clearance Decisions



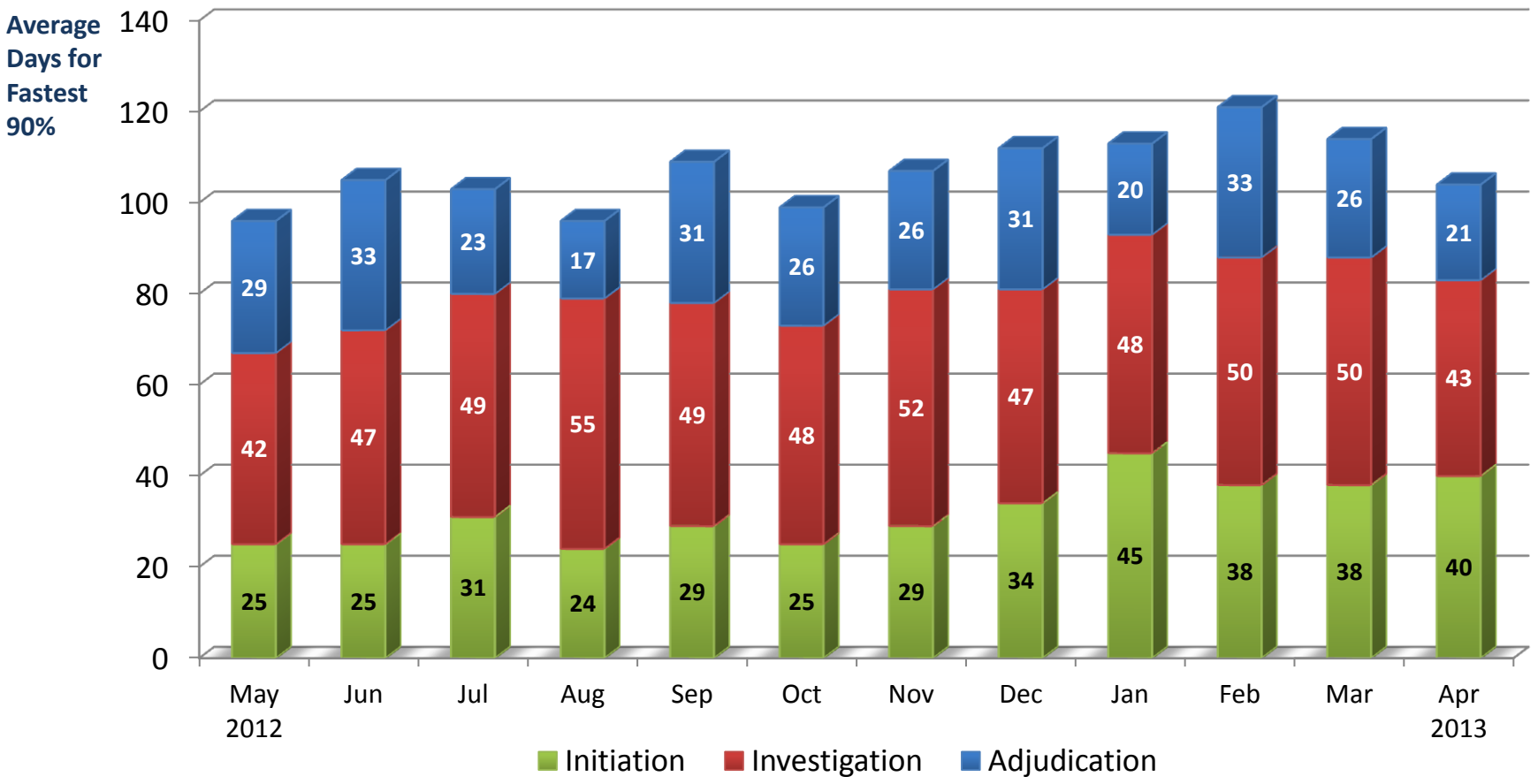
	May 2012	Jun 2012	Jul 2012	Aug 2012	Sep 2012	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013
100% of Reported Adjudications	81	66	100	63	83	44	92	64	71	65	91	69
Average Days for Fastest 90%	97 days	106 days	105 days	98 days	110 days	104 days	109 days	119 days	111 days	116 days	118 days	107 days

NRC's Average Timeliness Trends for 90% Initial Top Secret (Q) Security Clearance Decisions



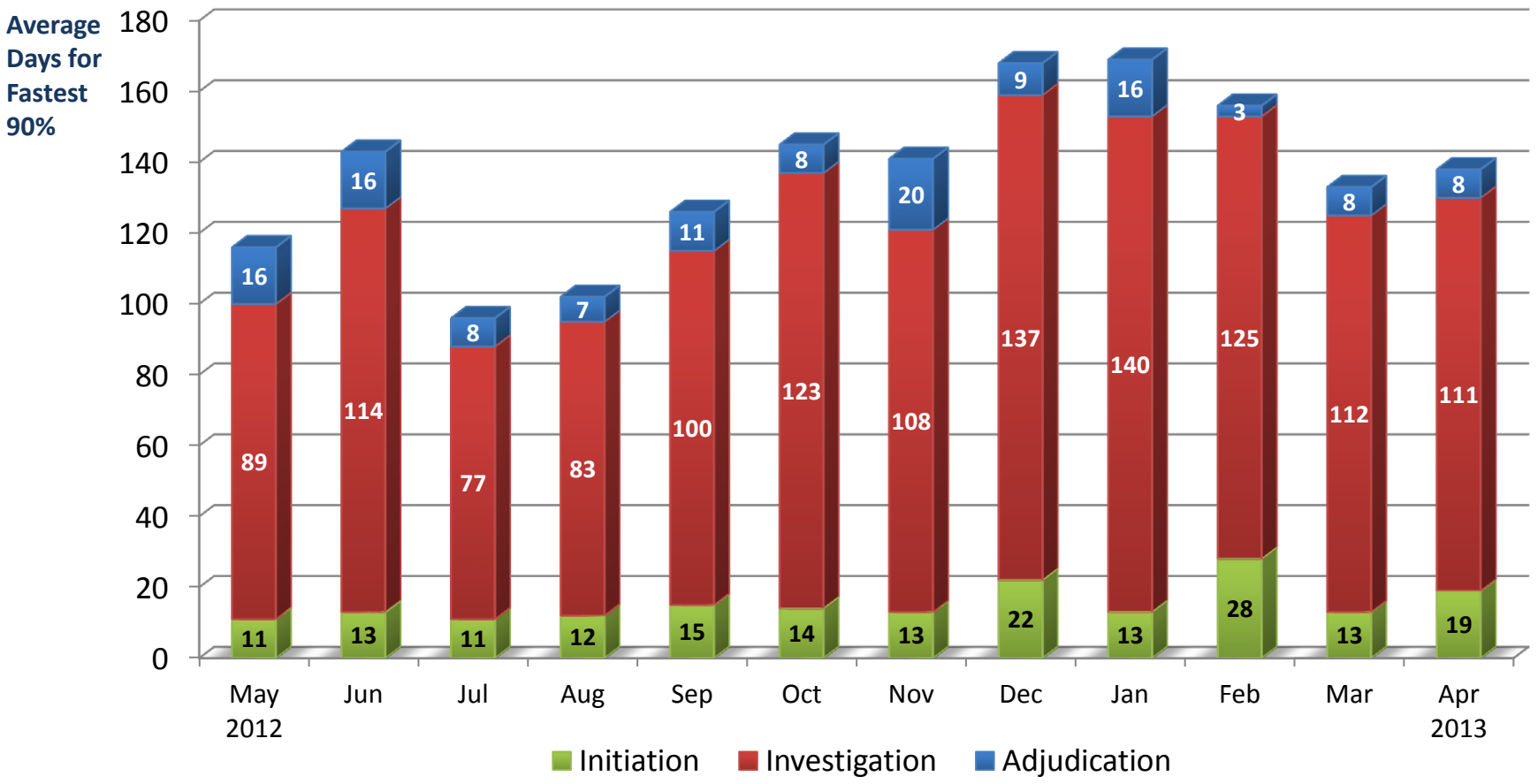
	May 2012	Jun 2012	Jul 2012	Aug 2012	Sep 2012	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013
100% of Reported Adjudications	11	15	10	4	7	9	6	7	16	21	22	7
Average Days for fastest 90%	105 days	117 days	126 days	122 days	98 days	126 days	131 days	183 days	105 days	114 days	130 days	135 days

NRC's Average Timeliness Trends for 90% Secret (L) /Confidential Security Clearance Decisions



	May 2012	Jun 2012	Jul 2012	Aug 2012	Sep 2012	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013
100% of Reported Adjudications	70	51	90	59	76	35	86	57	55	44	69	62
Average Days for fastest 90%	96 days	105 days	103 days	96 days	109 days	99 days	107 days	112 days	113 days	121 days	114 days	104 days

NRC's Average Timeliness Trends for 90%
Top Secret(Q) Reinvestigation Security Clearance Decisions



	May 2012	Jun 2012	Jul 2012	Aug 2012	Sep 2012	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013
100% of Reported Adjudications	11	15	15	16	16	10	10	11	6	8	11	11
Average Days for fastest 90%	116 days	143 days	96 days	102 days	126 days	145 days	141 days	168 days	169 days	156 days	133 days	138 days

Attachment 10- DSS C&A Presentation

NISPPAC C&A Working Group Update for the Committee

May 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

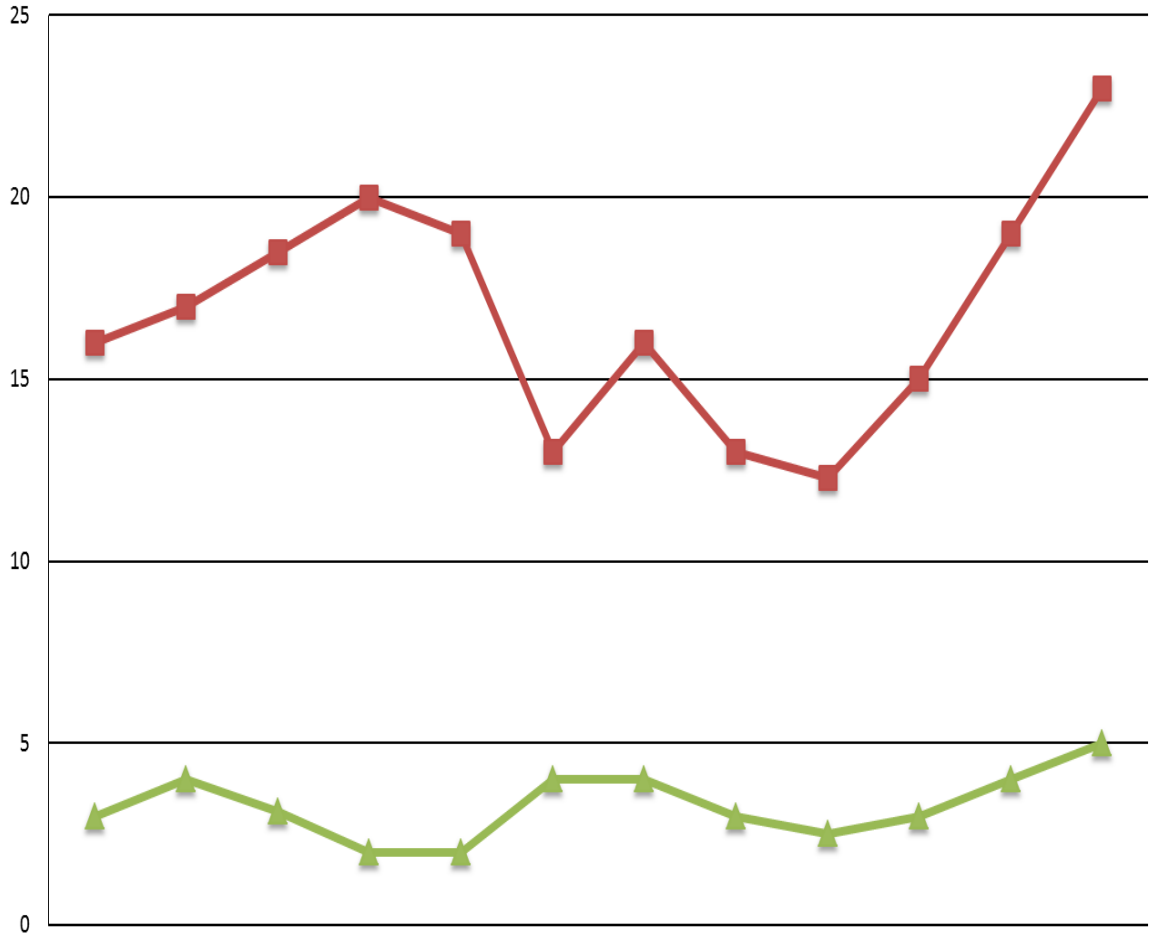
Certification & Accreditation

- 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 May 2012- April 2013



	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13
Total IATOs	140	183	179	178	193	156	145	143	153	125	158	193
Time from DSS Receipt of plans to Granting of IATOs	16	17	18	20	19	13	16	13	12	15	19	23
Industry Response Time to DSS Questions, Comments	3	4	3	2	2	4	4	3	3	3	4	5
# Second IATOs	5	10	5	11	11	14	14	15	6	4	17	15

4767 SSPs Reviewed

1946 IATOs Issued

Avg. 17 Days to Issue IATOs

1438 SATOs Processed

17 Days to Issue SATO

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

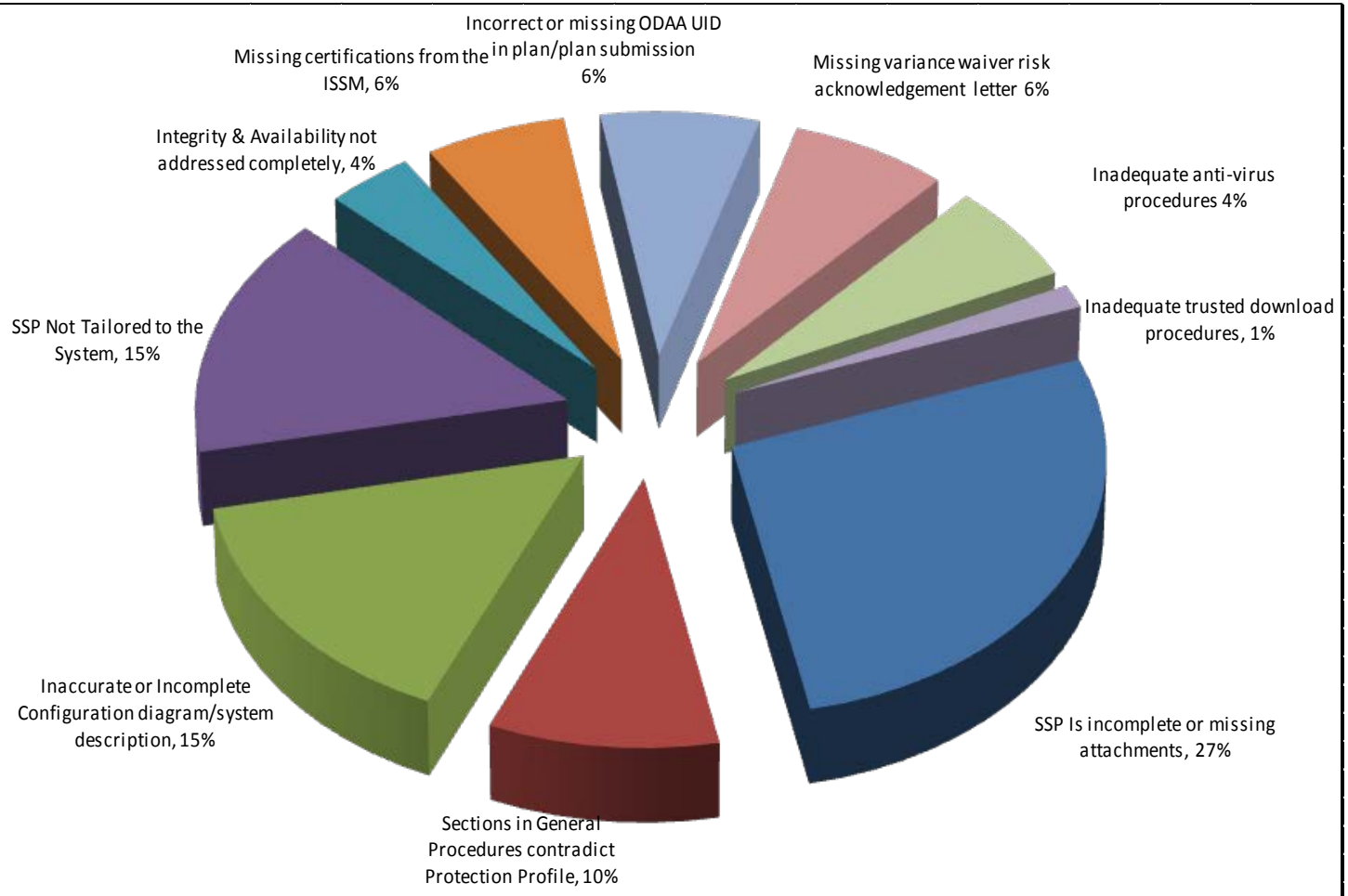
- 569 of the SSPs (15%) were granted IATO with corrections required

- 58 of the SSPs (2%) that went SATO required some level of correction prior to ATO

- 270 of the SSPs (7%) were reviewed and denied IATO (resubmitted after corrections)

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

Common Deficiencies in Security Plans from May 2012- April 2013

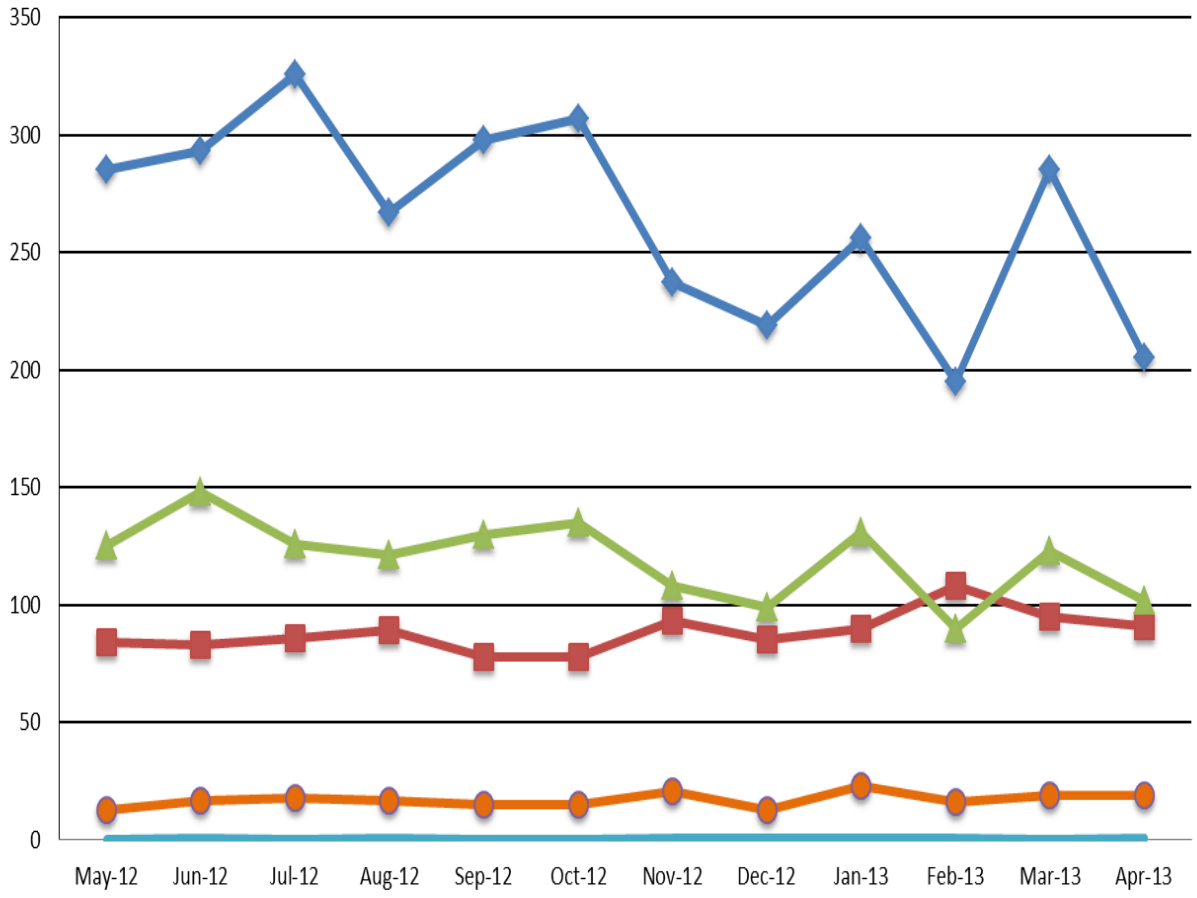


	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13
# Deficiencies	192	175	194	162	224	172	147	88	163	123	144	189
# Plans w/ Deficiencies	96	83	102	79	104	82	82	52	94	61	69	106
# Plans Reviewed	300	360	339	330	365	315	277	262	330	242	304	333
Avg Deficiency per Plan	0.64	0.49	0.57	0.49	0.61	0.55	0.53	0.34	0.49	0.51	0.47	0.57
Denials	34	24	25	25	34	19	9	15	28	21	15	21
Rejections	11	5	9	6	8	5	15	5	18	6	8	17

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 May 2012- April 2013



	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13
Total ATOs	285	293	326	267	298	307	237	219	256	195	285	205
Avg Days to Reg ATO	84	83	86	89	78	78	93	85	90	108	95	91
Total SATOs	125	148	126	121	130	135	108	99	131	90	123	102
Avg Days to SATO	13	17	18	17	15	15	21	13	23	16	19	19
% SATO's	44%	51%	39%	45%	44%	44%	46%	45%	51%	46%	43%	50%

During the Past 12 Months:

3173 ATOs

Avg 87 Days from IATO to ATO

1438 SATOs

Avg 17 days for SATOs

45% of all ATOs were SATO

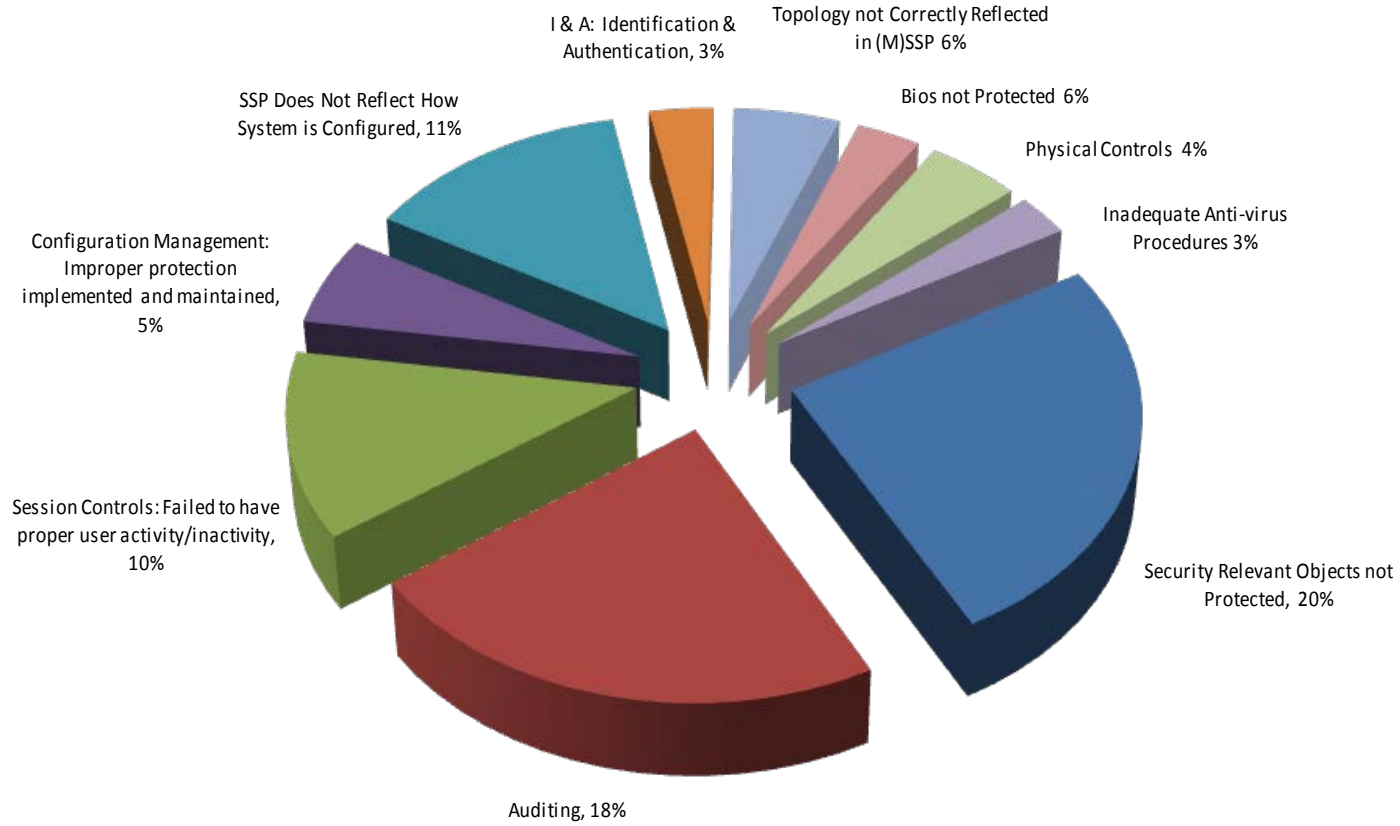
3028 ATO System Validations

- 2317 systems (77%) had no vulnerabilities identified.

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

- 51 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 May 2012- April 2013

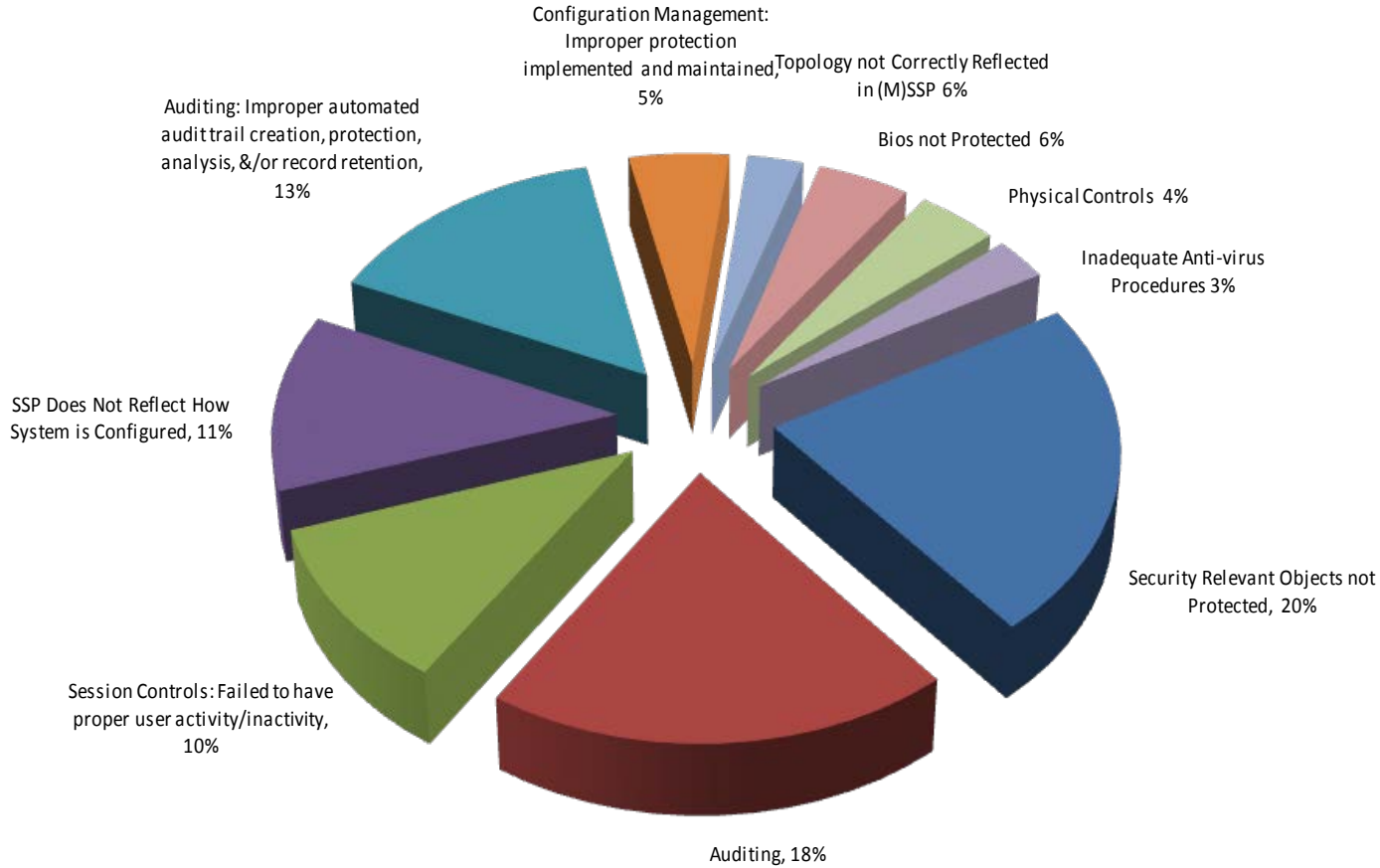


	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13
# Vulnerabilities	94	124	94	96	95	104	67	92	128	63	93	79
# Onsites w/ vulnerabilities	62	73	68	51	63	62	45	59	78	42	60	48
# Onsites	278	284	305	256	286	285	219	207	247	194	273	194
Avg Vulnerability per Onsite	0.34	0.44	0.31	0.38	0.33	0.36	0.31	0.44	0.52	0.32	0.34	0.41

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

Common Vulnerabilities found during System Validations from May 2012- April 2013



	May-12	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13
# Vulnerabilities	94	124	94	96	95	104	67	92	128	63	93	79
# Onsites w/ vulnerabilities	62	73	68	51	63	62	45	59	78	42	60	48
# Onsites	278	284	305	256	286	285	219	207	247	194	273	194
Avg Vulnerability per Onsite	0.34	0.44	0.31	0.38	0.33	0.36	0.31	0.44	0.52	0.32	0.34	0.41

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?

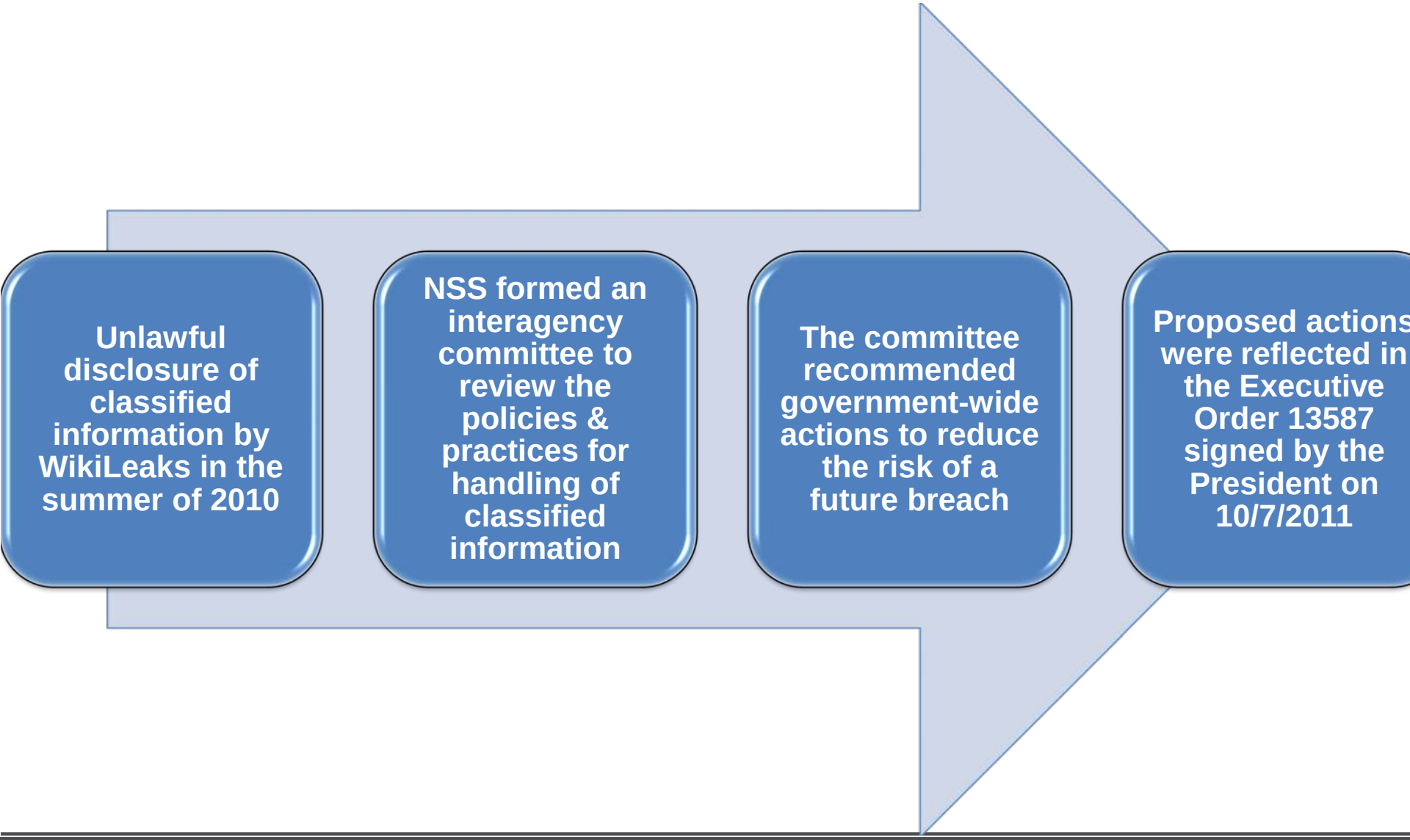
Attachment 11- EO 13587 Presentation

EO 13587 Update

Ray Sexton

Classified Information Sharing and Safeguarding Office

Background


Unlawful disclosure of classified information by WikiLeaks in the summer of 2010
NSS formed an interagency committee to review the policies & practices for handling of classified information
The committee recommended government-wide actions to reduce the risk of a future breach
Proposed actions were reflected in the Executive Order 13587 signed by the President on 10/7/2011

WikiLeaks Issues

Insider Threat Detection

Identity and Attribute–based Access Controls

Information Tagging and Access Limits

Enforcement Systems-level Security Policies

Enforcement of Network-level Data Transfer Authorization Policies

Roles and Responsibilities for Information Sharing And Protection Training

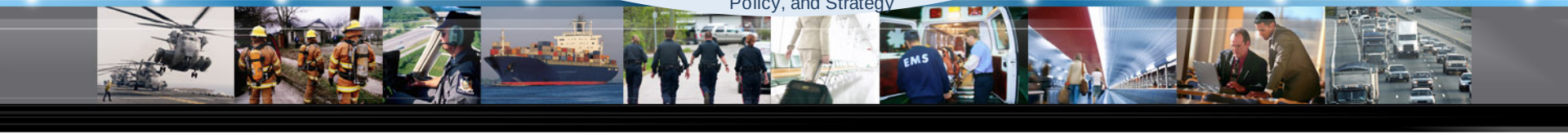
Continuous Monitoring and Immutable Audit Logs

Standards for Security Reciprocity and Information Stewardship Across Networks

Department-level Governance and Policy of People, Facilities, and Systems

Broad Whole-of-Government Standards Governing Identity, Security, and Access

Interagency Governance, Policy, and Strategy



WikiLeaks Mitigation

Governance Structure Established by EO

- A ***Senior Information Sharing and Safeguarding Steering Committee*** will have overall responsibility for fully coordinating interagency efforts and ensuring that Departments and Agencies are held accountable for implementation of information sharing and safeguarding policy and standards.

- A **Classified Information Sharing and Safeguarding Office** within Program Manager, Information Sharing Environment, will provide sustained, full-time focus on sharing and safeguarding of classified national security information. Will consult partners to ensure the consistency of policies and standards

- Senior representatives of the Department of Defense and the National Security Agency will jointly act as the **Executive Agent for Safeguarding Classified Information on Computer Networks** to develop technical safeguarding policies and standards and conduct assessments of compliance.

- An **Insider Threat Task Force** will develop a government-wide program for insider threat detection and prevention to improve protection and reduce potential vulnerabilities of classified information from exploitation, compromise or other unauthorized disclosure.

Responsibilities of Departments & Agencies

Agencies bear the primary responsibility for sharing and safeguarding classified information

- Designate a Senior Official
- Implement an Insider Threat Program
- Report to the Steering Committee
- Perform Self-Assessments of Compliance

Areas of Focus & Ongoing Improvement

- Enhancing control of removable media
- Identity Management; including reducing user anonymity and increasing user attribution
- Building a more robust insider threat program
- Enhancing access controls
- Improving enterprise audit capabilities

WikkiLeaks Lessons Learned

Then	Since Then	Now
Trusted insider leaked classified information		Same
Immediate actions to control communications – approved talking points, FAQ's, and engagement directions with Hill and media via PAO's		Same – reinforce directions and controls
Unclear leadership/governance, no single group in charge,	EO 13587 established the SISSSC, but it took a full year	This issue is within scope of the EO and the SISSSC, use it to lead the response effort rather than inventing another new group
Unclear facts about incident – especially weaknesses and responses, leadership direction to focus on systemic issues and structural reforms – not tactical, reactive Wikileaks Whack-a-Mole	SME team formed to assess systemic weaknesses and recommended strategic, phased response that became the Steering Committee priorities, EO 13587 established NITTF, EA for Safeguarding and CISSO, but it took a full year	Same approach, except SME teams already exist from EO 13587 – NITTF, EA for Safeguarding (tied to CNSS) and CISSO – use them to identify weaknesses, assess mitigation options (costs, benefits, risks, probability of success, and timeframes for implementation), and develop recommendations, again do not overreact to specifics of this individual incident – focus on strategic, systemic improvements

WikkiLeaks Lessons Learned

Then	Since Then	Now
Need to protect integrity of investigation separate from and parallel to response assessment, planning, and implementation	The investigation of Bradley Manning proceeded in parallel with the structural reforms	Same approach, do not interfere with investigation but also do not wait for investigation to finish before beginning response effort, proceed with both in parallel
Lacked coherent approach to align priorities, resources, deadlines, and performance metrics	Established priorities, budget data request, IOC/FOC definitions, agency agreed completion dates, and performance metrics/process (KISSIs), but it took a full year after the EO was signed	Leverage the priority setting, resource alignment, deadline setting and performance metrics framework to reassess current plans and revise them to align with new priorities (e.g. acceleration of current efforts and/or addition of new ones)
National Strategy for Sharing guided post-911 CT and homeland security efforts	National Strategy for Information Sharing and Safeguarding expanded scope to intentionally include post-Wikileaks improvements	Leverage implementation of the NSISS to integrate governance, priorities and progress across fabrics
Need to protect integrity of investigation separate from and parallel to response assessment, planning, and implementation	The investigation of Bradley Manning proceeded in parallel with the structural reforms	Same approach, do not interfere with investigation but also do not wait for investigation to finish before beginning response effort, proceed with both in parallel

Questions?