Minutes of the
National Industrial Security Program Policy Advisory Committee (NISPPAC)
Meeting on November 14, 2013

The NISPPAC held its 46th meeting on Thursday, November 14, 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 January 29, 2014.

I. Welcome and Administrative Matters

Mr. Fitzpatrick welcomed the attendees, and after introductions, reminded everyone that NISPPAC meetings are recorded events. He welcomed two new industry representatives, Bill Davidson and Phil Robinson, and then acknowledged Tony Ingenito as the new Spokesperson for industry. He then asked Greg Pannoni, the NISPPAC Designated Federal Official (DFO), to review the Committee's old business. See Attachment 1 for a list of those in attendance.

II. Old Business

Mr. Pannoni reviewed the two Action Items from the July 17, 2013 NISPPAC meeting. He reported that the briefing to update the Committee on Executive Order (E.O.) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," would be tabled until the March 19, 2014 meeting. See Attachment 2 for a list of Action Items.)

III. Reports and Updates

(A) Department of Defense (DoD) Update:

Steve Lewis, Office of the Undersecretary of Defense for Intelligence (OUSD(I)) updated the progress on the conforming change to the National Industrial Security Program Operating Manual (NISPOM) , and noted that it will implement the minimum standards for insider threat promulgated a year ago by the President, and levy those requirements on industry. In addition, he advised that it addresses the reporting requirements under Section 941 of the National Defense Authorization Act (NDAA), which requires the Secretary of Defense to levy reporting requirements for industry to report intrusions into unclassified systems in which DoD information is successfully exfiltrated from a contractor's network or information system. He noted that the conforming change is in the DoD formal coordination process, and that he expected this action to be completed in approximately 90 days, and then it would be sent to the Cognizant Security Authorities (CSA) for completion of their formal coordination process. He then provided an update on electronic fingerprint submissions, a requirement for all industrial contractors under the security cognizance of the Defense Security Service (DSS). He reminded the Committee that the primary reason for DoD's electronic fingerprint submission requirement, as a part of the personnel security clearance (PCL) process, was necessitated approximately three

years ago as a result of the roughly 60% rejection rate levied by the Office of Personnel Management (OPM) due to missing or illegible fingerprints. Mr. Lewis noted that when fingerprints are submitted electronically there is, within 24-48 hours, a response that indicates whether there is an issue with the individual, and this response then generates a rejection or denial for the granting of interim access to classified information at the SECRET level.

(B) Defense Security Service (DSS) Update:

Stan Sims, DSS Director, reviewed the recent government and industry stakeholders' meetings and noted that there was a general interest in a review of DSS' oversight processes and procedures and specific interest on the PCL process. He added there was a significant discussion on what should be done to tighten the PCL process, as well as a general agreement that government representatives came away with a much clearer understanding of what DSS does in support of their contracts pertinent to PCLs. He advised that the primary concern raised by industry stakeholders was DSS's appraisal of the long-term effects the recent government shutdown would have on their continued ability to support industry's needs with regards to both the PCL process and classified information systems accreditations. He noted that the shutdown resulted in an approximately 29-day delay on PCL processing, and that vulnerability assessments were postponed, and would be rescheduled with the most critical requirements to be addressed first. Mr. Sims advised that 93 classified systems, 48 facility security clearances, and 136 vulnerability assessments were delayed in the accreditation process, because of the shutdown.

Mr. Sims noted that there were discussions at both stakeholder meetings of the on-going DoD reviews regarding the Washington Naval Yard shootings, and concluded that where these reviews may result in proposed changes to the government PCL and facility/installation access processes, he did not think those changes would impact industry since it already has procedures that are established in the NISPOM. He suggested that there will likely be enhanced adverse information reporting requirements levied on both government and industry. He mentioned the continuing discussions on the electronic fingerprinting process, as well as automation of the DoD Contract Security Classification Specification (DD Form 254). He noted that DSS is seeking additional funding for the DD Form 254 project, which they hope to complete within the next 18 months. He updated the progress in developing the Industrial Security Field Operations Process Manual, and noted that it will be published by the end of November and effective six months later. Mr. Sims spoke to the deployment of a new Facility Security Officer's (FSO) modular toolkit, and explained that it will capture all processes and procedures required by the NISPOM, and would be accessible through their website. In response to a question from Michael Hawk, Department of State,, regarding the latest direction from the Office of the Director of National Intelligence (ODNI) on PCL assessments and levels, up to and including SCI, Mr. Sims stated that all parties should expect guidance to be forthcoming, and that DSS must first review and update its own PCL posture prior to the issuance of any procedural changes to other entities. In addition, he noted that while DSS is uncertain exactly what form such guidance will ultimately take; he expected some form of government agency adaptation to the assessment principles outlined by the ODNI, as well as some specific instructions for industry, perhaps either through an Industrial Security Letter or as additions on the DSS website.

The Chair provided follow up information related to Mr. Sims' comment regarding the concurrent reviews in progress as a result of the recent Navy Yard incident, explaining that all such reviews address PCL issues, including access to classified information, access to facilities, and status within workforces and at different levels within DoD. He noted that three reviews were being conducted by DoD, and a fourth under the authority of the Office of Management and Budget (OMB). He explained that the DoD reviews were nearing completion, whereas the OMB's review, which includes ISOO because of its NISP oversight responsibilities, is just now getting under way. In addition, he pointed out that as we learn the results of these reviews it should be understood that matters relating to government contractors were purposefully included in the scope of the government-wide reviews, so the composition of the panel not only included a cross section of Agency representatives, but also ISOO and those agencies that have an active and ongoing interest in the NISP. Finally, he reminded the Committee that the revisions to 32 Code of Federal Regulations (CFR), Part 2004, the NISP implementing directive, will be published in the Federal Register which will ensure that the revisions are open for review and comment.

(C) Combined Industry Presentation:

Tony Ingenito, Industry Spokesperson, began his presentation (See Attachment 3) by acknowledging the leadership and support of Fred Riccardi and Shawn Daley during their four-year tenure on the NISPPAC. He then referenced issues related to insider threat, and pointed out industries involvement in the implementation of insider threat policy. He noted industry's concern regarding the impact of the enhancements required under E.O. 13587, and how the directive will impact its implementation. In addition, he highlighted industry's concerns regarding the control of removable media, and the impact of the OUSDI memorandum requiring two-person integrity, on both the Sensitive Compartmented Information and Special Access Program communities. He advised that if they are applied, these policies will have major impacts on both contract affordability and scheduling. The Chair suggested that industry representatives meet with the CSAs and other DoD officials to discover what actions might be taken so that specific problem identification can be realized, and industry's concerns addressed. Next, Mr. Ingenito addressed industries comfort with the current status of the implementation of the E.O. on Controlled Unclassified Information (CUI). The Chair noted that ISOO plans to publish the CUI Implementer via a CFR issuance early in the New Year, which would initiate the formal interagency review process, followed by a public review and comment period. He noted that the CUI implementer is not significantly different than when industry last reviewed it; but had been restructured to address federal regulatory requirements. The Chair noted that the CUI office would provide an update on its processes at the next meeting. The Chair described the remainder of the regulatory process and promised a comment resolution and revision phase, followed by a completed draft later which will be made available for public review and comment.

Mr. Ingenito continued his report by expressing industry concerns with possible ramifications resulting from the Enhanced Security Clearance Act (ESCA) of 2013, and in particular how industry might be impacted by such issues as adding social media to the process for gathering clearance investigative information, as well as the requirement for agencies to provide complete clearance lists to OPM. The Chair responded that there is indeed a lot of interesting legislative language on the topic of security clearances, and that perhaps it would be helpful between now

and the next meeting for the Personnel Security Clearance Working Group (PCLWG) to spend some time determining what all that language actually means. In addition, he suggested that since it is probable that some of the new requirements will likely be applied to the NDAA as well, the PCLWG should provide any of those new updates regarding issues of interest to industry. He suggested that having a single database containing all this information would be helpful at any time we surface reciprocity issues. However, he cautioned against finalizing any new security clearance dialogue until the 120-day review is complete. Lisa Loss, OPM, added that OPM was not responsible for recommending updates to the ESCA, but they do plan to work with Congress on any technical issues that it might find helpful. Mr. Ingenito reminded the Committee that in the past industry has expressed some concerns with PCL reciprocity issues related to the RAPID Gate program, and is anxiously awaiting an Inspector General's report, which may address the key issue governing this question. He also mentioned that industry has recently been able to submit comments to the latest draft of the Office of the Designated Approval Authority's Process Manual, and that they are beginning to see residuals from the Special Actions Programs Working Group's efforts as they flow to the Program Security Officer and Contractor Program Security Officer levels.

(D) Personnel Clearance Working Group (PCLWG) Report:

Lisa Loss, OPM, updated timeliness performance metrics for industry PCL submissions, investigations, and adjudications (see Attachment 4). She explained the FY 2013 timeliness metrics for initial investigations and periodic reinvestigations (PRs) and noted that their goal of 74 days for completing initial investigations was met for all four quarters. However, she noted that the Top Secret (TS) investigations goal (114-days) was only met in the last three quarters due to an especially high volume of PRs that were submitted in the first quarter. She explained that initial investigations have priority over PRs, and that after the first quarter, the timeliness of the initial TS investigations declined. She noted that the timeliness goal for initial Secret and Confidential (S/C) investigations were met in all four quarters of FY13, and that TS re-investigation goals were met in all but the second quarter. She presented the monthly timeliness metrics for the initial TS, S/C, and TS PRs, noting that all ended the FY having achieved their timeliness goals. She suggested that there was a real challenge in keeping to the 150-day goal for TS PRs simply because of the immense volume coupled with the need to manage initial investigations. Ms. Loss credited the failure to meet the goal in the month of September as resulting from a combination of the earlier furloughs and the government shutdown, and postulated that these numbers could increase dramatically in future measurements. Mr. Sims surmised that the electronic fingerprint requirement will have an impact on DSS's processing procedures since fingerprints must now be returned prior to initiating the clearance process.

Dan Purtill, Deputy Director of the DoD Consolidated Adjudication Facility (CAF), continued the PCLWG's report with an update of the CAF's industry adjudications' program (see Attachment 5). He explained that while the CAF has a considerable backlog in industrial adjudications, they have completed their functional consolidation and have subsequently base-lined all metrics. He stated that progress has been intermittent as the CAF has, along with everyone else, been impacted by sequestration and furloughs. However, he noted that since September they have made progress by implementing some limited use of overtime, thus alleviating some of the burden imposed on their diminished staffing level. He stated that they

are now digging deeply into the backlog, and have reversed the previous trend, and are beginning to achieve measurable gains. In addition, he noted that while they are well below Intelligence Reform and Terrorism Prevention Act (IRTPA) timeliness requirements (90% efficiency in adjudicating cases in 20 days or less) they anticipate metrics to be erratic as they continue to reduce the backlog and some of the old caseload. He noted that they continue to make progress towards blending the former DISCO and DOHA adjudicators into a single division within the CAF, having now located them in the same facility and onto a common computer network. Finally, he assessed that the elimination of the industrial backlog is now estimated at two years. Mr. Purtill then responded to several questions from membership: To the question regarding, he explained that while industrial cases constitute the vast majority of the backlog, that it is easier to shift work between the adjudicators who handle government cases than it is for those who work industry cases, since they operate under slightly different rules, which takes a little more effort to get the staff properly trained and comfortable with those differences. To Mr. Dodson, Industry, regarding whether the current ODNI security clearance review procedures, could cause some cases to fall out of the backlog, Mr. Purtill noted that while such a possibility exists, and that when this kind of initiative is undertaken it is likely to result in some clearances being limited at the S level, while others are raised to the TS level, and that in either case, the CAF's workload will increase, which will in turn impact the elimination of the backlog. To Jim Shamess, MOU Representative, regarding whether the CAF uses a tool to measure process effectiveness, Mr. Purtill noted that while they have not formally established performance effectiveness metrics, they do perform a quality review of a percentage of all adjudicated cases. He described quality review efforts as an internal process that examines between one and five percent of the cases, based on the division and experience of the personnel performing the tasks. In addition, he noted that new adjudicators' work is 100% reviewed until they are fully certified and working independently. Further, these quality reviews cover such items as whether the databases are being updated correctly and properly annotated. Also, the CAF has a quality assessments cell of approximately 12 people who perform these evaluations full-time. In response to a follow-up question from Mr. Dodson as to whether there was any kind of feedback loop that accesses the percentage of people who were cleared by the CAF but who subsequently had their clearance revoked for some kind of suitability issue, and if so, are we capable of determining if the CAF's process failed to identify these issues during the initial adjudication process, Mr. Purtill noted that while the CAF typically does not track such data it could produce such a metric, and pointed out that they always perform a review of prior investigations whenever a negative incident comes to light, and that this aspect is a part of the quality assessment process, and that any adverse action would generate a second-level review. Bill Davidson, Industry, asked if such a review would automatically address the investigative part of the process, and would OPM get involved so that they can re-examine their process, to which Mr. Purtill advised that this was dependent upon whether or not the issue required an investigation, and noted that if the incident was a failed drug test, then they normally would not be required to run any field leads, and therefore we would not loop into the OPM process. The Chair suggested that the PCLWG devise a way to characterize these quality reviews that would answer questions regarding the volume of the workload, their overall success rate, as well a description of the manner of redress or adverse actions. Mr. Shamess noted that the recent stakeholder's meeting provoked a discussion as to why we cannot get adverse information on a person prior to a move from one company to another, and that knowing about adverse information is critical to making a proper decision. Mr. Dodson added that there is a real challenge between working with the government

personnel system verses the different privacy laws in each state, and that gathering such data could impact legal and privacy boundaries, and necessitate the discovery of negative information at a later date. Mr. Sims suggested that in view of the fact that said contractor has signed agreements that permit the government to collect and use their personal information to determine their viability for a PCL and subsequent access, that they have the authority to transfer adverse information to their personnel security database so that they can identify any information that would impact their clearance and in the same instance avoid violations of privacy rights, since there is no expectation of privacy when it comes to incidents or actions that could impact an individual's privilege to obtain and/or maintain a PCL. In addition, he suggested that the Chair ask the PCLWG to devise some instructions relative to such a procedure, which we would then refine and subsequently staff through the legal community. Ms. Ruth Olsen, ODNI, said she would welcome the opportunity to brief the Committee on ODNI's plan of continuous evaluation, in part so as to prevent the NISPPAC from covering the same ground and also in the hope that these discussions might open new ground for the ODNI community. The Chair agreed, noting there are a number of NISPPAC members who are also involved in the OMB directed120-day review process, and pointed out that everyone is wrestling with the tension between what information can be shared, and whether its utility in one process can actually create vulnerabilities in another. That is, perhaps the utility in making decisions about whether somebody who has a clearance should also have facility access, or computer access, while at the same time there are vulnerabilities when there is a private provider of the information versus the government making its decisions on its own authority. In addition, he noted that there are systemic examples, the recent Navy Yard case being one, that these dots ought to be connected, and that the system must surely be built in a way to accomplish that objective, even as we know that it is not at present designed that way. The Chair suggested that the NISPPAC should provide input to the OMB activity regarding industry's specific concerns; since we certainly have a desire to be more helpful in the reciprocity process, which then will require a legal framework as well. He added that it is suitable for discussion by this body, and we welcome a look at the plans are for continuous evaluation in the future. Finally, he assured the Committee that ISOO will certainly report whenever there are findings pertinent to any other clearance-related reviews.

Ms. Hickman, DSS, reviewed the Electronic Questionnaires for Investigations Processing (e-QIP) reject metrics from both DSS and OPM (see Attachment 6). She stated that the reject rates continue to decrease, and that both DSS and OPM are pleased with the progress and the quality of the investigations submissions. She explained that the primary reason for the rejects continues to be the missing fingerprint cards, and that there is a requirement that all fingerprints must be submitted electronically by the end of December 2013. She reminded everyone that DSS has posted on its website the five options from which industry might choose for electronic fingerprint submission. She noted that the Defense Manpower Data Center maintains a list on its website of the third party vendors that can provide fingerprint capture services, and that many of them are also approved as Federal Bureau of Investigation (FBI) service providers. She suggested that another viable option for industry is for companies who have excess electronic fingerprint capture capability to share that capability with others, and that larger contractors might reach out to the smaller companies with offers of fingerprinting assistance wherever possible. She recommended that our government partners who have electronic fingerprint capture equipment should consider reaching out to their contractor personnel. She reminded the Committee of the impacts of furlough and sequestration that would impact the FY 2014 funding authorization and

that necessitated the temporary halt in the submission of personal security investigations to OPM, and which created an almost one-month backlog (approximately 13,500 cases) . She reminded everyone that PSMO processes its investigations on a first in, first out basis, notwithstanding compelling need requests, which must be kept to the absolute minimum. Ms. Hickman explained that the PSMO has suspended notifications of overdue PRs, except in the case of those for the key management personnel, as they are tied to facility and interim clearances. Mr. Sims then added that in light of the numerous recent and/or pending process changes, he wanted to assure everyone that DSS will be working closely with the OUSDI and ODNI communities to make these change requirements occur as seamlessly as possible, and he asked that everyone visit the DSS website frequently, or call with any questions.

Mr. Mark Pekrul, DOE, reported that DOE's initiation and adjudication timeliness, as well as the TS, S and C security clearance decisions all remain within prescribed timeframes, and that TS PRs also remain within acceptable levels (see Attachment 7).

Ms. Valerie Kerben, NRC, reported that since the last updates timeliness goals for adjudication have been achieved (see Attachment 8). She pointed out that submissions timeliness, largely as a result of their prescreening process, will inevitably remain above the desired 14 days. She reminded the Committee that NRC's latest metrics show that overall end-to-end timeliness in each category was reduced for each quarter, and that for some as yet unexplained reason, PR timeliness increased.

The Chair reminded the membership that the PCLWG seeks to characterize the entire NISP experience, and that while that is greater or lesser in some areas, it is nevertheless important to understand that the standards apply equally to all. Also, he explained that due to the impacts of the recent government shutdown, the Intelligence Community (IC), based largely on their collection methodology, was unable to present the metrics they normally report at this forum, but that we hope to welcome them back at the next meeting.

(E) Certification and Accreditation Working Group (C&AWG) Report:

Tracy Brown, DSS, provided the C&AWG report (see Attachment 9), and reminded the Committee that DSS is the primary government entity responsible for approving contractor information systems to process classified information. She noted that processing times for reviewing System Security Plans (SSP) and performance metrics for onsite validation visits had improved. She then explained that the working group's initiatives included: Windows 7 and Windows 8 configuration baseline standards,(released in July 2013); the Industrial Security Field Operations Process Manual, soon to be posted on the DSS website; a continuing review of the Security Content Automation Protocol tool to determine the feasibility of leveraging the tool for systems compliance; and an ongoing assessment of the requirements for tracking vulnerabilities recorded in accordance with risks associated with classified information reporting of common discrepancies. She noted that in FY 13 DSS reviewed over 3,600 SSPs, which resulted in the issue of either an Interim Approval to Operate (IATO) or an immediate Approval To Operate (ATO) within 20 days. She cautioned the Committee that because of the impact of the recent furlough the timelines might temporarily increase to as much as 30 days. She reported that only 9% of the SSPs were rejected or otherwise denied accreditation; with the top three reasons being

incomplete or missing attachments, issues with configuration diagrams, and plans not tailored to the specific system. She reported that during the past year they performed over 2,900 on-site validations, and that approximately 23% had minor errors that required immediate corrections prior to issuance of an ATO, and that the average time required to process from issue of an IATO to an ATO was 96 days, with only 2% of all reviewed systems requiring a revisit prior to the issue of the ATO. She explained that during onsite validations, when they detect vulnerabilities and improperly protected security-relevant objects, that are unique to the specific facility, they stop and provide system administrator education, and grant permission to apply immediate corrections. She reported that by doing business in this manner they are experiencing high rates of effective and timely SSP updates and validations, as the overarching objective is to issue as many ATOs as possible. She explained that DSS's cyber security readiness inspection program is an enormous undertaking that dramatically impacts their workload, so everyone should expect to incur a minimum timeliness increase. She further explained that the Office of Designated Approving Authority's (ODAA) Business Management System which will automate and streamline C&A activities is scheduled to be online in FY 2014, and that ODAA will post notifications on the intranet, Facebook, and Twitter sites, and in the monthly FSO newsletter, as well as deploy several system training products, tutorials, and job aids.

The Chair then reminded everyone in attendance that all NISPPAC working groups meet between the regular Committee meetings, where they collate data, raise issues, and work on new initiatives that are subsequently prepared and presented to the membership. He encouraged everyone to raise observations or pose questions through the ISOO staff, so that they can be directed to the attention of the appropriate working group.

IV. New Business

E.O. 13636 & Presidential Policy Directive (PPD) 21 Overview:

The Chair reminded the Committee that the primary reason for their existence is directly linked to the unique partnership they share as government and industry representatives engaged in the activities of the cleared contractor workforce. He described the nature of this activity as bi-directional, as it is centered in both access to accredited classified national security information systems, and at the same time immersed in the world of cyber security and critical infrastructure. He noted that we recognize that there are longstanding structural ways that security requirements are promulgated for the purpose of ensuring security in the cleared contractor space, and that we play an important role as members of an industrial society beyond whose duties are merely the responsibilities associated with cleared industry. He added that we are poised at the intersection where these two worlds are rapidly merging, and that there are significant initiatives that we must adapt, and that we must quickly come to understand where they overlap, so that we can prepare to complete the coordination necessary to facilitate the implementation of security-oriented executive orders and policy directives. He introduced Jeanette Manfra, Deputy Director of the Department of Homeland Security's (DHS) E.O.-PPD Integrated Task Force, who would familiarize the Committee with the framework and contents of E.O.13636, "Improving Critical Infrastructure Cybersecurity," and Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience."

Ms. Manfra pointing out that this initiative is an Executive Branch priority, and that her team has developed the roles, responsibilities, and strategies, that ensure we meet the governmental and sociological mergence of the cyber security and critical infrastructure. She described how E.O. 13636 represented an effort to push the boundaries of the federal government's capabilities in working with existing authorities towards the advancement of critical infrastructure and cyber security, even as PPD 21 represented an effort to address all hazards that could have a debilitating impact on national security, economic stability, and public health and safety. She pointed out that both the E.O. and PPD 21 were issued simultaneously, because we wanted to bring the physical security and cyber security disciplines together, both within government and industry, and among our state and local partners. She explained that the E.O. required DHS to initiate a voluntary program to partner with mature cyber security practitioners, to help implement the cyber security requirements across the critical infrastructure, and that the federal government will also be looking at how we adapt the framework accordingly. She pointed out some of the other deliverables are concerned with expediting private sector security clearances. She contrasted DHS's authority to grant private sector clearances to critical infrastructure owners and operators, from the traditional contract relationship where the contractor gets a security clearance by being part of a contract that requires access to classified information, noting that under their concept, they need to be able to have classified conversations within the private sector, and so either persons that work out in the field, critical infrastructure owners and operators, or government employees can nominate industry critical infrastructure personnel for these clearances, that would then go through the standard vetting process. She noted that this unique program had been reenergized, and DHS can now expedite standard clearances at both the TS and S levels. She mentioned other deliverables that were concerned with rapidly declassifying classified information so that it can be disseminated to the users that need it to facilitate action. She detailed a requirement to put in place a process that assesses whether or not such information was of any value to the receiving party(s), and would include not only both classified and unclassified information, but even broader strategic briefings that need to be shared as well. She highlighted that the final part of the E.O concerned the protection of privacy, civil rights, and civil liberties, and noted the work that is being evaluated by our privacy, civil rights, and civil liberties officials at DHS and at seven other agencies. She explained that these reports are not only privacy impact assessments, but are also broader evaluations of potential privacy, civil rights, and civil liberties impacts. She noted that there will be other reports concerned specifically with incentives for adopting the cyber security framework, as well as potential procurement incentives for adopting this framework that can be found on the Department of the Treasury, DOC, DHS, and White House websites.

Ms. Manfra explained that after September 2011 there was a renewed impetus for gathering entities into the critical infrastructure community, so that DHS could identify and understand our vulnerabilities, and then to work on mitigating those vulnerabilities, and devise strategies for better identification and protection of critical infrastructure assets. She noted that the focus on critical infrastructure, security, and resilience had shifted slightly, especially in the federal government, from one of protection to security and resilience, and was now focusing on a broader life cycle that included protection and resilience in both our cyber and our physical protection systems. She explained the new focus was the genesis for creation of the "National Infrastructure Protection Plan (NIPP) 2013, "Partnering for Critical Infrastructure Security and Resilience," that required the federal government to work with state, local, tribal, territorial, and

industry partners to identify our priorities, and to develop guiding principles to achieve them. She advocated clearly enunciating those guiding principles from the beginning, working at every turn to maintain them throughout the planning and implementation stages of the process. She noted that the only way to achieve the security and resilience goals was through a collaborative, open, and transparent partnership and a joint commitment of both government and the private sector. She explained that the NIPP contains five articulated goals, that are broad in scope, that aim to affirm the desire for a national level focus on advance planning and mitigation, and an ongoing program of enhanced coordination between the planning groups and the responders. She noted that the government has refocused its continuous learning efforts through actionable and relevant information-sharing, to better understand interdependencies across sectors, the government and private sector domains, and to delineate our common dependence on critical functions and services such as communications, energy, water, and transportation in an increasingly cyber-dependent nation. She noted efforts at international collaboration, particularly in cyber security, and advocated that we must work to harmonize standards, because of their impact on multinational businesses, and on issues having multi-faceted approaches. She reminded the Committee that the NIPP was submitted to the White House in early November, and that they were working vigorously to make as many of the documents outlined in both the E.O. and PPD 21 as publically available as possible. The Chair asked if the framework, which may or may not align with requirements and principles in the NISP, would then spawn the development of best practices and standards to achieve the desired protection objectives. Ms. Manfra responded that no new standards were being developed and that the framework primarily addressed existing standards and best practices. The Chair explained that within the space in which many of us traditionally work, we decide what things need protection more than others, and that those things that need protection are often identified because they relate to or contain information of this type, asked if that was the methodology used by the framework to decide which assets need which kinds of protection. Ms. Mantra responded that indeed the framework is cyber security focused, but that its present objective is to guide users through a discovery of what are the questions they should be asking. She noted that what is being done now is to work with industry volunteers who are studying IT sector guidance to create implementation procedures based on the framework. Mike Witt, industry, informed the Chair that the vast majority of the industry personnel in attendance here today are members of the Defense Industrial Base Sector Coordinating Council (DIBSCC), whose objective is to improve the sharing and reliability of public and private threat and hazard information, and which meets on a regular basis in direct support of this initiative. He added that one of the DISSCC's most significant accomplishments to the partnership is the Defense Security Information Exchange through which the members share cyber threat information, in a non-attribution environment before the government ever informs the industrial community of such a threat's existence. Ms. Manfra confirmed that the DIBSCC provided significant support in all the initiatives that have has been discussed.

V. General Open Forum/Discussion

The Chair opened the floor for comments on any topic not previously posted to the agenda. Richard Donovan, DOE, informed the attendees that his agency is currently involved in writing a series of technical standards that deal with asset protection, and that one of the standards nearing completion and that will likely be out for agency coordination within the next month is on the conduct of self-assessments. He noted that when that standard enters the coordination period it

will be accompanied by a website containing a number of tools that could be used to conduct reviews of classified material and other physical security developments. He advised that anyone having an interest in being a participant in their joint government/ contractor working groups for this project or otherwise have questions related to the project to contact him, and he will guide them to the correct forum.

VI. Closing Remarks and Adjournment

The Chair reminded everyone that the next NISPPAC meeting is scheduled for March 19, 2014. He noted that ISOO will partner with the National Classification management Society (NCMS) to host the June NISPPAC meeting during their annual seminar at National Harbor in Maryland. He thanked Mr. Leonard Moss, NCMS, for helping us accommodate that, and for holding the conference locally. He added that the budget circumstance for the Federal government, and the National Archives and Records Administration (NARA), remains as it was in FY 2013, so our inability to reimburse for travel and other costs will continue as before. The Chair noted that a teleconferencing capability will be available for anyone who cannot attend in person. And that he was grateful to our out of town industry representatives who came to today's meeting by their own means. Lastly, he noted the target date for the third meeting in 2014 is November 19th at NARA. There being no further business, the meeting adjourned at 12:04 p.m.

Attachment #1

Attachment 1

NISPPAC MEETING ATTENDEES/ABSENTEES

The following individuals were present at the November 14, 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
• Ryan McCausland	Department of the Air Force	Member
• Jeffery Bearor	Department of the Navy	Member
• Dennis Hanratty	National Security Agency	Member
• Eric Dorsey	Department of Commerce	Member
• Richard Donovan	Department of Energy	Member
• Anna Harrison	Department of Justice	Member
• Ruth Olsen	Office of the Director of National Intelligence	Member
• Dan Cardenas	Nuclear Regulatory Commission	Member
• Anthony Ingenito	Industry	Member
• William Davidson	Industry	Member
• Richard Graham	Industry	Member
• Phillip Robinson	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
• Christal Fulton	Department of Homeland Security	Alternate
• Lisa Desmond	Department of the Army	Alternate
• Michael Hawk	Department of State	Alternate
• Mark Pekrul	Department of Energy	Alternate/Presenter
• Steve Lewis	Department of Defense	Alternate/Presenter
• Valerie Kerben	Nuclear Regulatory Commission	Alternate/Presenter
• Kathleen Branch	Defense Security Service	Alternate
• George Ladner	Central Intelligence Agency	Alternate
• Steve Peyton	National Aeronautics & Space Administration	Alternate
• Richard Hohman	Office of the Director of National Intelligence	Alternate
• Lisa Loss	Office of Personnel Management	Presenter
• Dan Purtill	Department of Defense	Presenter
• Laura Hickman	Defense Security Service	Presenter
• Tracy Brown	Defense Security Service	Presenter
• Jeanette Manfra	Department of Homeland Security	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
• Christy Wilder	Office of the Director of National Intelligence	Attendee
• Jay Buffington	Defense Security Service	Attendee
• Natasha Wright	Defense Security Service	Attendee
• Keith Minard	Defense Security Service	Attendee
• Jeff Moon	National Security Agency	Attendee
• Brent Younger	Department of the Air Force	Attendee
• Amy Roundtree	Nuclear Regulatory Commission	Attendee
• Drew Pretzello	Nuclear Regulatory Commission	Attendee*
• Mitch Lawrence	Industry	Attendee
• Jim Euton	Industry	Attendee
• Steve Abounader	Industry	Attendee
• Michelle Sutphin	Industry	Attendee
• Aprille Abbott	Industry	Attendee
• Vince Jarvie	Industry	Attendee
• Shawn Daley	Industry	Attendee
• Richard Weaver	Industry	Attendee
• David Best	Information Security Oversight Office	Staff
• Alegra Woodard	Information Security Oversight Office	Staff
• Robert Tringali	Information Security Oversight Office	Staff
• Joseph Taylor	Information Security Oversight Office	Staff

* Attended via teleconferencing

Attachment #2

ACTION ITEMS FROM NOVEMBER 14, 2013 NISPPAC MEETING.

1) The PM/ISC update on the implementation of Executive Order 13587, which was postponed from the November 2013 meeting, will be presented at the March 2014 meeting.

2) The CUI office will provide an update to the NISPPAC on its implementation efforts.

3) The PCL Working Group will :

    a. Identify issues and concerns for industry relating to on-going Federal Government efforts to change laws and regulations regarding personnel security clearance processes.

    b. Characterize the size and scope of issues related to personnel security clearance investigations for industry personnel; contrasting the overall impact of revocation and adverse actions on the process of adjudicating the candidate for a clearance.

4) ODNI will provide a presentation on their plan for a continuous evaluation program, so as to address issues and concerns from industry into the priorities they recommend to OMB.

Attachment #3

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

Industry

14 November 2013

Outline

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

National Industrial Security Program

Policy Advisory Committee Industry Members

Members	Company	Term Expires
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
Bill Davidson	Davidson Associates LLC	2017
Phil Robinson	CGI Federal	2017

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

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

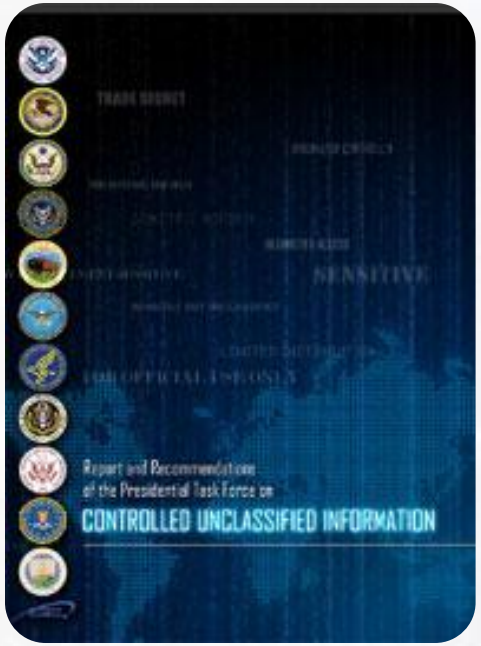
Executive Order #13556

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

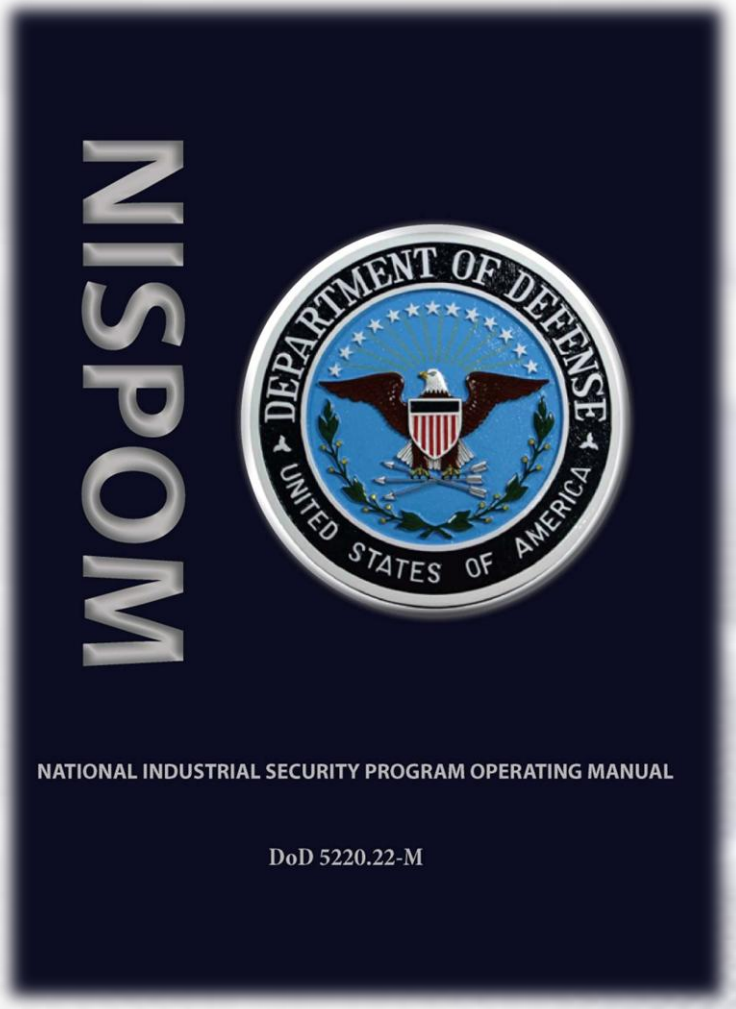
Security Policy Update

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
  - 70+ 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
- 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
    - Sequestration recovery plan
  - Enhanced Security Clearance Act of 2013 impact (Social Media; Agencies providing OPM complete clearance listing)
  - USN's RapidGate Program and Air Force Base access criteria challenges (IG Navy report impact)
- 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. Implementation at PSO level visible.
    - Expected to improve reciprocity

Additional Significant Activities

- Controlled Unclassified Information
  - Meeting with ISOO and CUI Executive Agent Team on 17 July 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”
      - TPI concerns relative to affordability and lack of risk mitigation

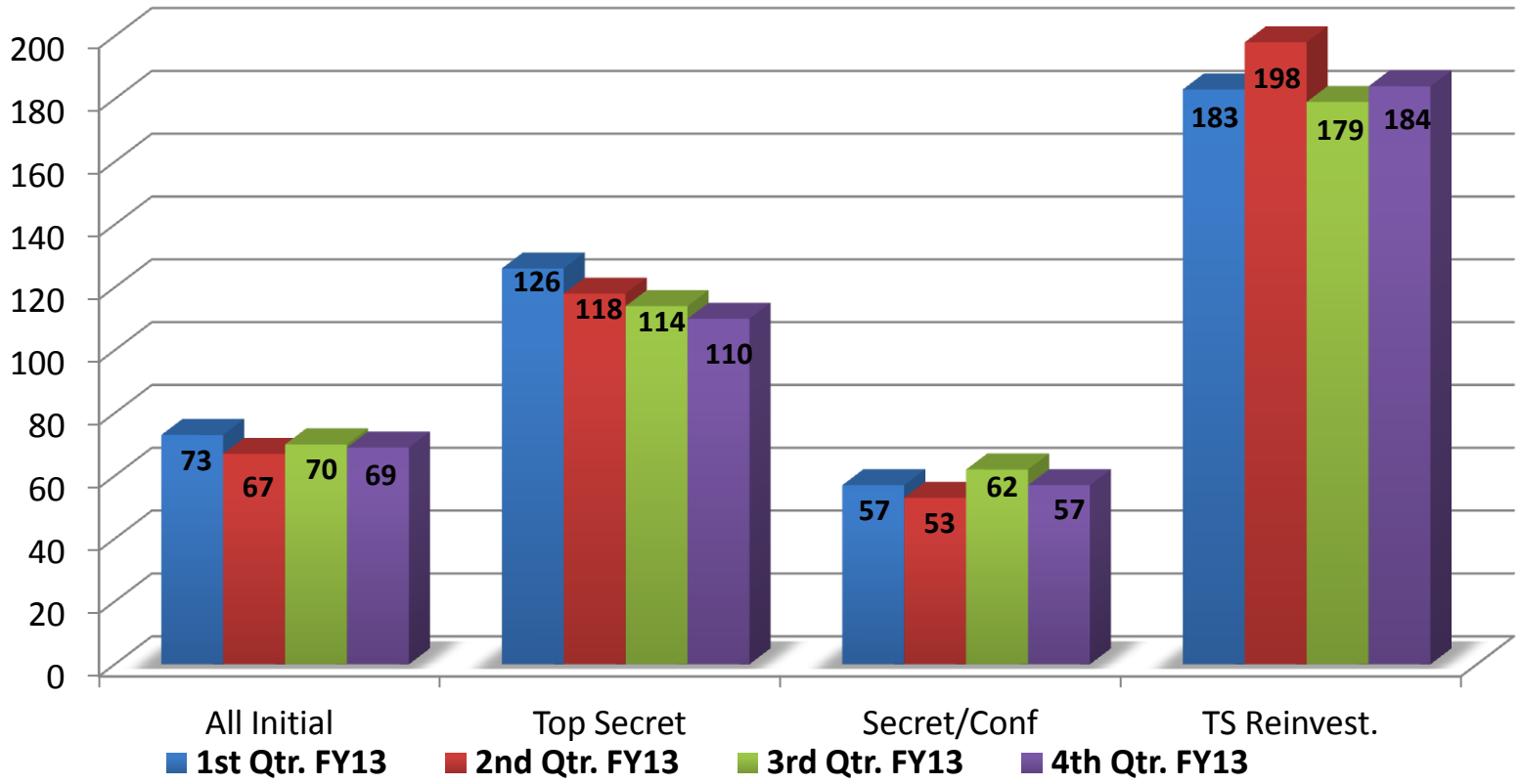
Attachment #4

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

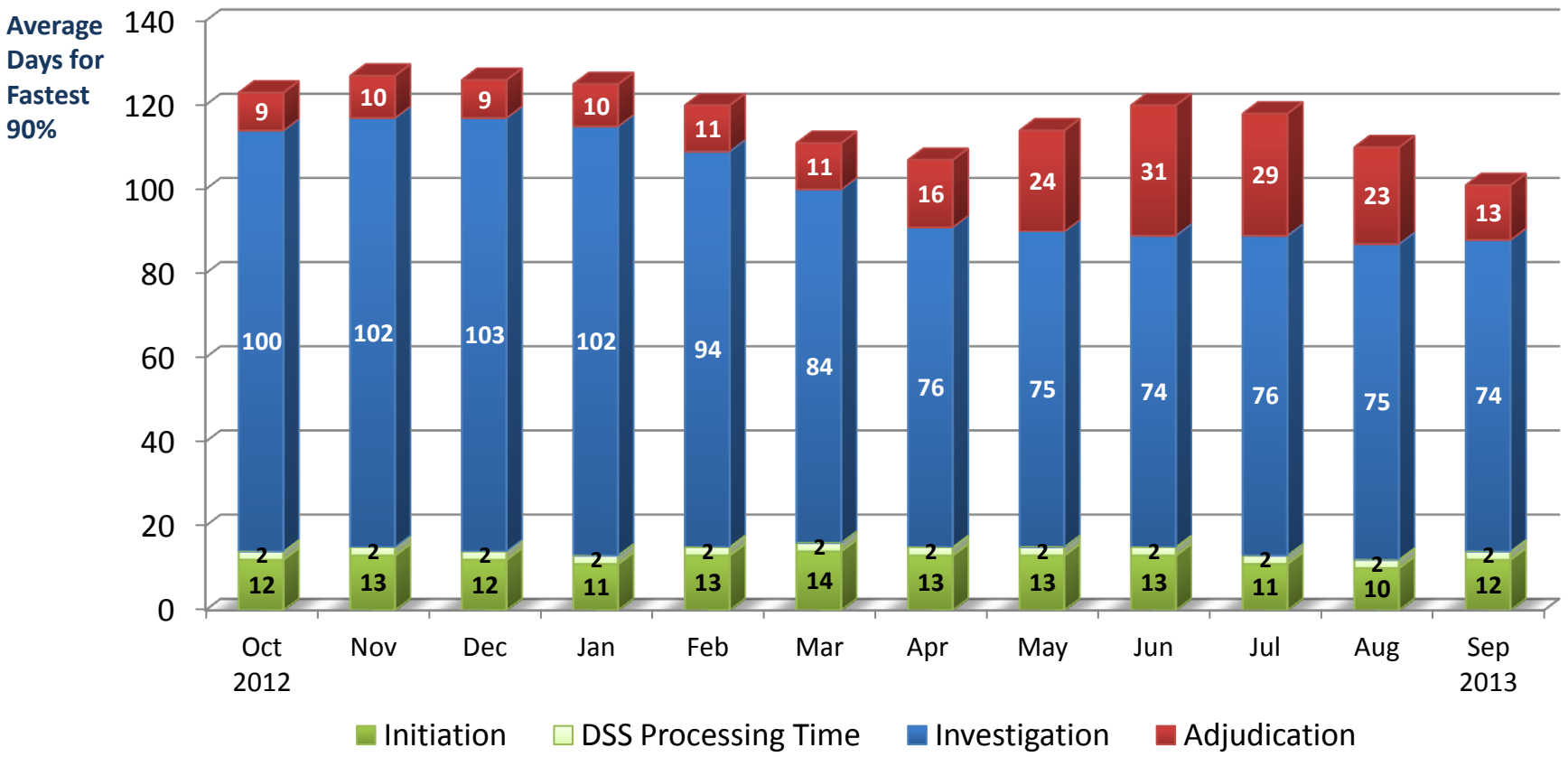
Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 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
Adjudication actions taken – 3rd Q FY13	24,033	4,182	19,851	10,199
Adjudication actions taken – 4th Q FY13	25,264	5,898	19,366	16,632

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

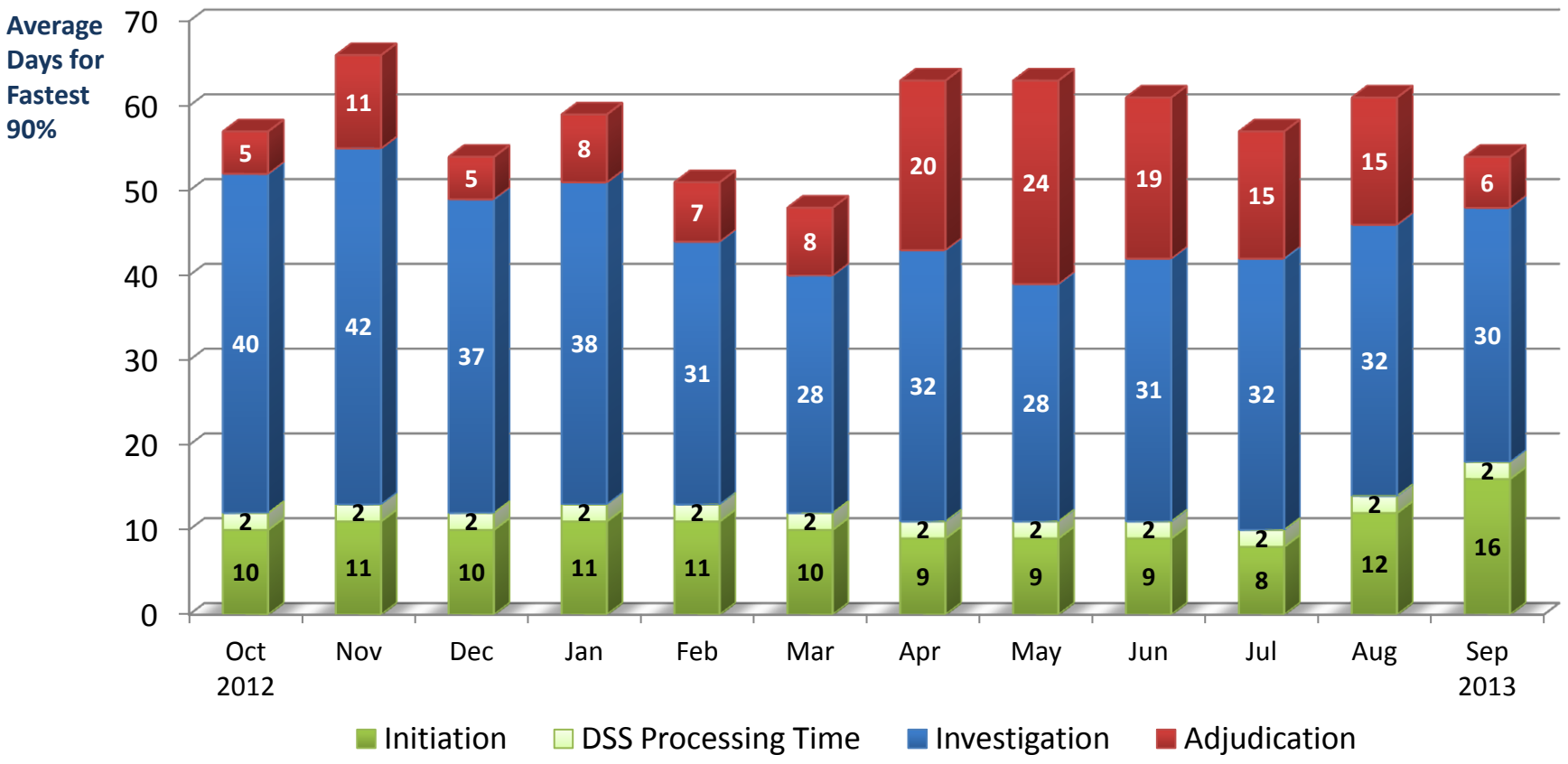
Industry's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



GOAL: Initiation – 14 days ***Investigation – 80 days*** ***Adjudication – 20 days***

	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013
100% of Reported Adjudications	740	718	1,945	1,805	1,910	2,073	1,637	1,182	1,368	2,283	1,407	2,219
Average Days for fastest 90%	123 days	127 days	126 days	125 days	120 days	111 days	107 days	114 days	120 days	118 days	110 days	101 days

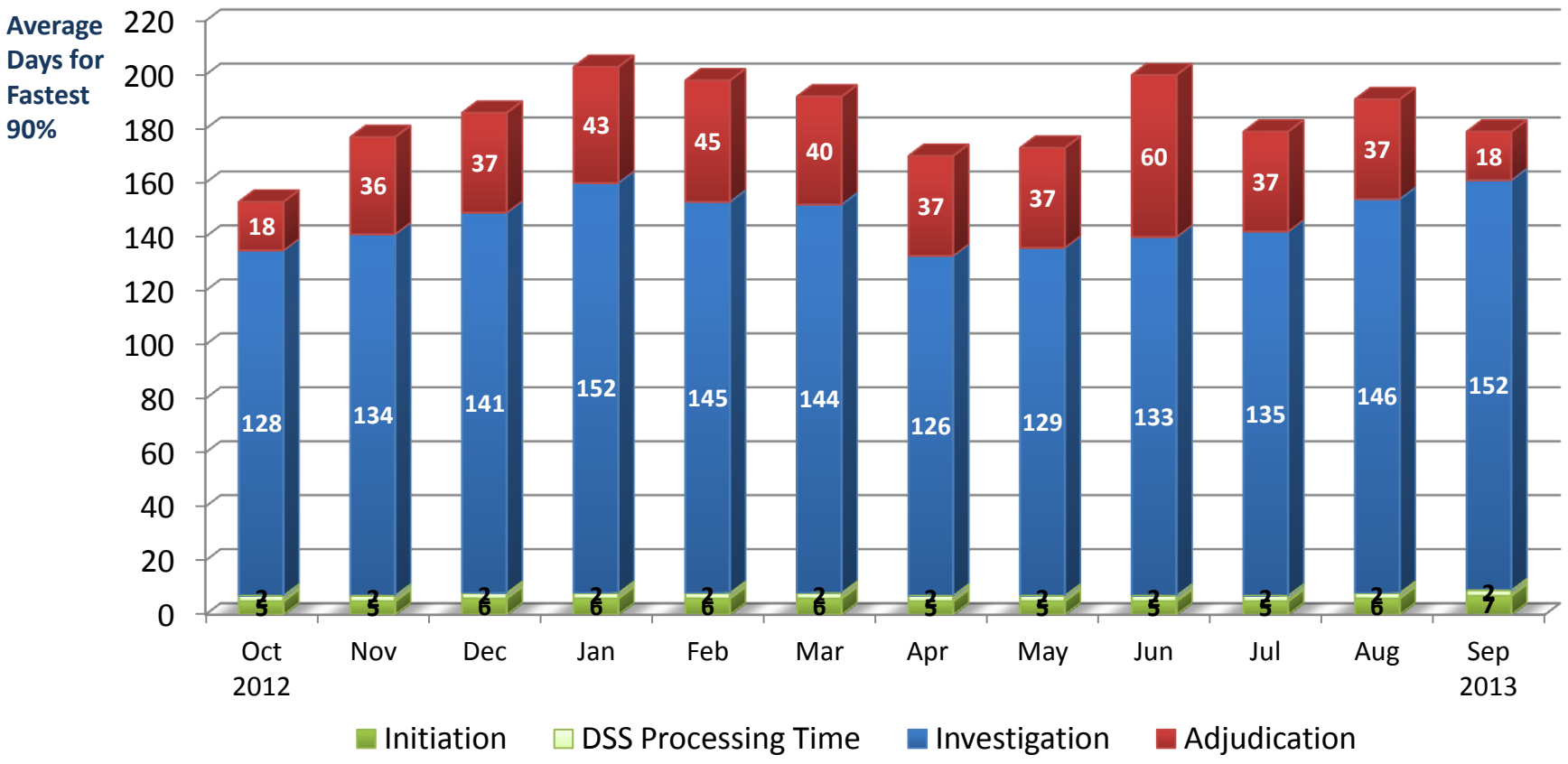
Industry's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



GOAL: Initiation – 14 days ***Investigation – 40 days*** ***Adjudication – 20 days***

	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013
100% of Reported Adjudications	3,005	2,625	5,956	6,905	6,482	6,983	6,327	7,515	6,015	5,836	7,404	6,144
Average Days for fastest 90%	57 days	66 days	54 days	59 days	51 days	48 days	63 days	63 days	61 days	57 days	61 days	54 days

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



GOAL: Initiation – 14 days ***Investigation – 150 days*** ***Adjudication – 30 days***

	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013
100% of Reported Adjudications	1,317	1,783	3,443	3,125	3,122	2,380	4,114	3,667	2,324	4,205	7,515	4,934
Average Days for fastest 90%	153 days	177 days	186 days	203 days	198 days	192 days	170 days	173 days	200 days	179 days	191 days	179 days

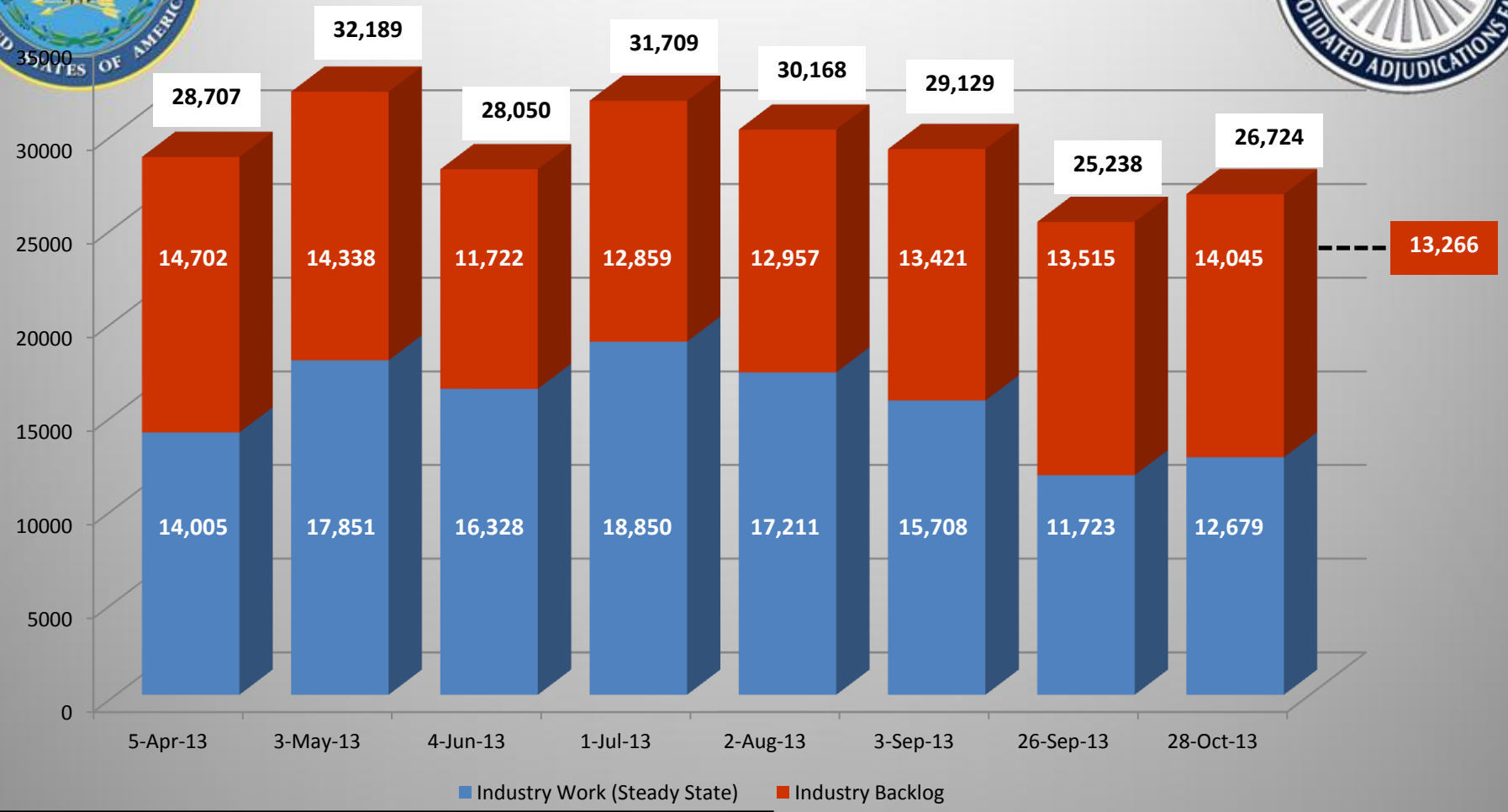
Attachment #5

DoD Consolidated Adjudications Facility (CAF) Presentation

NISPPAC

14 November 2013

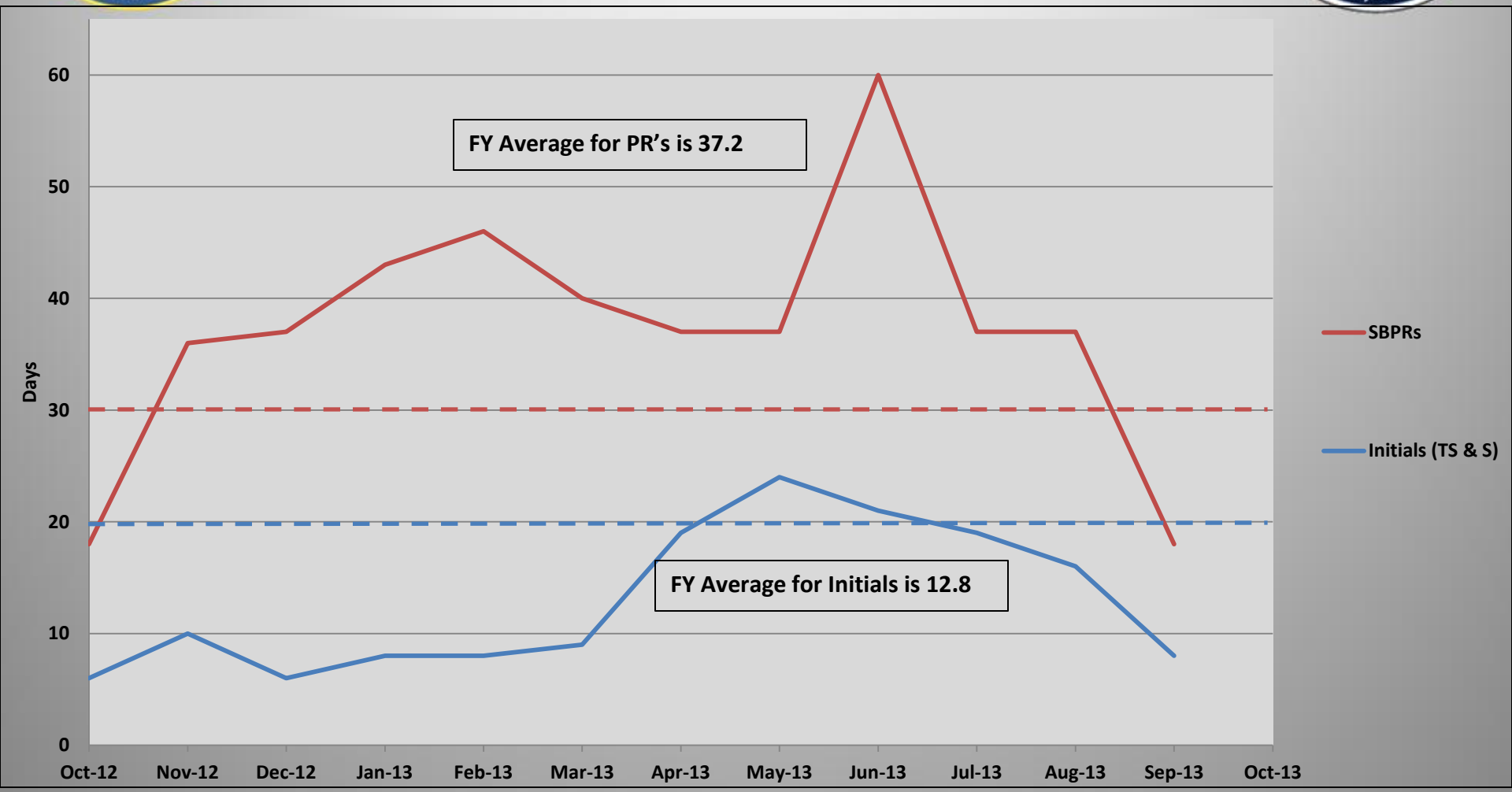
DoD Consolidated Adjudications Facility (CAF)
Pending Industry Workload



- Plan to reduce backlog faltered due to FY13 $$ restraints
- Restart of overtime in late-SEP gave solid results
- Gov't Shutdown in OCT reversed these SEP gains
- Without $$ challenges backlog would likely = 13,266
- Current path eliminates IND backlog NET 2015

Month	NISP Backlog	Annual NISP Receipt	Backlog % of Total NISP
April	14,702		8.1%
September	13,515		7.5%
	-1,187	~ 180,000	

Industry
Intelligence Reform and Terrorism Prevention Act Performance



- Efficiencies beginning to be realized by merger of Industry adjudicators
- Timeliness to fluctuate/increase during FY14-15

DoD Consolidated Adjudications Facility (CAF) Summary and Takeaways:

- **IRTPA**
  - 92.5% of Industry cases are adjudicated in < 20 days
- **DoD CAF Caseload Inventory**
  - DoD CAF to improve timeliness and eliminate backlog via:
    - Improved Processes
    - New Efficiencies
    - Reallocation of adjudicator manpower to NISP cases

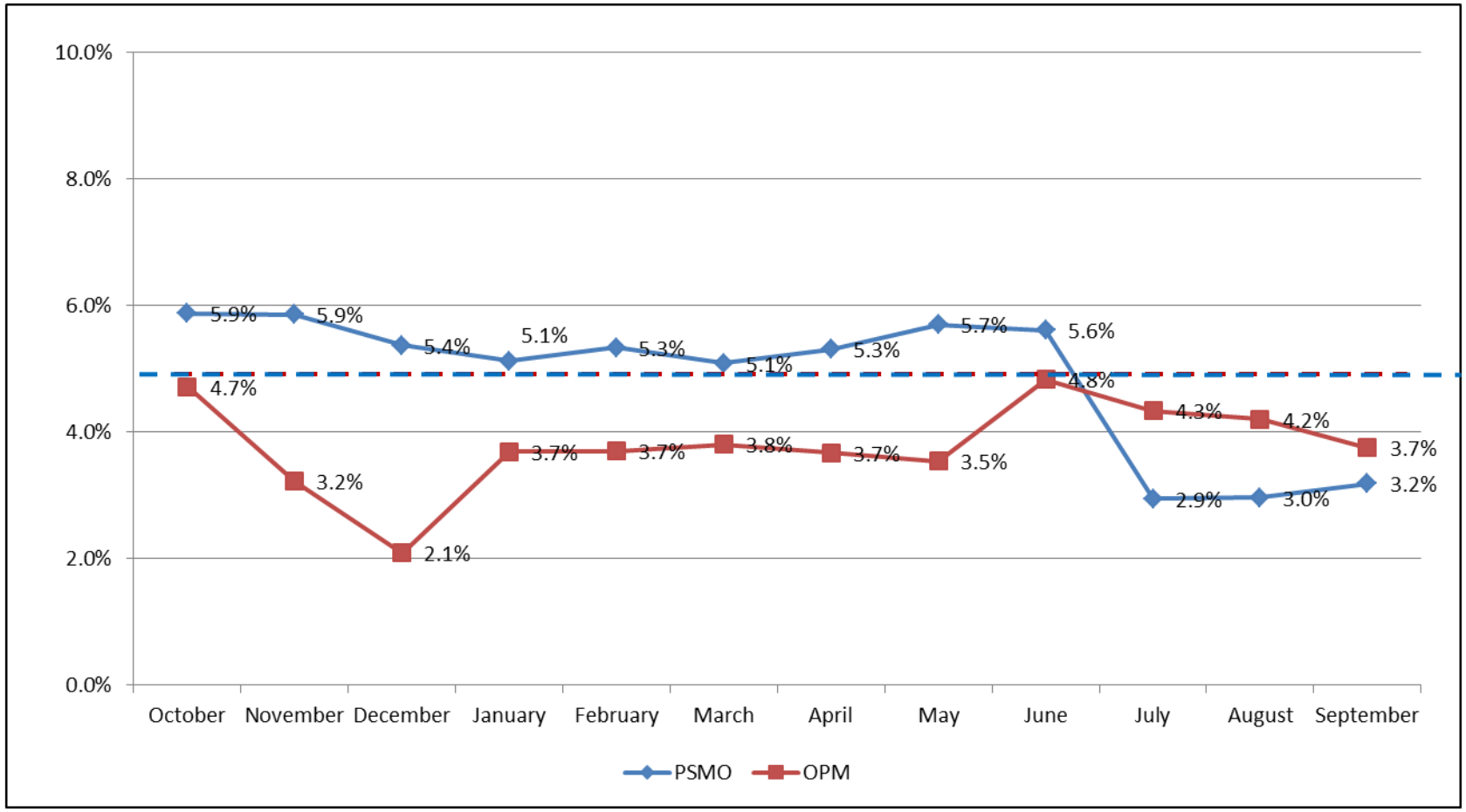
    } On-going merger of former DISCO and DOHA; reducing "touch time"
  - Progress contingent on avoiding additional furloughs
- **DoD CAF Director Assessment:**
  - Given current trends, it will take at least 2 years to fully eliminate Industrial case backlog
  - We should maintain full IRTPA compliance, but overall timeliness for "Initials" likely to increase as we adjudicate more & older backlog cases
  - Given fiscal challenges, DoD CAF is succeeding better than expected

Attachment #6

Defense Security Service

FY 13 PSMO and OPM Reject Rates

Initial and Periodic Reinvestigation Clearance Requests

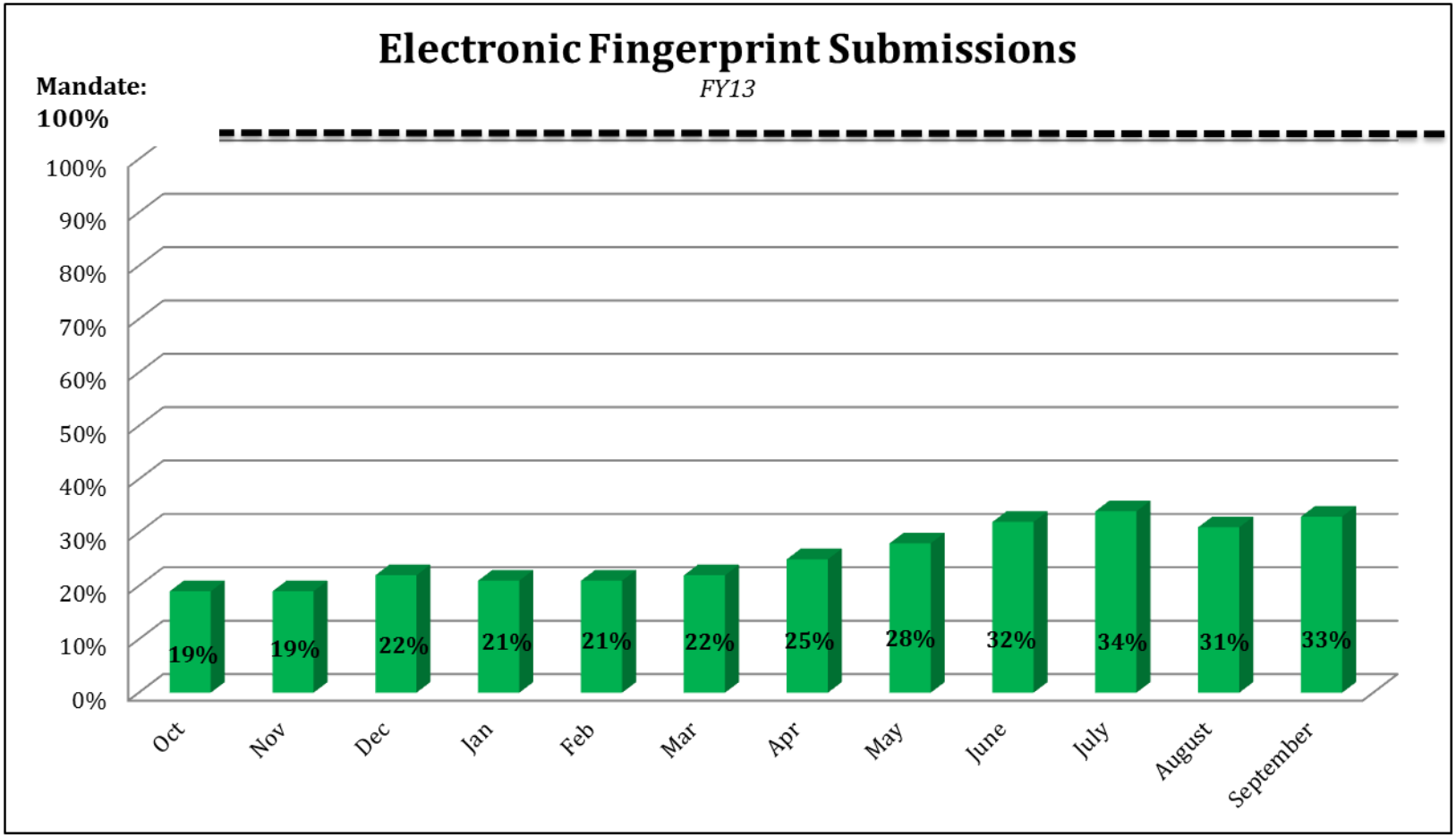


Defense Security Service

Reasons for Case Rejection by OPM

Top Five OPM Rejection Reasons	Percent
Missing Fingerprint Cards (not submitted with SF 86)	62%
Certification and Release Forms not signed or submitted	27%
Discrepancy with applicant's place of birth and date of birth*	7%
Missing or Discrepant Reference Information	3%
Missing previous Employer Information	1%
Top Five Grand Total	**100%**

Defense Security Service



Defense Security Service

PSI Update - as of 4 November 2013

- PSMO-I
  - Total submissions in JPAS: 13,690
    - ❑ Oldest e-QIP: 1 Oct 13
    - ❑ PPR: 5,404
    - ❑ SSBI: 1,533
    - ❑ NACLC: 6,753
  - JPAS request from Industry: ~600/day
  - Overdue PR and Aging Interims: ongoing project
  - Reminder to submit new SF312

- Inventory workload strategy:
  - Work cases according to receipt date in the queue
  - Announcement posted on http://www.DSS.mil

Defense Security Service

PSMO-I Contact Information

The Personnel Security Management Office for Industry (PSMO-I) has moved!

Our new contact information is as follows:

Address:	Defense Security Service ATTN: PSMO-I 7556 Teague Road, Suite 500 Hanover, MD 21076
Phone:	443-661-1320
Fax:	443-661-1140
Email:	AskPSMO-I@dss.mil

Attachment #7

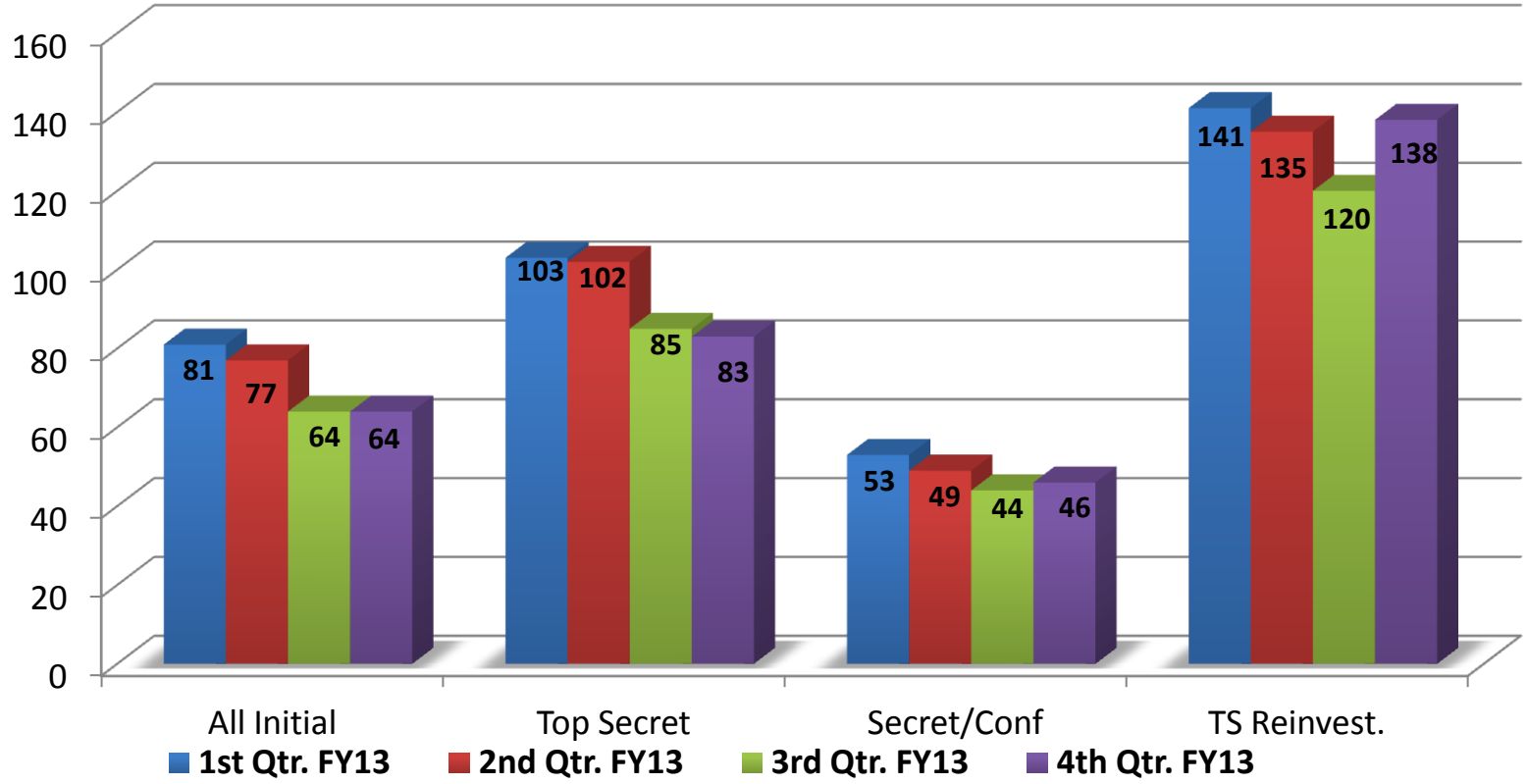
a New Day for Federal Service

Timeliness Performance Metrics for Department of Energy's Personnel Submission, Investigation & Adjudication Time

FY 2013

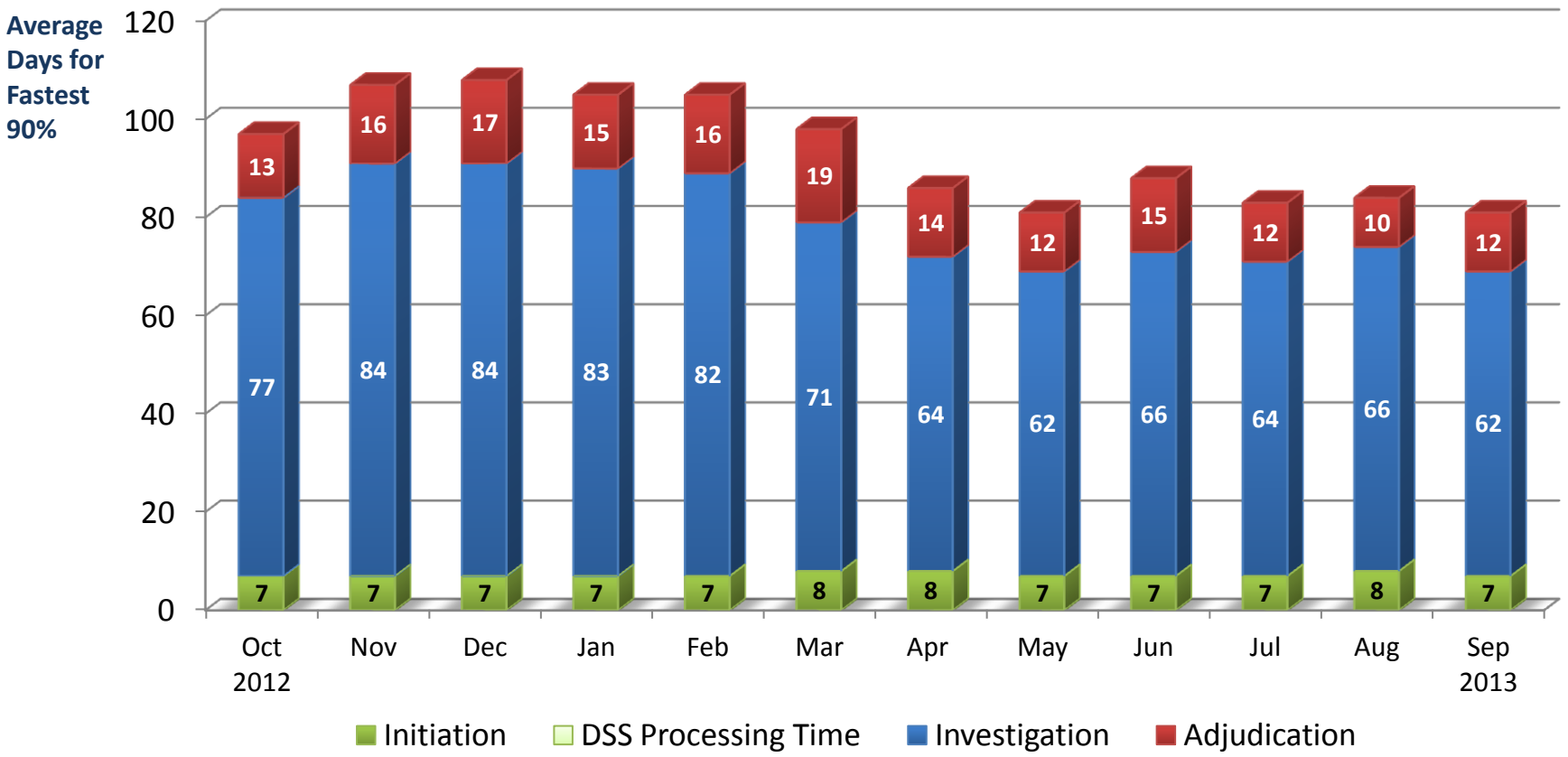
Timeliness Performance Metrics for DOE's Personnel Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 1st Q FY13	1,362	770	592	1,895
Adjudication actions taken – 2nd Q FY13	1,679	914	765	1,971
Adjudication actions taken – 3rd Q FY13	1,896	979	917	2,961
Adjudication actions taken – 4th Q FY13	1,535	758	777	3,743

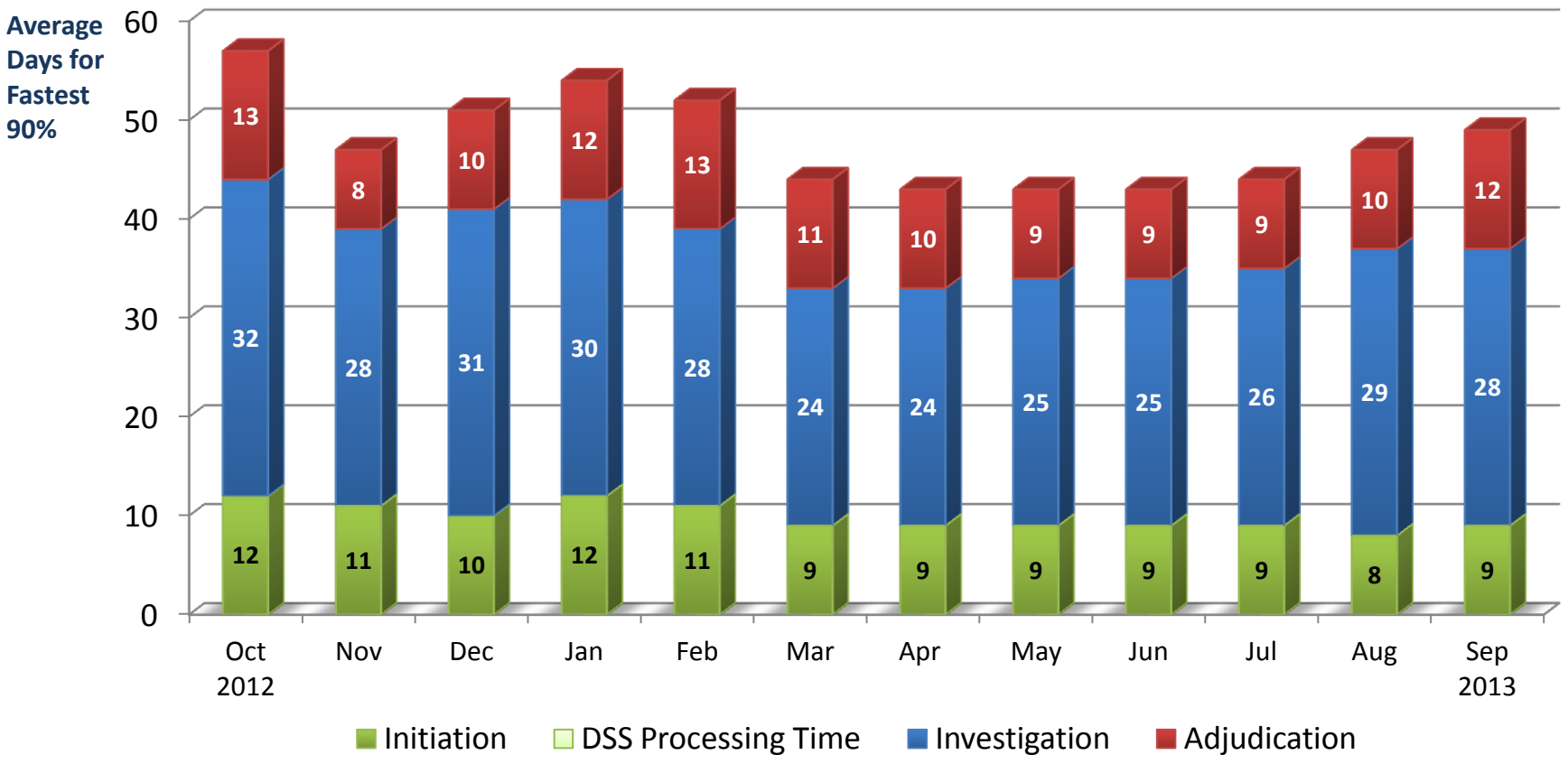
DOE's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



GOAL: Initiation – 14 days ***Investigation – 80 days*** ***Adjudication – 20 days***

	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013
100% of Reported Adjudications	263	232	244	302	285	311	381	323	274	266	249	231
Average Days for fastest 90%	97 days	107 days	108 days	105 days	105 days	98 days	86 days	81 days	88 days	83 days	84 days	81 days

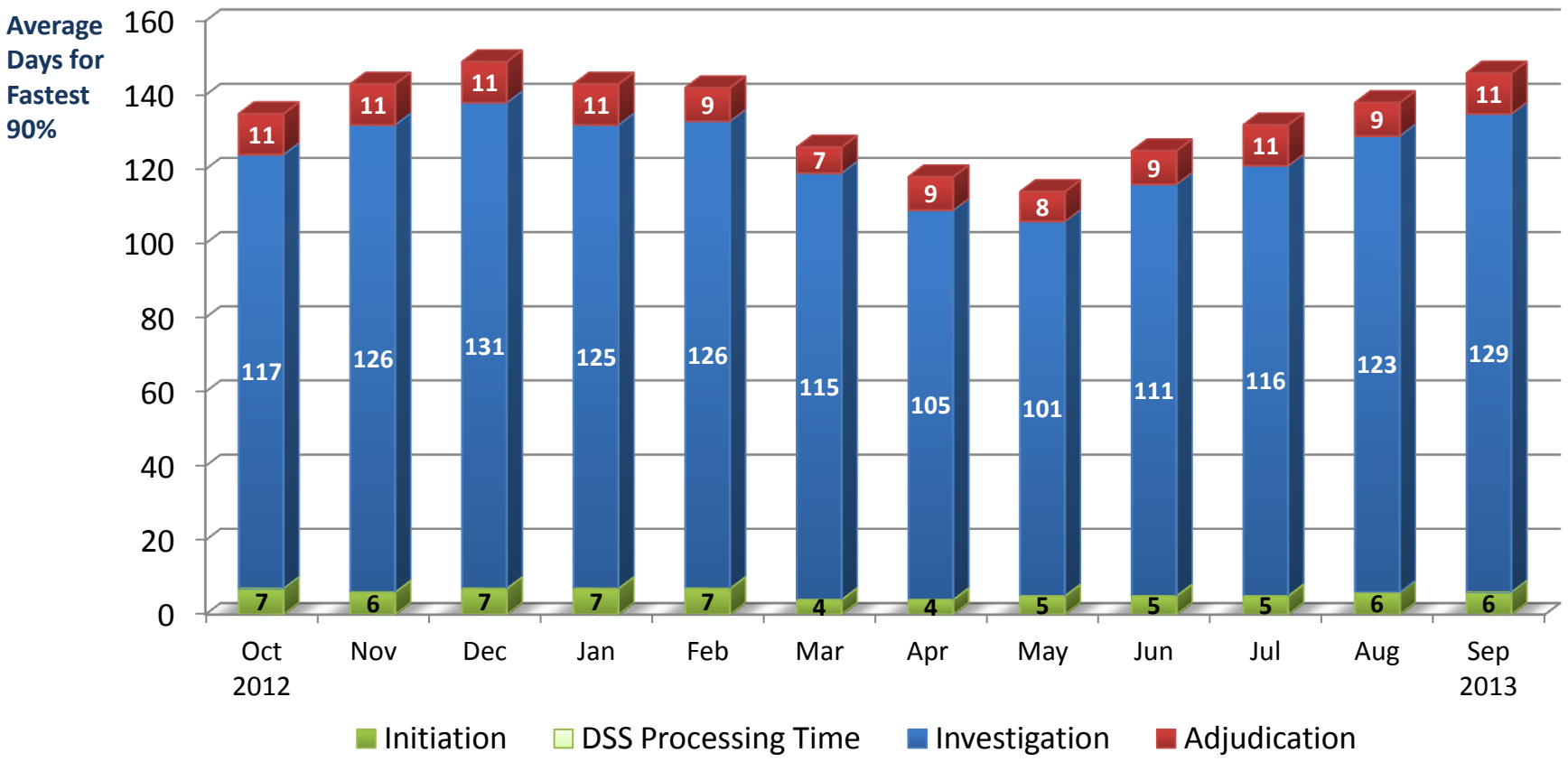
DOE's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



GOAL: Initiation – 14 days ***Investigation – 40 days*** ***Adjudication – 20 days***

	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013
100% of Reported Adjudications	184	183	165	221	209	285	338	321	233	286	278	197
Average Days for fastest 90%	57 days	47 days	51 days	54 days	52 days	44 days	43 days	43 days	43 days	44 days	47 days	49 days

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



GOAL: Initiation – 14 days ***Investigation – 150 days*** ***Adjudication – 30 days***

	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013
100% of Reported Adjudications	831	540	479	500	580	860	1,159	773	1,011	1,184	1,392	1,148
Average Days for fastest 90%	135 days	143 days	149 days	143 days	142 days	126 days	118 days	114 days	125 days	132 days	138 days	146 days

Attachment #8

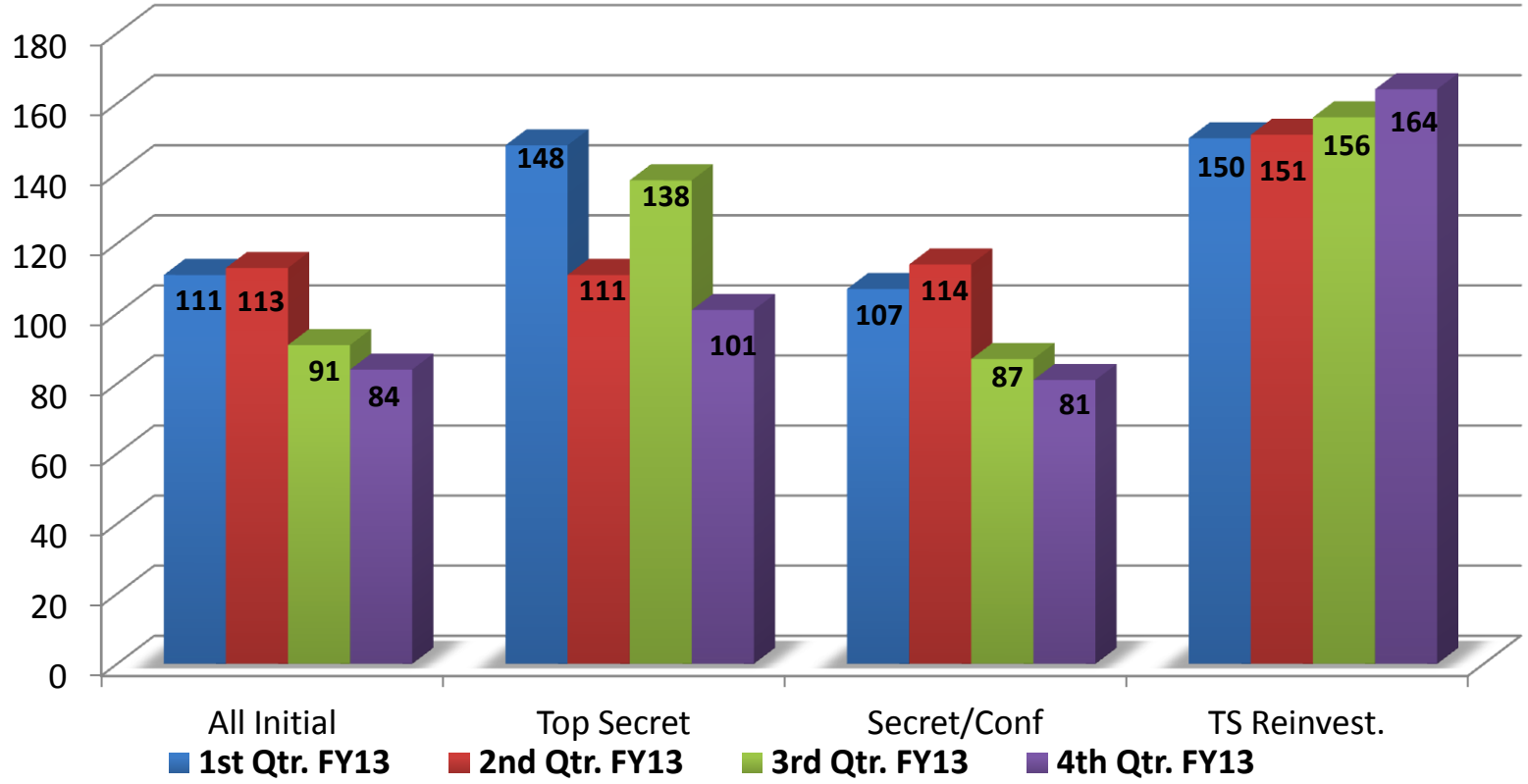
a New Day for Federal Service

Timeliness Performance Metrics for Nuclear Regulatory Commission's Personnel Submission, Investigation & Adjudication Time

FY 2013

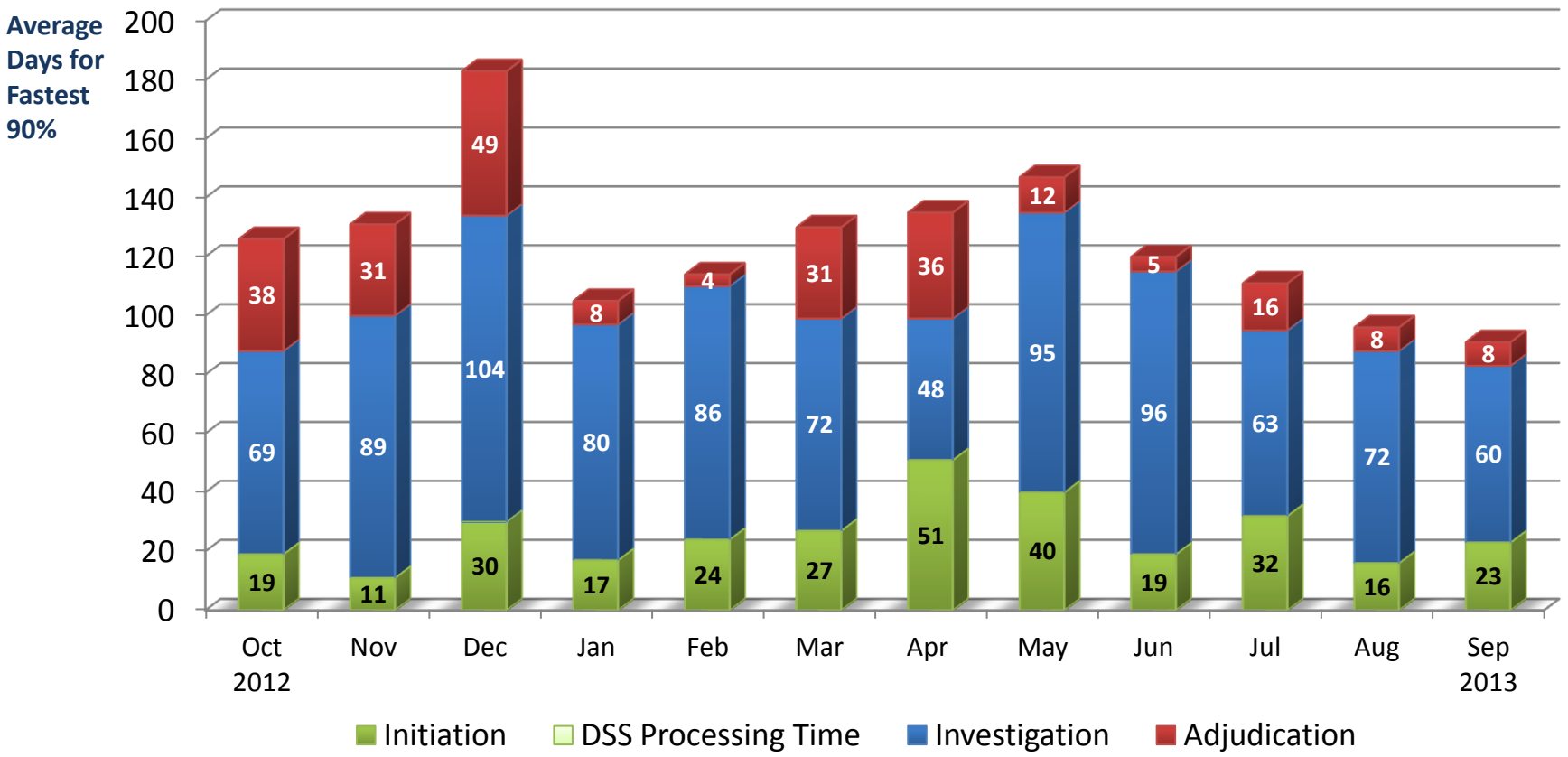
Timeliness Performance Metrics for NRC's Personnel Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 1st Q FY13	201	22	179	31
Adjudication actions taken – 2nd Q FY13	227	59	168	25
Adjudication actions taken – 3rd Q FY13	254	22	232	22
Adjudication actions taken – 4th Q FY13	265	35	230	49

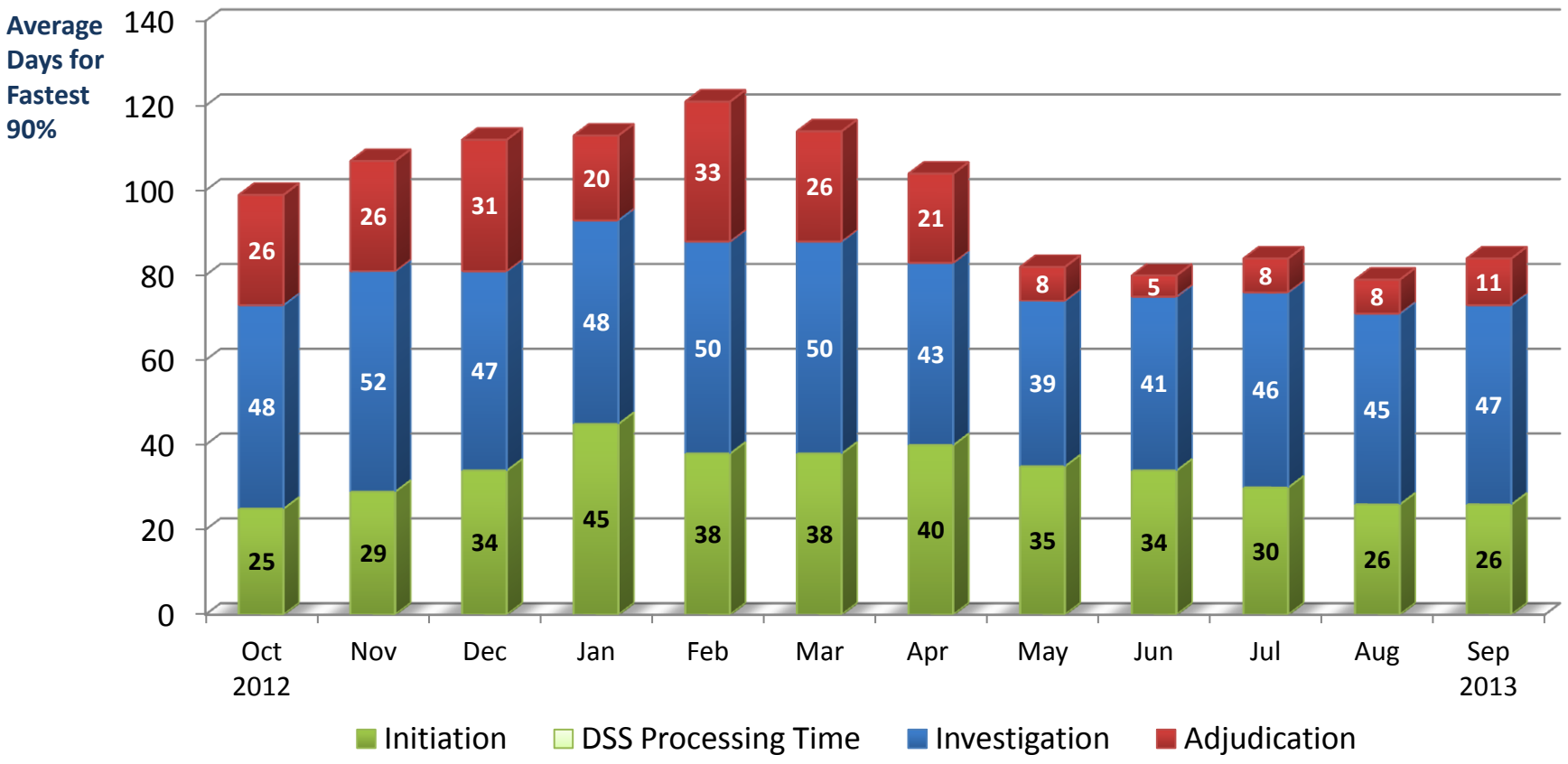
NRC's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



GOAL: Initiation – 14 days ***Investigation – 80 days*** ***Adjudication – 20 days***

	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013
100% of Reported Adjudications	9	6	7	16	21	22	7	11	4	15	10	10
Average Days for fastest 90%	126 days	131 days	183 days	105 days	114 days	130 days	135 days	147 days	120 days	111 days	96 days	91 days

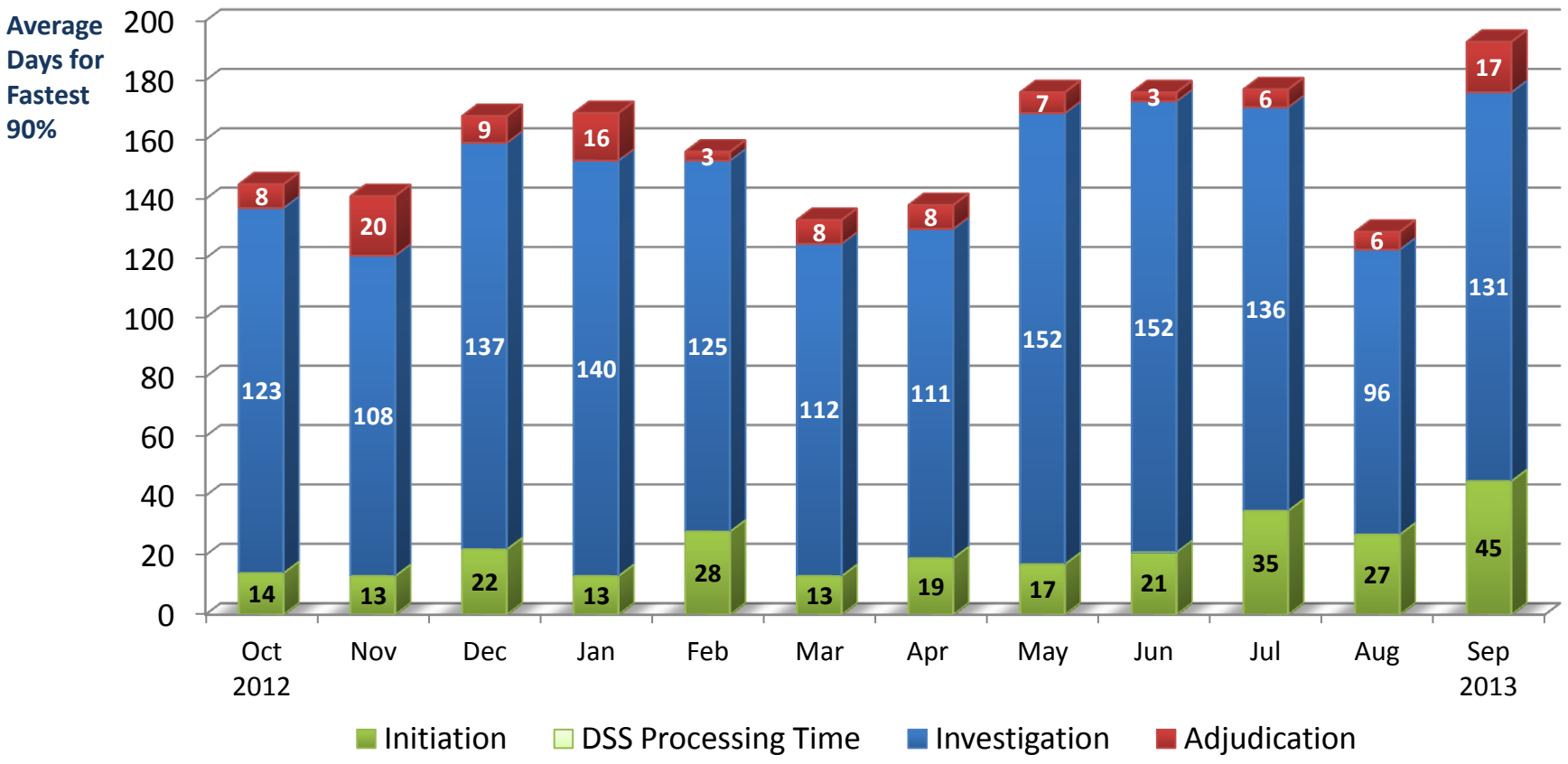
NRC's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



GOAL: Initiation – 14 days ***Investigation – 40 days*** ***Adjudication – 20 days***

	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013
100% of Reported Adjudications	35	86	57	55	44	69	62	82	87	94	79	58
Average Days for fastest 90%	99 days	107 days	112 days	113 days	121 days	114 days	104 days	82 days	80 days	84 days	79 days	84 days

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



GOAL: Initiation – 14 days ***Investigation – 150 days*** ***Adjudication – 30 days***

	Oct 2012	Nov 2012	Dec 2012	Jan 2013	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013
100% of Reported Adjudications	10	10	11	6	8	11	11	4	7	14	17	18
Average Days for fastest 90%	145 days	141 days	168 days	169 days	156 days	133 days	138 days	176 days	176 days	177 days	129 days	193 days

Attachment #9

NISPPAC C&A Working Group Update for the Committee

Oct 2013

Overview:

- Working group initiatives
- 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

Certification & Accreditation

- DSS is the primary government entity responsible for approving cleared contractor information systems to process classified data.

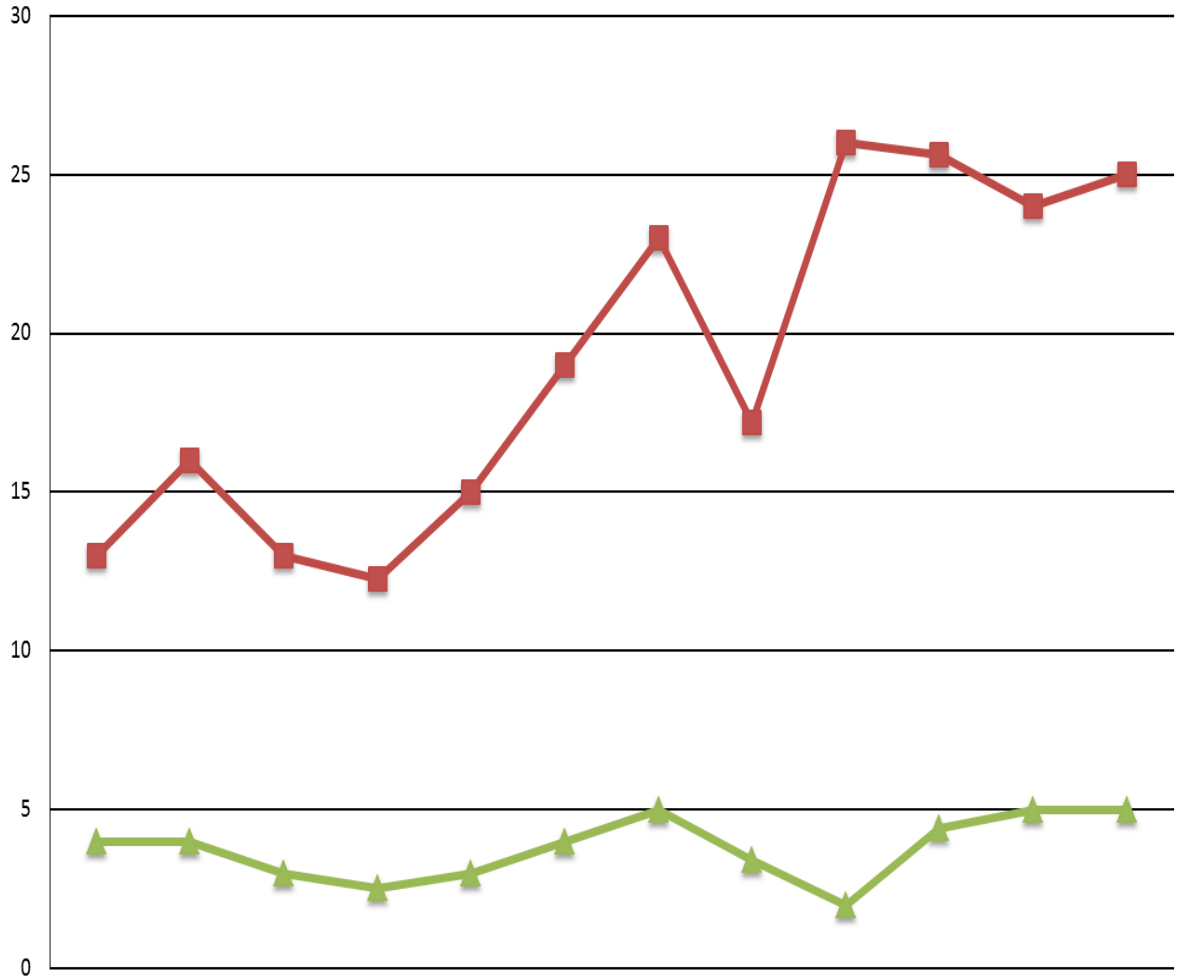
- Work with industry partners to ensure information system security controls are in place to limit the risk of compromising national security information.

- Ensures adherence to national industrial security standards.

Working Group Initiatives

- Windows 7 & 2008 Server Baseline Stds
  - Completed July 2013
- ISFO Process Manual draft complete and under final coordination for release approval
  - Review completed September 2013
- Reviewing DoD security content automation protocol (SCAP) for possible use in assessing compliance on NISP information systems
- Assessing requirements to ranking vulnerabilities reported according to the risk to classified information vice the documented top common discrepancies.

Security Plan Review Results from Oct 2012- Sept 2013



	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13	May-13	Jun-13	Jul-13	Aug-13	Sep-13
Total IATOs	156	145	143	153	125	158	193	189	155	223	145	170
Industry Response Time to DSS Questions, Comments	4	4	3	3	3	4	5	3	2	4	5	5
# Second IATOs	14	14	15	6	4	17	15	12	12	28	13	14
Time from DSS Receipt of plans to Granting of IATOs	13	16	13	12	15	19	23	17	26	26	24	25

3699 SSPs were received

1955 IATOs were issued

Avg. 20 days to issue an IATO

1362 SATO were processed

20 days to issue a SATO.

908 of the SSPs (25%) required some level of correction

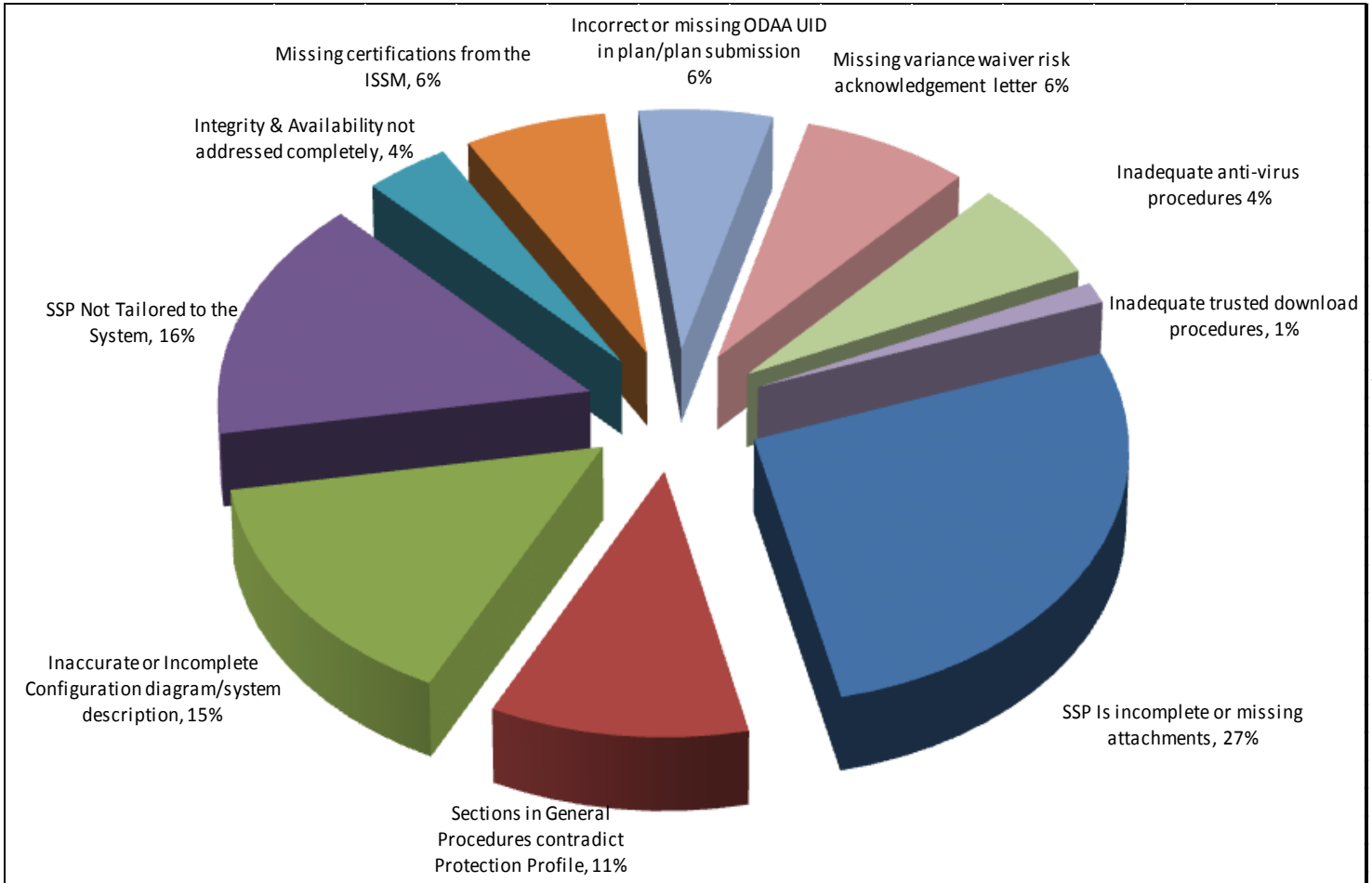
- 544 of the SSPs (15%) were granted IATO with corrections required.

- 101 of the SSPs (3%) that went SATO required some level of correction.

- 263 of the SSPs (7%) 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 Oct 2012- Sept 2013

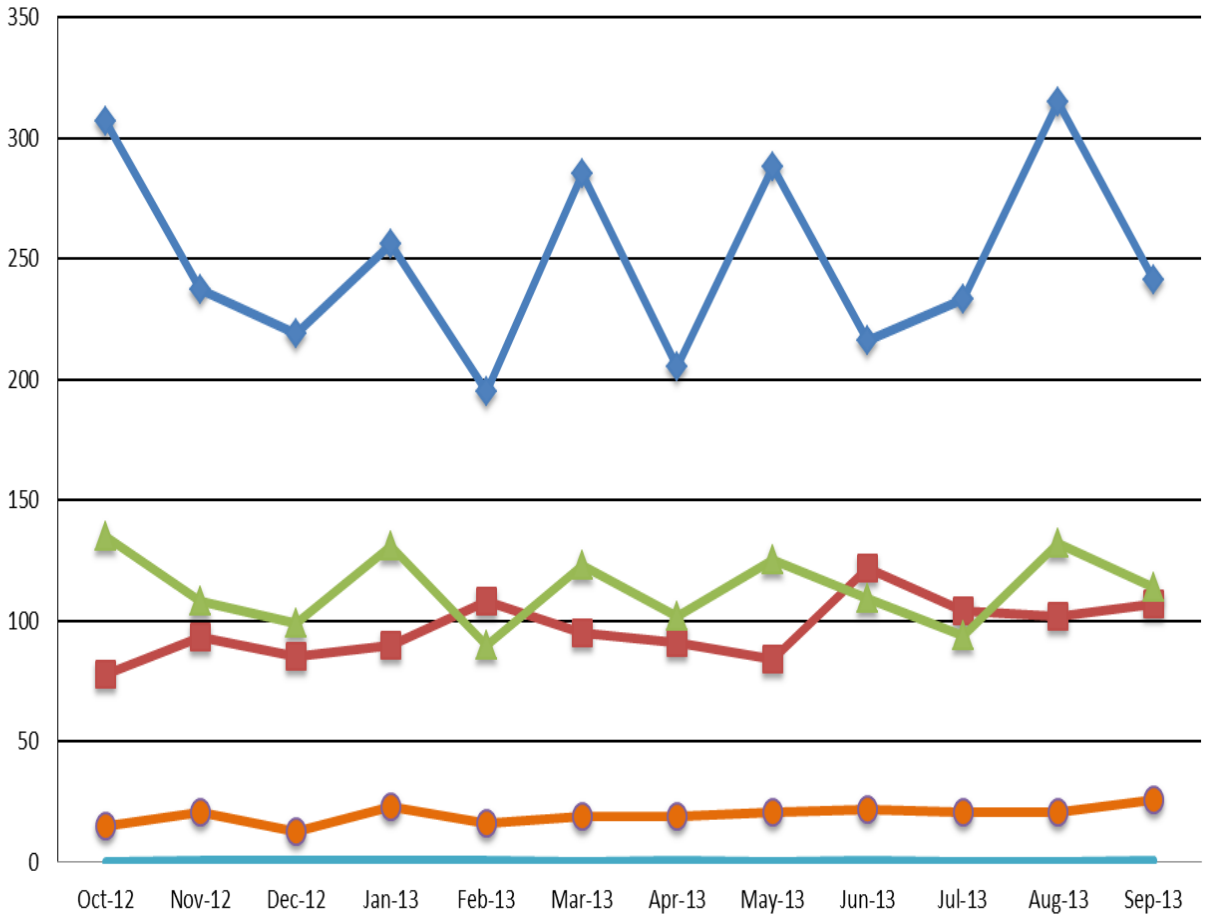


	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13	May-13	Jun-13	Jul-13	Aug-13	Sep-13
# Deficiencies	172	147	88	163	123	144	189	124	180	217	168	239
# Plans w/ Deficiencies	82	82	52	94	61	69	106	81	81	115	92	112
# Plans Reviewed	315	277	262	330	242	304	333	343	302	354	309	328
Avg Deficiency per Plan	0.55	0.53	0.34	0.49	0.51	0.47	0.57	0.36	0.60	0.61	0.54	0.73
Denials	19	9	15	28	21	15	21	16	30	29	29	31
Rejections	5	15	5	18	6	8	17	13	8	8	3	13

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 Oct 2012- Sept 2013



	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13	May-13	Jun-13	Jul-13	Aug-13	Sep-13
Total ATOs	307	237	219	256	195	285	205	288	216	233	315	241
Avg Days to Reg ATO	78	93	85	90	108	95	91	84	122	104	102	107
Total SATOs	135	108	99	131	90	123	102	125	109	94	132	114
Avg Days to SATO	15	21	13	23	16	19	19	20	22	21	21	26
% SATO's	44%	46%	45%	51%	46%	43%	50%	43%	50%	40%	42%	47%

During the Past 12 Months:

2997 ATOs

Avg 96 Days from IATO to ATO

1362 SATOs

Avg 20 days for SATOs

45% of all ATOs were SATO

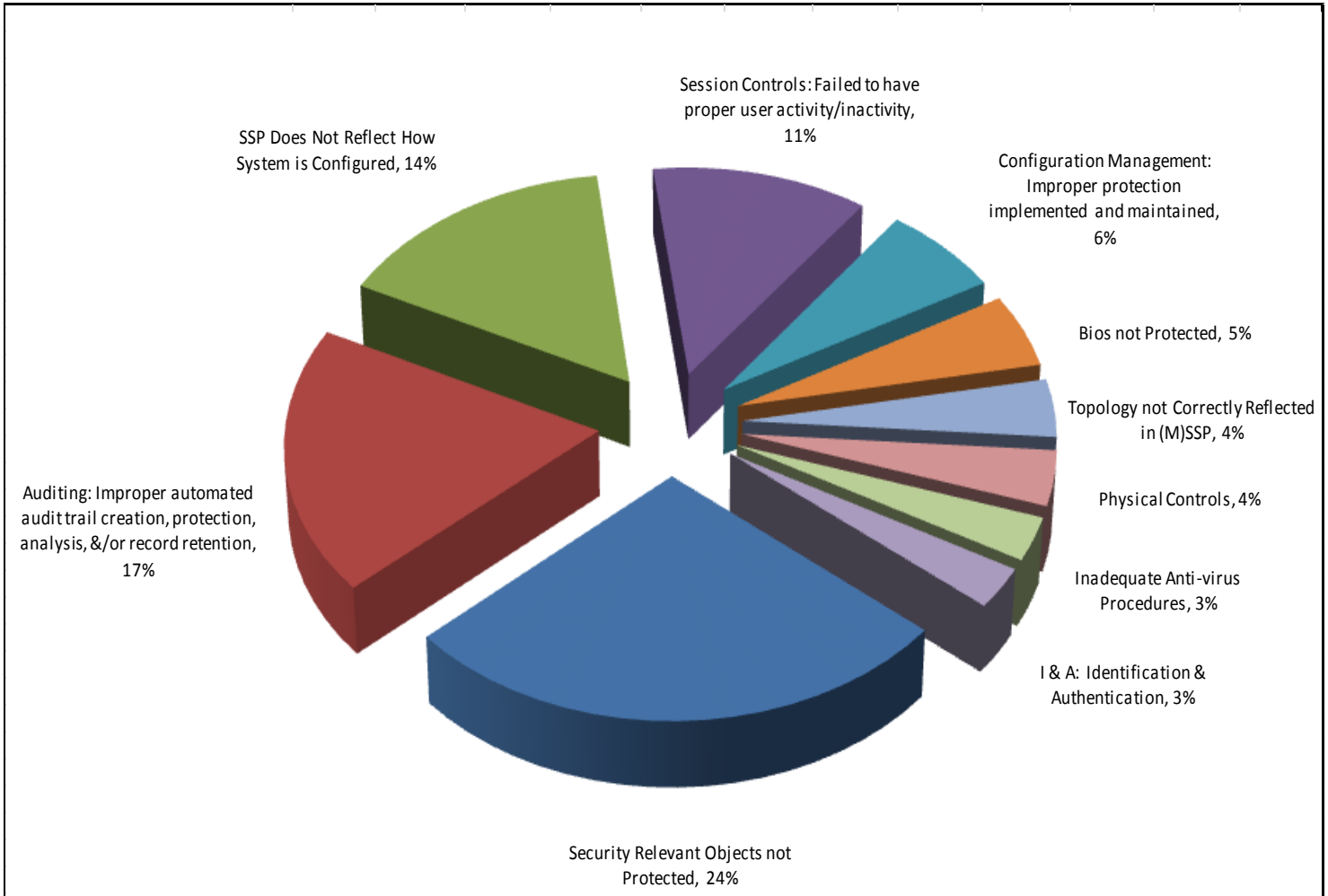
2880 ATO System Validations

- 2168 systems (75%) had no vulnerabilities identified.

- 660 systems (23%) had minor vulnerabilities identified that were corrected while onsite.

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

Common Vulnerabilities found during System Validations from Oct 2012- Sept 2013



	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13	May-13	Jun-13	Jul-13	Aug-13	Sep-13
# Vulnerabilities	104	67	92	128	63	93	79	108	70	95	77	105
# Onsites w/ vulnerabilities	62	45	59	78	42	60	48	54	54	67	69	74
# Onsites	285	219	207	247	194	273	194	280	203	234	309	235
Avg Vulnerability per Onsite	0.36	0.31	0.44	0.52	0.32	0.34	0.41	0.39	0.34	0.41	0.25	0.45

Top 10 Vulnerabilities

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

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 #10

Implementing Executive Order 13636 and Presidential Policy Directive 21

Jeanette Manfra
Deputy Director, EO-PPD Integrated Task Force
November 12, 2013

Homeland Security

A Changing Environment

America faces changing risk, strategic, and operating environments for critical infrastructure.

"Over the last few decades, our Nation has grown increasingly dependent on critical infrastructure, the backbone of our national and economic security. America's critical infrastructure is complex and diverse, combining systems in both cyberspace and the physical world -- from power plants, bridges, and interstates to Federal buildings and the massive electrical grids that power our Nation…."

"…We must continue to strengthen our resilience to threats from all hazards including terrorism and natural disasters, as well as cyber attacks. We must ensure that the Federal Government works with all critical infrastructure partners, including owners and operators, to share information effectively while jointly collaborating before, during, and after an incident..."

- President Barack Obama
  October 31, 2013

Homeland Security

Taking Action

While the Administration continues to believe that comprehensive legislation is needed to fully address the threat, it is working within existing law to drive action toward national cyber and physical security and resilience

Executive Order 13636: Improving Critical Infrastructure Cybersecurity

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience

The EO and PPD (February, 2013) address evolving threats through an updated and overarching national framework that acknowledges the increased role of cybersecurity in securing physical assets.

Homeland Security

Milestones

120 days – **June 12, 2013**

- Publish instructions: unclassified threat information
- Report on cybersecurity incentives
- Publish procedures: expand the Enhanced Cybersecurity Services

150 Days - **July 12, 2013**

- Identify cyber-dependent critical infrastructure
- Evaluate public-private partnership models
- Expedite security clearances for private sector

240 Days* – **November 8, 2013**

- Develop a situational awareness capability
- Publish a successor to the National Infrastructure Protection Plan
- Publish draft voluntary Cybersecurity Framework

365 days – **February 12, 2014**

- Report on privacy and civil rights and civil liberties cybersecurity enhancement risks
- Stand up voluntary program based on finalized Cybersecurity Framework

Beyond 365 - **TBD**

- Critical Infrastructure Security and Resilience R&D Plan

Homeland Security

*Original 240-day deadline amended following the government shutdown

NIPP 2013: PARTNERING FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Purpose and Challenge

Purpose:

Guide the collective effort to strengthen the security and resilience of the Nation's critical infrastructure.

Challenge:

Developing the Plan in collaborative manner, recognizing the evolving risk landscape and complex decision-making environment of diffuse authorities and responsibilities

Guiding Principles

Through partnerships, infrastructure is made more secure and resilient

Build on the successful work to date and leverage existing knowledge and structures wherever possible

Describe the conditions that necessitate an updated approach to critical infrastructure security and resilience

Lay out the broad principles and policies that underpin this approach in the public and private sectors

Describe the national program that will implement these principles and policies to achieve shared outcomes

Impacts for SLTT Partners

SLTT considerations played a major role in the creation of the Plan, as well as EO-PPD deliverables and working groups

- Promotes regional partnerships in addition to national ones
- Strengthens Information Sharing
- Reaffirms the roles of various public-private coordination structure
- Identifies government resources to support regional and local efforts
- Sets goals for the national effort, which are focused on security and resilience
- Supports a forward looking approach to Enterprise Risk Management and dependency/interdependency examination

Goals of National Effort

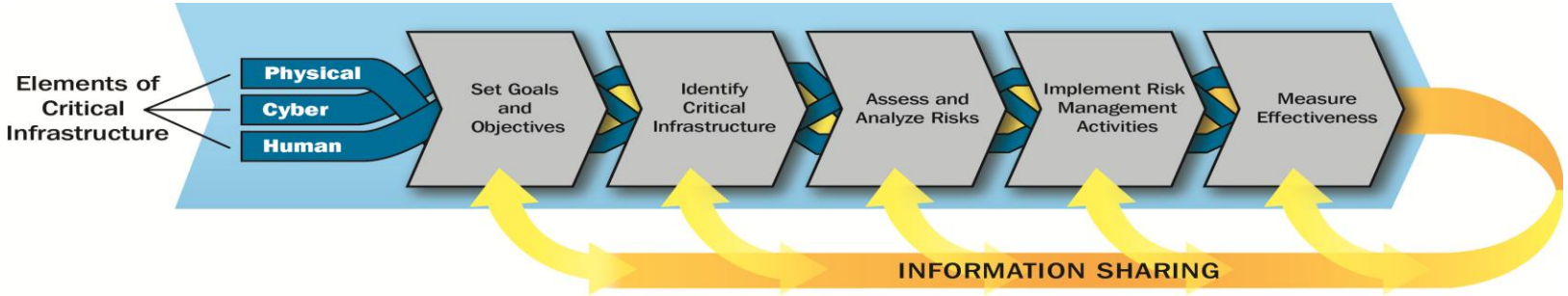
Articulated Goals

- Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities;
- Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;
- Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation, as well as effective responses to both save lives and ensure the rapid recovery of essential services;
- Efficiently share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and
- Promote learning and adaptation during and after exercises and incidents.

Changes and Evolution from 2009 NIPP

The 2013 Plan is more strategic and flexible than the previous NIPP

- Recognize the change in the strategic environment
  - Risk landscape Infrastructure Operations Policy Changes
- Focus on actions and implementation
- Retains a focus on risk management as the foundation of national CI security and resilience; makes enhancements to framework
- More closely integrates *information-sharing* as an essential element of the risk management framework



Changes and Evolution cont.

The Plan elevates security and resilience as the primary aim of Critical Infrastructure planning efforts

- Draws alignment between critical infrastructure risk management efforts and the National Preparedness System (across five mission areas)
- Focuses on national priorities jointly determined by public and private sectors, while limiting discussion of Federal programs
- Integrates cyber and physical security and resilience efforts into an enterprise approach to risk management
- Continues progress to support execution of the *National Plan* at both the national and community levels

Changes and Evolution, cont.

The Plan is a collaborative document developed for national, regional and local partners, as well as international partners

- Affirms the reality that critical infrastructure security and resilience efforts require international collaboration;
- Incorporates practical lessons learned from national program and feedback from partners
- Is mindful of the perspectives and capabilities of different partners – including Federal roles outlined in PPD 21 -- and how this affects collective efforts
- Includes a detailed Call to Action, with steps that the Federal Government will undertake – working with CI partners – to make progress toward security and resilience

Call to Action

Build upon Partnership Efforts

1. Set National Focus through Joint Priority Setting
2. Determine Collective Actions through Joint Planning Efforts
3. Empower Local and Regional Partnerships to Build Capacity Nationally
4. Leverage Incentives to Advance Security and Resilience
5. Enable Risk-Informed Decision-Making through Enhanced Situational Awareness

Innovate in Managing Risk

6. Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects
7. Rapidly Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents
8. Promote Infrastructure, Community, and Regional Recovery Following Incidents
9. Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education
10. Improve Critical Infrastructure Security and Resilience by advancing Research and Development Solutions

Focus on Outcomes

11. Evaluate Achievement of Goals
12. Learn and Adapt During and After Exercises and Incidents

QUESTIONS

Homeland Security