Minutes of the June 19, 2014 Meeting of the
National Industrial Security Program Policy Advisory Committee (NISPPAC)

The NISPPAC held its 48th meeting on Thursday, June 19, 2014, at 10:00 a.m. at the Gaylord National Resort and Convention Center, 201 Waterfront St., National Harbor, MD, 20745. John Fitzpatrick, Director, Information Security Oversight Office (ISOO) chaired the meeting, and began by thanking Leonard Moss, President of the National Classification Management Society (NCMS), and all those NCMS professionals that worked behind the scenes to host this NISPPAC meeting. Minutes of this meeting were certified on October 6, 2014.

I. Welcome and Administrative Matters

After introductions of the members and those in attendance, Mr. Fitzpatrick welcomed everyone and reminded them that NISPPAC meetings are recorded events and that minutes of the meeting will be provided at a later date. He reminded those present that the primary function of the NISPPAC is to provide an opportunity for industry members to engage with the national level policy officials from key agencies in a dialogue about the state of the National Industrial Security Program (NISP). He emphasized that ISOO and all of the government officials who participate in this process, are continuously grateful for the dedication of industry professionals who sacrifice time from their busy corporate lives and gain the support of their corporate leaders to participate in this activity. He noted that the NISPPAC has a standing rotation of industry representatives for a specific term of service, and that today would be the last meeting for two of those representatives, Rosalind Baybutt and Michael Witt. The Chair presented each a token of the Committee's appreciation for their dedicated service, and a certificate of appreciation. He then asked Greg Pannoni, ISOO and 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 noted that there were four action items from the March 19, 2014 NISPPAC meeting. He explained that the first item was a request for the Office of the Undersecretary of Defense for Intelligence (OUSD(I)) to brief the procedures, guidance, and information (PGI) for safeguarding and protection of Department of Defense (DoD) controlled technical information (CTI). He stated that the Committee would hear an update from Valerie Heil during the DoD update. He noted that the second item resulted from the Chair's request for the Personnel (Security) Clearance (PCL) Working Group (PCLWG) to develop a new format for reporting their activities and metrics concerning the PCL process as it relates to industry. He assured the Committee that the PCLWG would continue to provide its performance metrics in the meeting's agenda packet as a matter of record, but they will no longer be briefed in detail. Additionally, the DFO noted that there was discussion at the last PCLWG meeting concerning the DoD Central Adjudication Facility (CAF) processes as they relate to interaction with the Defense Office of Hearings and Appeals (DOHA). Thus the Chair asked for a more comprehensive explanation of that process in terms of the adjudication actions for some of the cases that touch both DOHA and the DoD CAF. Mr. Pannoni noted that the third item stems from the Chair's request to the Office of the Director of National Intelligence (ODNI) to brief the Committee on the Intelligence Authorization Act's (IAA) 2013 report on security clearance determinations, and

he added that today's agenda packet contained a full copy of that report. The fourth item concerned the establishment of a Controlled Unclassified Information (CUI) Working Group (CUIWG) under the authority of the NISPPAC, and he noted that the working group had been established and held meetings with both government and industry representatives separately in order to discuss the way forward, particularly with regard to the oversight of industry under the proposed CUI regime and that it will continue to meet as its mandate evolves. (See Attachment 2 for a list of Action Items)

III. Reports and Updates

(A) DoD Update:

Valerie Heil, OUSDI, began the DoD update noting that the Defense Federal Acquisition Regulation (DFAR) clause for safeguarding CTI had been submitted to the Director of the Defense Acquisition Regulations Council (DARC) for its review and approval. She explained that an Aerospace Industries Association/National Defense Industrial Association working group met with the OUSD for Acquisition, Technology, and Logistics (AT&L) and representatives of the Chief Information Officer to discuss the clause and its implementation, and that those discussions were instrumental in assisting DoD in crafting and modifying the clause. Further, she noted that as soon as it is published they will inform the NISPPAC that it is available on DARC's part of the Defense Procurement and Acquisition Policies website. Next, she updated the NISPPAC on conforming change 2 of the NISP Operating Manual (NISPOM) and noted that the internal coordination process within DoD had been completed. She explained that this conforming change will include the requirement for establishment of an insider threat program, as well as an appendix D, which will cancel the 1995 supplement to the NISPOM. Further, she indicated that it contains other changes related to Chapter 8, as well as proposed text regarding the mandatory reporting of cyber intrusions from Section 941 of the FY 2013 National Defense Authorization Act. She advised that the DoD goal is to publish the NISPOM change by the end of 2014, with an effective date six months later. She indicated that discussions were on-going related to internal DoD guidance concerning national interest determinations (NID), which are required for access to proscribed information (Top Secret, Special Access Program (SAP), Sensitive Compartmented Information Communications Security, and Restricted Data information) for those companies that are cleared under special security agreements. She advised that DoD had completed internal coordination on a proposed internal DoD directive which will streamline the NID process. Finally, she reported that ISOO would host a NISPPAC working group meeting on June 24, 2014, to review the proposed revisions of the DD Form 254, " Contract Security Classification Specification," and its' instructions. She noted that industry would have another opportunity to comment when it went through the Office of Management and Budget (OMB) coordination process.

(B) The DSS Update:

Stan Sims, DSS Director, congratulated the winners of the 2014 James S. Cogswell Outstanding Industrial Security Achievement Award, and thanked Leonard Moss and the NCMS for hosting them at their 50th anniversary seminar. He noted that the topics of interest at the quarterly industry and DSS stakeholders meeting included: the impending changes with regard to the NISPOM conforming change 2, the NID process, details regarding the validation of PCLs, and

the planned reduction of overdue Periodic Reinvestigations (PR) by the end this year. Mr. Sims advised that a revised interim PCL process would not be instituted within industry until there was an automated process that would permit DSS to retrieve fingerprints and complete a review of the Standard Form (SF) 86, and the results of national agency checks. He described how DSS was embarking on an initiative to open up the stakeholder's meetings so that government colleagues, such as AT&L and the Defense Logistics Agency (DLA), who have processes that impact and support the NISP could attend. Finally, he explained that there was a lively discussion about cyber reporting and noted that OUSD(I) has solicited comments from industry, especially since there are challenges and/or confusion with the requirement

(C) Combined Industry Presentation

Tony Ingenito, Industry, began (see Attachment 3) by restating industry's appreciation to Ms. Baybutt and Mr. Witt for their dedicated service to the NISPPAC. He reminded the Committee that industry continues to devote much energy to shaping insider threat program initiatives and was currently monitoring eight initiatives ranging from the Counterintelligence Program Objective Memorandum, to memos from OUSD(I), and an insider threat memoranda dealing with the recent Washington Navy Yard incident. He stated that industry's goal is to share in a common approach with government that would ensure consistent insider threat policy implementation. He noted that industry had developed an effective framework for working CUI issues and initiatives. He described industry's support of the developments of common computer system requirements, and of their desire to share in the development of initiatives supporting implementation of any forthcoming training programs. With regards the new DFAR clause for DoD CTI, Mr. Ingenito cited industry's concerns and noted that they anxiously await the DoD PGI procedural resolution. He explained that one of the key areas in the DFAR clause was the identification of a contractual technical database, and that industry was attempting to ensure they have a solid understanding of those requirements, while understanding that this clause may eventually be incorporated under the CUI FAR clause. He noted that industry was currently monitoring nine separate cyber policy initiatives across the government, and providing ongoing and effective input to them. He advised that industry was anxiously awaiting the release of the NISPOM and conforming change 2, and the SAP supplement manuals. Mr. Ingenito reiterated that industry welcomed the changes made in direction by the PCLWG, as well as the transparency in DOHA cases. He welcomed the move of DOHA adjudicators to the DoD CAF, and noted that there was a clear plan to address long-term, middle-term, and new cases, so as to efficiently eliminate the backlog. He noted that industry believes that the key to moving forward lies in the electronic adjudication business rules, and anxiously awaits their impact in accelerating the process. Continuing, he mentioned that industry provided a number of items to our government partners through the Certification and Accreditation (C&A) Working Group (C&AWG) relating to Microsoft XP's end of life guidance and mitigation, and that they were seeing results from that effort. He noted that industry continues to work on the evaluation tools, and is prepared to engage with the Intelligence Community (IC) and SAP C&A communities to ensure that industry's concerns and issues could be addressed based on potential program implementation. He noted that industry was pleased with the progress on the DD Form 254 automation process, and was able to identify user requirements, for both present and future systems. He expressed appreciation for the prudent approach in using an existing AT&L system for hosting the new electronic DD Form 254 module, noting that as there is an ensured

infrastructure and years of implementation experience that can be assimilated into the new process. Mr. Ingenito stated that he will continue to flow information to the Memorandum of Understanding groups so that they will in turn share with their membership and get needed feedback on issues and incongruities in industrial security policy. Finally, he noted that industry participated in the system requirements phase for DSS' National Industrial Security System (NISS), and thanked Quinton Wilkes, Industry, and Michelle Sutphin, Industry, for their contributions to that initiative. The Chair then reminded the Committee that ISOO would now begin the process of working with the industry representatives on the nomination of two new industry representatives to replace those leaving, and hoped that these new members will be in place by the next NISPPAC meeting.

(D) PCLWG Report

Mr. Pannoni introduced the PCLWG's report (see Attachment 4) by providing a description of recent procedural changes. First, he reminded the Committee that much of the substantive work of the NISPPAC is accomplished by the various working groups, such as the PCLWG. He noted that this Group has had an impact in the development of mechanisms that reduce the time required for security clearance submissions, investigations and adjudications. He provided an overview of the elements for refocusing the PCLWG to address industry's primary issues and concerns. He reminded the Committee that the metrics data they have been accustomed to viewing would remain in the agenda packet, but that not all of the individual elements would be reported or discussed at each meeting. He noted that Perry Russell-Hunter, DOHA, would speak to the procedures governing DOHA cases. Further, he noted that the PCLWG would focus on several key issues to include discussions of needed improvements to business rules for e-adjudication, as well as the need to study HSPD-12 e-adjudication criteria so as to enhance our own rates of success; the triage of adverse information reports; the overdue PRs reflected in the Joint Personnel Adjudication System (JPAS); reports relating to the DoD Call Centers' inconsistency in providing information; interim clearance process changes; and engagement of industry for suggestions to improve the clearance validation process. The Chair then called on Christy Wilder, ODNI, to present the performance metrics from the ODNI, as the Security Executive Agent (SEA).

Ms. Wilder updated (see Attachment 5) the NISPPAC on the results of the, "2013 Intelligence Authorization Act Report on Security Clearance Determination." She described the first year's report (2011) as only capturing the number of people who were actually granted access to classified information, and noted that in the second year's report (2012), the methodology was altered to focus on the number of individuals who were cleared, but not granted access to classified information. She advised that in the third year's report (2013) the focus became why the numbers continued to reflect a significant increase despite a substantial number of individuals having been debriefed from access, and attributed this anomaly to the fact that debriefed individuals retain security clearance eligibility for two years, causing the numbers to remain high. Further, she noted that for this past year we reported the total numbers of eligible, meaning those people who were in access, as well as those who were investigated and adjudicated, but not briefed into access. Ms. Wilder clarified that the numbers in the 2013 report also reflected both those with eligibility and in access, as well as those with eligibility and not in access. She noted that the numbers of those in access decreased from 2012 to 2013, and that those without access increased. She noted that the 5.1 million clearance figure is indicative of

those that are both in access and not in access, and that the 3.1 million people who are actually in access are the ones validated by the agencies to the ODNI. She described a second initiative which asked the agencies to review their overdue PRs and identify and submit those within their highest risk population. She noted that ODNI would continue to work with agencies to ensure this initiative is being met. She noted that these two initiatives are being tracked by the program management office and would be reported at the next NISPPAC.

The Chair noted that efforts such as the 120-day report and DoD's study of the Washington Navy Yard tragedy had produced initiatives in the OMB and DoD that are of interest to this Committee. He explained that the ODNI, as the SEA, has representatives on the Suitability and Security Performance Accountability Council, and that the suitability executive agent is represented today by Lisa Loss, Office of Personnel Management (OPM). He noted that ISOO, as one of the other agencies represented on that Council, has a primary role in bringing the industry perspective and impacts into that discussion. The Chair also pointed out that with the many government efforts resulting from the Washington Navy Yard tragedy, both DoD's internal processes as well as those of the NISPPAC need to identify which initiatives would be important for the NISP community. He stated that the administration's approach to such initiatives is highly focused on both the transparency of those efforts and on the accountability for their accomplishment, and that there exists an environment where one can ask where things are and what is being planned. He noted that there is a published version of the 120-day report on the OMB website, and recommended that members familiarize themselves with this report, as well as initiatives relating to clearance reform.

Steve DeMarco, DoD CAF, updated the Committee on CAF activities (see Attachment 6). He noted that in January 2014, the CAF had a backlog of approximately 14,500 cases and that by May 2014 that backlog, had been reduced by 50%; due primarily to an infusion of additional resources and the implementation of new strategies. He described their goal as to reduce both inventory and processing times so that they comply with Intelligence Reform and Terrorism Prevention Act (IRTPA) requirements. He emphasized that the CAF completes about 180,000 adjudications for industry every year, and issues a Statement of Reasons (SOR) for about 4% of that caseload. He described a spike in the adjudication of initial investigations in the April-May timeframe due to emphasis on reducing the backlog. Mr. DeMarco further explained the SOR process, noting that if the CAF cannot favorably adjudicate an individual, they draft an SOR, which then goes to DOHA for a legal sufficiency review. Then, if DOHA concurs, the case is returned to the CAF who in turn issues the SOR to the subject. He continued, explaining that when the CAF gets the response back it's forwarded to DOHA for their review. He pointed out that the CAF has sent over 44,000 cases to DOHA since the beginning of FY 2013, with 40% of these having been sent since the beginning of this year. He detailed that it took 35 to 37 days for the sufficiency review, an average of 13 days to get the SOR completed and to the subject, as well as an average of 45 days for an individual to respond back to the CAF. He noted that getting information on cases at DOHA is now simpler since the DOHA adjudicators have been merged into the CAF and the SORs are processed through the CAF. He offered that generally, if an individual has received and responded to an SOR, it is with DOHA, and if they haven't responded, it is with the CAF.

Perry Russell-Hunter, DOHA Director, thanked the NISPPAC for providing the opportunity to clarify issues regarding DOHA processes, and he offered appreciation to the CAF for their

excellent effort since consolidation (see attachment 7). He informed the Committee that when JPAS indicates a case is with DOHA, such information is often inaccurate. He noted that, contrary to what is reported in JPAS, there are far less than the 10,000 cases reported at DOHA, and indicated that the number is actually around 1,000 cases that include 520 cases pending with the attorneys at DOHA for SOR review, and about 200 cases in the hearing process. He also noted that about 100 cases are in for a decision on a written record -- that's when the individual says they don't want a hearing; but rather prefer that an administrative judge to make the decision. He identified another 40 cases that are before the DOHA appeals board, which is used when an individual is dissatisfied with the administrative judge's decision and formally appeals it to that panel. He stressed the importance of issue resolution and noted that if the industry Facility Security Officer can help the individual include that information on the SF 86 then both OPM and the DoD CAF will have captured the information, resulting in a much faster case resolution. He stated that by the time a case gets to DOHA it is anticipated that many of the issues that result in SORs have already been addressed. He reiterated that the CAF consolidation meant that if a case is being adjudicated, it's at the DoD CAF, and if a SOR was issued and the responses submitted, then that case is at DOHA. He noted that the vast majority of DOHA adjudications are favorable, and that historically less than 2% of all industrial security clearance applications, to include PRs, result in unfavorable adjudications as either denials or revocations. He explained that the standard has become: the written statement of reasons; the opportunity to respond in writing; the ability to appear personally, to cross-examine anybody who's made an accusation; and finally a detailed decision explaining the pros and cons and ultimately why the decision was made. He noted that once a case is going to be denied or revoked, and once the adjudicator has concluded that it is the appropriate thing to do, that's when they draft the SOR, which is then reviewed by the DOHA department counsel, prior to issuance. He reminded everyone again that it's never too early to provide mitigating information, and noted that NISPOM, section 2-202 is the governing authority for such action.

The Chair asked the PCLWG to explore the most appropriate way for us to understand the status of those 10,000 errant entries in JPAS and to know when they're diminishing or gone. Mr. Russell-Hunter responded that this topic was discussed during an NCMS panel discussion, and that the DoD CAF Director indicated it was impractical to try to change 10,000 or more JPAS entries that incorrectly reflect cases being at DOHA, and suggested that we just work through them until they are reduced and advised everyone to call to ascertain the location of a specific case file. The Chair remarked that this was the sort of aggregate understanding he was suggesting for the November meeting, that is, how much of that 10,000 have been worked through? He noted that there is now an understanding of the post consolidation procedures at DoD CAF, clarification about how SOR cases go through DoD CAF's process, as well as about what cases are with DOHA. He opined that as the DoD CAF catches up on its backlog, they should get to a state where they are able to track actual case status through their workload. Mr. Russell-Hunter explained that DoD will be working through those cases, because the vast majority are favorable cases, with financial issues that can be easily resolved, and thus the problem will eventually be eliminated. The Chair reiterated that at the November meeting he would like an update on how many of the erroneous entries of DOHA cases have been resolved.

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

Tracy Brown, DSS, updated the Committee on the C&AWG activities (attachment 8). Ms. Brown noted that over the last year the group completed several major initiatives. She described the first as the publication of the Industrial Security Field Operations Process Manual, which became effective May 2014, and the release of the new System Security Plan (SSP) template that supports the requirements of the process manual. She noted that over the last year the C&AWG's activities included the release of a new configuration baseline for both Windows 7 and Windows server 2008. She forecasted the group's activities for the upcoming year, noting that they will be working with the other Cognizant Security Agencies (CSA) to identify their compliance processes and where they can be leveraged across the NISP. She reviewed specific metrics regarding approvals by the Office of the Designated Approval Authority, noting that they continue to process interim approval-to-operate (IATO) in 20 days, and that the implementation of the straight to approval-to-operate (SATO) guidelines have not resulted in a significant decrease in the 23-day processing time. She explained that the primary discrepancy seen during the plan submission process is that SSPs are still missing attachments, or they're incomplete, and that during the on-site validation process, the top issue being observed is that security relevant objects are not being protected. She noted that security relevant objects are specific to the facility, so Information System Security Managers have to work with their Information System Security Professionals to better identify items that are considered security relevant in order to address the problem. She noted that IATO to approval-to-operate (ATO) timeframes were averaging 104 days. She emphasized the key takeaways as: SSPs are being processed and reviewed in a timely manner; most common deficiencies to SSPs include missing attachments and documentation not being tailored to the system; onsite validations are being completed in a timely manner, and most common vulnerabilities identified included security controls auditing and unprotected security-relevant objects. She concluded, noting that they will continue to focus on processing more SATOs whenever practical, because they increase efficiency and reduce risk.

(F) Controlled Unclassified Information Working Group (CUIWG) Report

Mr. Pannoni updated the Committee on activities regarding the implementation of the CUI program (see Attachment 9). He noted that the newly established CUIWG has met twice, first with the government members and then with the industry partners. He reviewed the areas of focus, emphasizing that the CUI FAR clause would be the document that drives all program and information technology requirements for industry. He explained that the CUI executive order requires a moderate level of confidentiality, and that ISOO is working with the National Institute of Standards and Technology (NIST) and OMB on this issue. He noted that the CUIWG was mindful of industry concerns and will continue to focus on these issues. Mr. Pannoni explained that the CUI FAR clause will establish a process that is based on a self-certification and selective validation model being developed by the executive agent. He noted that a self-certification approach was appropriate because of the immense numbers of contractors (potentially 700,000) doing business with the government and having access to CUI. He explained further that ISOO was working with the General Services Administration (GSA), which already has an automated award management system in place to set up a repository for CUI self-certifications, and noted that GSA was receptive to supporting the effort. He then explained the timeline for the phased implementation of the FAR clause and NIST publication for CUI, and noted that April 2014 was the starting point for both actions, with the CUI implementation document projected for publication in the Code of Federal Regulations and provided for comment in FY 2015. He

explained that the NIST standard and guidelines for industry will be an important document because it will set forth the array of security controls that will be required to achieve a moderate level of confidentiality, as well as allow for compensatory measures and alternatives for those industry partners that can demonstrate that they have controls in place that meet the NIST standard.

The Chair reiterated that the goal was to provide a sense of the approach to, as well as the timing of, a number of overlapping activities, some of which are in progress, and others which have a dependency on the formal conclusion of the federal rule. He noted also that CUI implementation by any department or agency is contingent on the Federal Register publication of the implementing directive in the spring of 2015. He explained that the promulgation of the federal rule is required prior to the formal processing of a FAR clause and thus ISOO has begun to educate the acquisition community with the needs of the CUI executive order and our regulatory approach. He reiterated that the FAR Council and NARA, as the executive agent for the CUI program continue to socialize CUI with the Office of Federal Procurement Policy, and the other FAR Council members, which include the DOD acquisition community, GSA, and NASA. The Chair explained that ISOO expects to present a package in the spring of 2015 which will include our final federal rule, the implementer for the CUI executive order, and the NIST standards and guidelines for industry. He noted there will also be applicability to both the contractor community and other nonfederal partners, such as the state/local/tribal entities that have some CUI in systems that they need to protect. The Chair noted that their approach had been validated as evidenced by the strong partnership with NIST as well as the ongoing activities with the FAR Council as we address all their concerns and shape the FAR and the regulatory package appropriately.

The Chair noted that the self-certification and selective validation process will be elective on the part of the government contracting authority. He explained that NISP participants may be part of a company that has both NISP and non-NISP contracts with federal government entities, and that they will have to make a corporate representation to the government that they have self-certified their compliance with the standards. He noted that the guiding principle in the CUI approach is to have a CUI self-certification function that will address any corporate entity, and that we want to ensure our NISP partners have a way that can assure that DoD, as the executive agent for NISP, has a common understanding and approach as to what tools are needed with regard to a CUI presence. He advised that recognition that national corporate entities deal with the government in many ways requires an approach which harmonizes the appropriate representations to be made about a company's program to both protect classified under the NISP and other information in the CUI context. Mr. Pannoni reminded the Committee that industry should question their applicable government customer if a CUI requirement in a contract is tied to a federal regulation, statute, or government-wide policy that says it must be protected, as well as if specified controls are consistent with moderate levels of confidentiality for information systems processing such information. The Chair noted that while much of the information that is CUI already exists, the formal CUI program will provide a more uniform and consistent way of approaching such information, by way of a FAR clause that prescribes a definitive set of requirements for protecting CUI. He also noted that while one could look in the CUI Registry today and see that information on its way to becoming CUI, the underlying question is if there is a federal regulation, statute, or government-wide policy that requires that it be protected. He

advised that in the future this FAR clause will negate custom clauses currently in use and substitute a singular set of requirements into industry contracts that requires protection of CUI. The Chair then described his recent testimony before the House Oversight and Government Reform Committee regarding CUI, and noted that there is confusion about who designates something as CUI. He acknowledged that there are 157 laws that require information to be protected, and that with CUI we are trying to stretch a new umbrella of policy and procedure over an existing environment in order to make it more orderly. He concluded that while the process looks new, the underlying requirement for protection has had a very long life in both statute and regulation.

(G) E.O. 13587 Update

The Chair introduced Alegra Woodard, ISOO, who provided a follow-up to the Classified Information Sharing and Safeguarding Office presentation at the last meeting. Ms. Woodard provided an update (see Attachment 10) regarding the many efforts and activities that are being led by the National Insider Threat Task Force, (NITTF), as it relates to the implementation of Executive Order (EO) 13587, *"Structural Reforms to Improve the Security of Classified Networks, and the Responsible Sharing and Safeguarding of Classified Information*". She recalled that this E.O. had its genesis in the acts of Private Bradley Manning, in which he passed over 700,000 documents and video clips to WikiLeaks. The E.O. also established the Senior Information Sharing and Safeguarding Steering Committee, and the NITTF, which had responsibility for preparing the National Insider Threat Policy and Minimum Standards. She explained that the insider threat policy and minimum standards prescribe that each department and agency will establish an insider threat program, and noted that this program remains one of our top national security priorities, as it is intended to deter cleared employees from becoming insider threats, detect insiders who pose a risk to classified information, and mitigate that risk through administrative, investigative, and other response activities. She detailed the initial 180-day requirement which required agency heads to designate a department or senior agency official (SAO) for insider threat; establish a policy to be signed by the agency or department head; and create a plan of action to reflect how these requirements would be met. She noted that over the past year members of the NISPPAC met with the NITTF to develop the policies for applying the insider threat policy and minimum standards for industry which will result in changes to the NISPOM and revisions to 32 CFR Part 2004, (the NISP implementing directive). She concluded, noting that recent events remind us that we have to continue to establish the path for coordinating and establishing the policy for the insider threat program.

The Chair noted that in addition to the policy changes underway, other activities, such as a government-wide meeting of SAOs recently hosted by the NITTF at the National Archives and Records Administration (NARA), where both the Deputy Attorney General and the Principal Deputy of National Intelligence identified the urgency of government agencies to designate an SAO for insider threat, develop an insider threat a policy and directive, and implement a program that meets E.O. 13587 requirements have been put into effect. The Chair noted that program startups are difficult, and wanted to give the Committee a sense of its progress. Mr. Sims noted that the government does have a plan in which they're evaluating how well they are doing in meeting those requirements for the NITTF, and that it is serious about evaluating their systems. He opined that the message to industry is to get ahead of the process, and to make sure they are

meeting the minimum standards, as there will be an evaluation of industry, similar to the one for the government.

IV. New Business

The Chair noted that Valerie Heil had spoken earlier in the meeting of the ongoing work with the DD Form 254, and that Booker Bland, DSS, as well as representatives from OUSD, DoD AT&L, and the DLA were here to introduce the Committee about a system called the NISP Contract Classification System (NCCS). Mr. Bland provided an update (see Attachment 11) on the status of the NCCS, also known as the DD Form 254 database. He reminded the Committee that a DD Form 254 conveys security requirements related to the performance of a contract. He explained that the goal of NCCS is to reduce and ultimately eliminate the paper process, and noted that there is currently no way of determining the exact number of classified contracts across the Executive Branch, nor the security requirements that accompany those contracts. He noted that the NCCS will be a role-based, privilege-based system, enabled by Public Key Infrastructure, with a projected operational date of March 2015. He noted that DSS partnered with the DoD AT&L to build NCCS onto the DoD AT&L's Wide Area Workflow (WAWF) Network. Mr. Bland noted that the first iteration of NCCS will be accessed through the National Information Protocol Routing network (NIPRNet), with future versions being discussed for the Secure Information Protocol Routing Network (SIPRNet) and the Joint Worldwide Intelligence Communications System (JWICS) platforms.

Bruce Propert, DoD AT& L, provided an overview of the WAWF explaining that it was built some years ago to automate the receipt and acceptance process for making vendor payments. Subsequently, contractors were permitted access to describe their products so that WAWF could route the information to the buyer of the item or service, who in turn would notify the payment office. The payment office would then match the contract to an invoice and, upon acceptance, pay the contractor. He noted that WAWF has saved, in interest alone, more than the system costs to operate every year. He added that WAWF handles millions of transactions and hundreds of thousands of users in both industry and government annually and that approximately 55,000 companies used it last year. He described WAWF as a system that takes what was originally a paper form, routes it from the person who created it to all the people who have a need for access, gets it approved at each of the steps in the process, and sends it on to the final user point. It is then converted into a data-driven platform, permitting the client to query the results. Mr. Propert explained that when his office became aware of the requirement for NCCS they notified DSS that they might have a system that could support the electronic DD Form 254 effort. Thus, it was decided that rather than build an entirely new system they would determine if WAWF could manage the DD Form 254 process. He emphasized that the WAWF is not only a system serving invoicing and acceptance, but one that has added miscellaneous payments, government property transfers, a capability for vendors to view payments, and a tool for appointing contracting officer representatives. He noted that in adapting the NCCS process in this way, our industry partners are permitted access to a system with which they are already familiar.

James Johnson, DLA, then described how the first iteration of NCCS will be included in the WAWF 5.7 release in April 2015. He explained that DSS has presented a list of requirements which will be utilized in the initial release, and that additional requirements are planned for the subsequent 5.8 release scheduled for October 2015. He noted also that the backup slides

accompanying this presentation provide the full detailed schedule of projected events between now and initial release. The Chair asked how industry would participate in this effort, and how would they know when to begin working from the process. Mr. Sims responded that NCCS will be rolled out in the exact same way as they do all other systems, that is, through a series of notices posted on their website, and noted that DSS will prescribe a specific period of time for implementation, so there should be no surprises. The Chair expressed his appreciation to Mr. Propert for giving this presentation and for relating a great story, especially one where someone offered assistance, as was done here, which resulted in this terrific opportunity for improvement. Mr. Sims heartily agreed that the system would save significant time, in as much as it services the exact same community that uses that system today. He addressed questions of responsiveness of the system, stating that DoD AT&L has assured DSS that the configurations and changes will be responsive to their requirements. Mr. Propert agreed, noting that they will ensure that all stakeholders, including industry, are invited to any design reviews or testing processes, and that in the governance process, all stakeholders will be represented.

Ms. Heil then spoke of the recent DSS and DLA presentations to the NISP CSAs, and noted that one of the questions asked was whether WAWF would employ a current Personal Identity Verification (PIV) card. Mr. Propert concurred that the intent in this part of the WAWF process would be to access via a PIV card. Ms. Heil cautioned that there are costs associated with the procurement of PIV cards that must be planned and budgeted for by industry, so it is prudent to begin this planning process soon. Mr. Johnson acknowledged that he had communicated with the WAWF developers to get an understanding of what it would take to provide a PIV or Common Access Card process for industry. He noted that since it is a government system, it requires extending their technology to make sure that industry has the right PIV cards in order to ensure compatibility. The Chair noted that when DoD, as the executive agent for the NISP, brings all of its influence to bear on an issue, great things like this can happen, and that this represents a real testament to everyone's efforts.

V. General Open Forum/Discussion

The Chair opened the meeting to comments from the attendees, and asked for inputs on any issues anyone would like to raise. There were no comments subsequent to this offer, and the Chair again took the occasion to thank the NCMS, and offered Mr. Moss an opportunity to bring the NCMS annual seminar to a close. Mr. Moss recognized the efforts of the NCMS Board of Directors and Seminar Committee in making the conference such a success. He announced that the 2015 Seminar will be at the Bellagio Hotel in LasVegas, Nevada.

VI. Closing Remarks and Adjournment

The Chair reminded everyone that the next NISPPAC meeting is scheduled for November 19, 2014, at NARA. He noted that the budget forecast for FY 2015 maintains the status quo with previous budgets, and that as such there will be no travel funds available for our industry representatives. He reiterated that he was grateful for all who attend the meetings on their own, and thanked their company leadership for sponsoring their travel. He reminded the members that a dial-in capability will again be available for any who cannot travel to the meetings. The Chair adjourned the meeting at 11:57 a.m.

Attachment #1

Attachment 1

NISPPAC MEETING ATTENDEES/ABSENTEES

The following individuals were present at the June 19, 2014, NISPPAC meeting:

• John Fitzpatrick,	Information Security Oversight Office	Chairman
• Greg Pannoni,	Information Security Oversight Office	DFO/Presenter
• Stan Sims	Defense Security Service	Member/Presenter
• Michael Hawk	Department of State	Member
• Anthony Lougee	National Security Agency	Member
• Kathy Berry	Department of Justice	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
• J.C. Dodson	Industry/ MOU Representative	Member
• Eric Dorsey	Department of Commerce	Alternate
• Anthony B. Smith	Department of Homeland Security	Alternate
• Carl Pietchowski	Department of Energy	Alternate
• Valerie Heil	Department of Defense	Alternate/Presenter
• Valerie Kerben	Nuclear Regulatory Commission	Alternate/Presenter
• Kathleen Branch	Defense Security Service	Alternate
• Kenneth Campbell	Central Intelligence Agency	Alternate
• Christy Wilder	Office of the Director of National Intelligence	Presenter
• Lisa Loss	Office of Personnel Management	Presenter
• Steven DeMarco	Department of Defense	Presenter
• Tracy Brown	Defense Security Service	Presenter
• Booker Bland	Defense Security Service	Presenter
• Bruce Propert	Department of Defense	Presenter
• Perry Russell-Hunter	Department of Defense	Presenter
• James Johnson	Defense Logistics Agency	Presenter
• Alegra Woodard	Information Security Oversight Office	Presenter
• Chris Forrest	Department of Defense	Attendee
• Kathy Branch	Defense Security Service	Attendee
• Christine Beauregard	Defense Security Service	Attendee
• Dan Purtill	Department of Defense	Attendee
• Laura Hickman	Defense Security Service	Attendee
• Kimberly Lew	Department of Homeland Security	Attendee
• Keith Talley	Department of Housing & Urban Development	Attendee
• Matthew Jacobs	Defense Logistics Agency	Attendee
• Jay Buffington	Defense Security Service	Attendee
• Rebecca Bernier	Defense Security Service	Attendee
• George Goodwin	Defense Security Service	Attendee

• Karen Duprey	Industry/ MOU Representative	Attendee
• Mark Rush	Industry/ MOU Representative	Attendee
• Kirk Poulsen	Industry/ MOU Representative	Attendee
• Leonard Moss, Jr.	Industry/ MOU Representative	Attendee
• James Shamess	Industry/ MOU Representative	Attendee
• Stephanie A. Sutton	Industry	Attendee
• Sheila Garland	Industry	Attendee
• George Fronske	Industry	Attendee
• Mitch Lawrence	Industry	Attendee
• Michael Malmgren	Industry	Attendee
• Yvonne Guzman	Industry	Attendee
• Klaus Herwig	Industry	Attendee
• Dianne Raynor	Industry	Attendee
• Eric Helthall	Industry	Attendee
• Oliver McLean	Industry	Attendee
• Quinton Wilkes	Industry	Attendee
• Chuck Nio	Industry	Attendee
• Dorothy Rader	Industry	Attendee
• William Grosley	Industry	Attendee
• Michelle Sutphin	Industry	Attendee
• Rhonda Peyton	Industry	Attendee
• Dennis Arriaga	Industry	Attendee
• Katie Timmons	Industry	Attendee
• Cathe Kaohi	Industry	Attendee
• Tameka Watts	Industry	Attendee
• Debbie Young	Industry	Attendee
• Beverly Harmon	Industry	Attendee
• William Henderson	Industry	Attendee
• Dela Williams	Industry	Attendee
• Robert Welch	Industry	Attendee
• Ann Martick	Industry	Attendee
• Sheryl Daniels	Industry	Attendee
• Mary Eddington	Industry	Attendee
• Jen Kirby	Industry	Attendee
• Allison Zweil	Industry	Attendee
• Natalia Averett	Industry	Attendee
• Gussie Scardina	Industry	Attendee
• Vince Jarvie	Industry	Attendee
• Josie Pearson	Industry	Attendee
• Harriet Sheffield	Industry	Attendee
• Mark Mondazzi	Industry	Attendee
• Michele O'Donnell	Industry	Attendee
• Jeff Walacu	Industry	Attendee
• Richard Knight	Industry	Attendee
• Aprille Abbott	Industry	Attendee
• Kathryn Hare	Industry	Attendee

• Stephanie Brewer	Industry	Attendee
• Doris Parr	Industry	Attendee
• Sarah Rudman	Industry	Attendee
• Jennifer Graham	Industry	Attendee
• David Best	Information Security Oversight Office	Staff
• Robert Tringali	Information Security Oversight Office	Staff
• Joseph Taylor	Information Security Oversight Office	Staff

Agencies Not Represented:

- Department of the Army
- Department of the Air Force
- National Aeronautics & Space Administration
- Department of the Navy

Attachment #2

Action Items

From 6/19/2014

NISPPAC meeting

1) ISOO, through the NISPPAC Executive Secretariat, will begin the process for nominating two new industry representatives for appointment to the Committee, prior to the November meeting.

2) The PCL Working group will:

A) Study the e-adjudication process to see if, with some adjustments, it can be made more effective for the process of adjudication of PCLs for industry.

B) Examine how to eliminate the problem in JPAS that inaccurately depicts the number of open cases at the Defense Office of Clearance and Appeals (DOHA), when report to the Committee on efforts to eliminate the inaccurate reporting.

(C) Look at the security clearance validation process to see if those being adjudicated for access to classified information are in fact being accessed as required. Report to Committee on number of persons in industry being approved for a clearance and then not being accessed to CNSI.

Attachment #3

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

Industry

19 June 2014

Outline

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

National Industrial Security Program

Policy Advisory Committee Industry Members

Members	Company	Term Expires
Rosalind Baybutt	Pamir Consulting LLC	2014
Mike Witt	Ball Aerospace	2014
Rick Graham	Huntington Ingalls Industries	2015
Steve Kipp	L3 Communications	2015
J.C. Dodson	BAE Systems	2016
Tony Ingenito	Northrop Grumman Corp.	2016
Bill Davidson	KeyPoint Government Solutions	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
  - Developing policies and minimum standards for sharing classified information
- Need consistent requirement across all the User Agencies relating to implementation SOPs.
- Monitoring eight separate policy/directive actions across the government and providing input where possible.

Security Policy Update

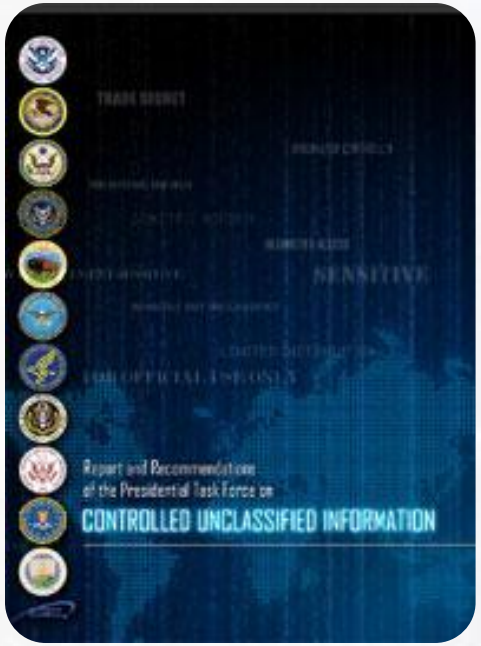
Executive Order #13556

EO # 13556

Controlled Unclassified Information (CUI)

4 NOV 2010

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



- Next Steps
  - Monitor development of marking, safeguarding, dissemination and IT Security policy
  - Implementation plan and NIST guidance development
- Meeting with ISOO CUI Executive Agent Team on 10 Jun. Discussed program & implementation plan. Positive feedback.

Security Policy Update

Defense Federal Acquisition Regulation (DFAR), Subpart 204.73: Safeguarding Unclassified Controlled Technical Information:

- Heightened security safeguards
  - Implementation of NIST 800-53 Safeguards required on all systems containing "controlled technical information"
    1. Access control
    2. Awareness and training
    3. Audit and accountability
    4. Configuration management
    5. Contingency planning
    6. Identification & authentication
    7. Incident response
    8. Maintenance
    9. Media protection
    10. Physical and environment protection
    11. Program management
    12. Risk assessment
    13. Systems and communication protection
    14. System and information integrity
- Incident reporting required
  - Possible exfiltration, manipulation, or other loss or compromise of any unclassified controlled technical information
  - Any other activities that allow unauthorized access to unclassified information systems on which unclassified controlled technical information is resident on or transiting

Concerns

- Cost affective implementation plan and data marking/identification guidance of CTI is critical to successful implementation.
- Some UA notifications indicated intent to modify existing contract with clause, but not fund implementation.
- Awaiting Procedure, Guidance & Instructions (PGI) from AT&L.

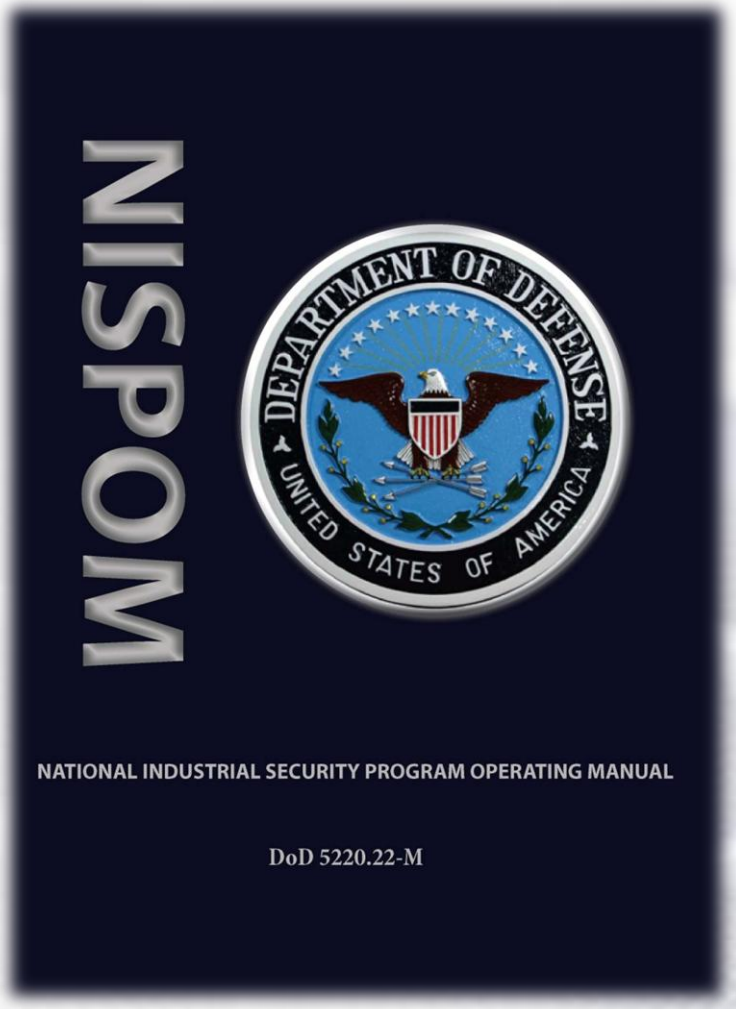
Security Policy Update

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
- IMPACT
  - Other government agencies moving forward with imposing IT Security measures and requirements
    - Controls are being interpreted differently by various programs and agencies, this creates multiple/duplicative approval tracks for industry.
    - Monitoring nine separate Cyber policy/initiatives actions across the government and providing input where possible.

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
  - Industry working under a series of interim directions
  - Strong industry coordination for this interim direction is inconsistent
  - Delay of single, integrated policy is leading to differing interpretation of interim direction by user agencies

National Industrial Security Program

Policy Advisory Committee Working Groups

- Personnel Security
  - Working group moving out to address areas of concern.
    - DOHA SOR Process. Providing transparency with caseload and aging of cases.
    - PCL information sharing across agencies
    - Risk in adjudication backlog. Sequestration recovery plan.
    - E-adjudication business rules.
  - Enhanced Security Clearance Act of 2013 impact (Involvement in implementation plan development)
- Automated Information System Certification and Accreditation
  - Provided DSS & OSD suggested XP End of Life guidance to mitigate the impacts across existing programs, including testing equipment.
  - Initiative to evaluate tools for use in the C&A process.
  - Engage IC and SAP C&A Communities relating to CC #2 (Note: will push the C&A process to CSA provided guidance. Engaging industry in the guide development).

National Industrial Security Program

Policy Advisory Committee Working Groups (cont.)

- Ad-hoc
  - NISPOM Rewrite Working Group
    - Awaiting further actions relating to NISPOM and Conforming Change #2
  - NISP Contractor Classification System (NCCS) – Automated DD254 system
    - Positive meeting with program team & AT&L this month.
    - Applaud the utilization of the AT&L WAWF system for the NCCS module. Cost effective infrastructure and ability to provide system in a timely fashion.
    - Standing by for further development meetings and the ability to beta test.
  - Development of National Industrial Security System (NISS)
    - Participating on the system requirements phase and standing by for further development meetings.
- ISOO sponsored Ad-hoc SAP Working Group
  - Meetings as necessary in 2014
  - SAPCO's and Industry (CSSWG) working changes on SAP Security Manuals (Vol 1 thru 3).

Attachment #4

Personnel Security Working Group (PCLWG) Report

- NISPPAC action items from 3/17/2014 meeting: (See attachment 2 in folder)

  - New reporting process.
  - Performance metrics data from OPM and PSMO are in folders and will be posted with NISPPAC minutes.
  - DOHA to provide details of current process for identifying and tracking cases truly in due process.
  - Focus on addressing industry's primary issues and concerns.

-Discussion Items:

  - Discussion of needed improvement to business rules for e-adjudication.
    - Improved review of front-end information, particularly financial data.
    - Consider HSPD-12 e-adjudication criteria when there are no issues.
  - Information Sharing & Alerts - - -Triage of adverse information reports.
  - Overdue PRs reflected in JPAS.
  - Call center(s) consistency in providing information.
  - Interim clearance process change.
  - Validation of need for access to classified information.

Attachment #5

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Industry Performance Metrics

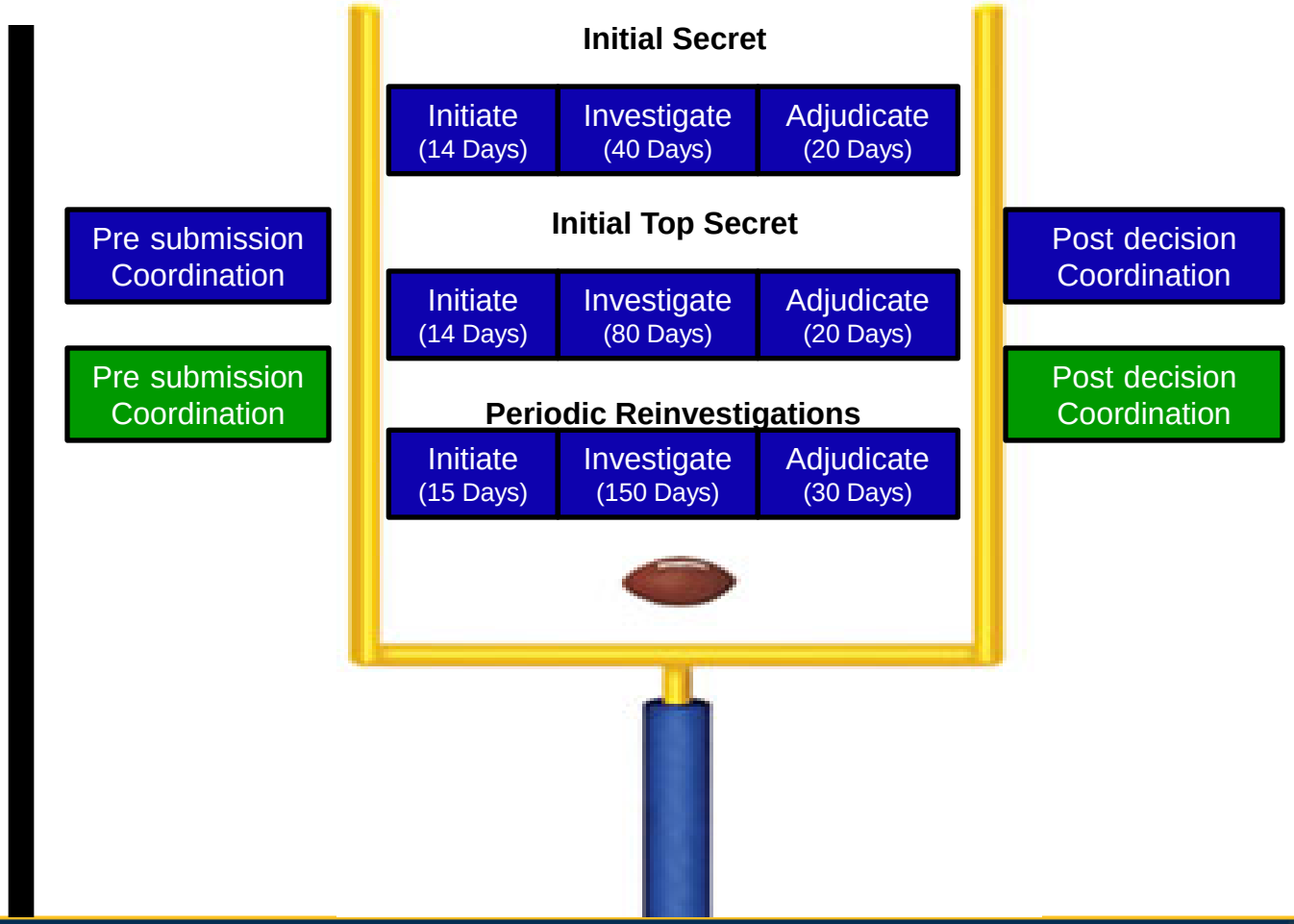
ONCIX/Special Security Directorate

LEADING INTELLIGENCE INTEGRATION

PCL Working Group
28 May 2014

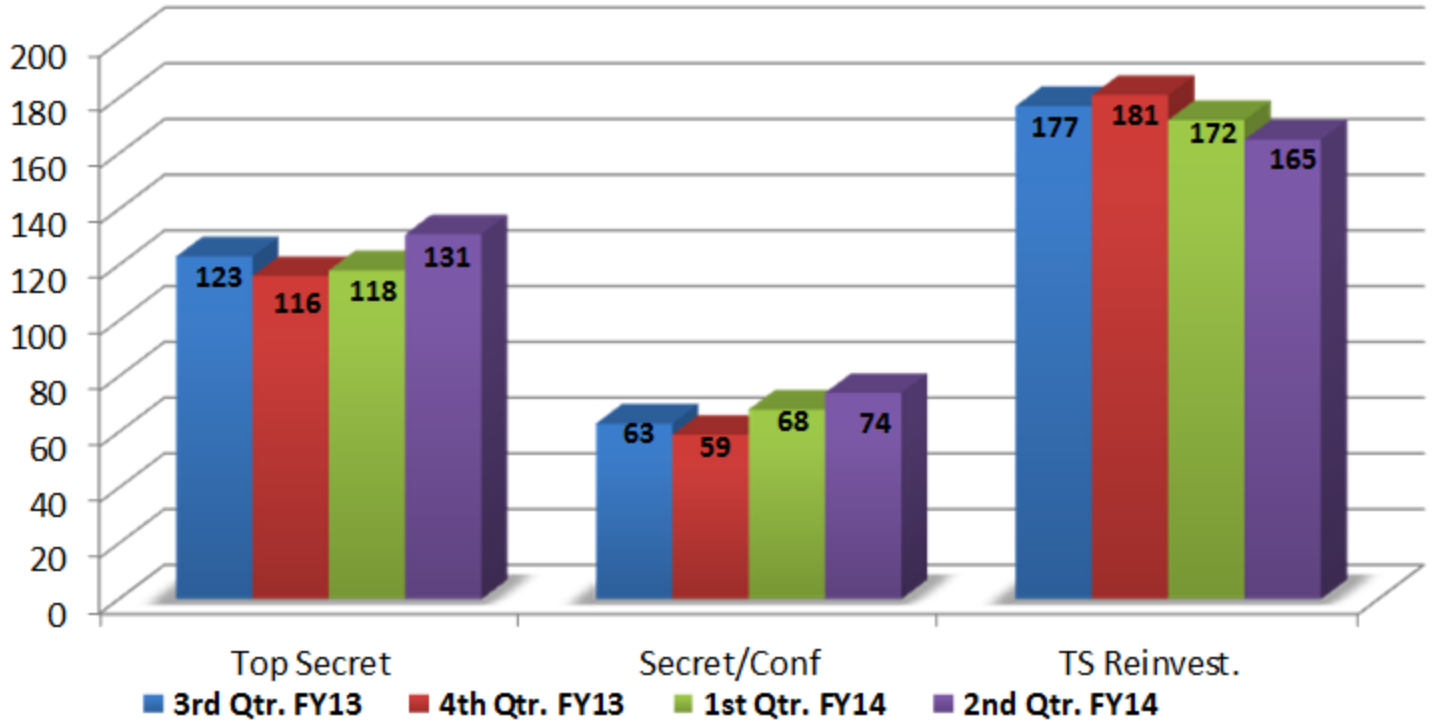
Performance Accountability Council(PAC) Security Clearance Methodology

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



Timeliness Performance Metrics for IC / DSS
Industry Personnel Submission, Investigation & Adjudication* Time

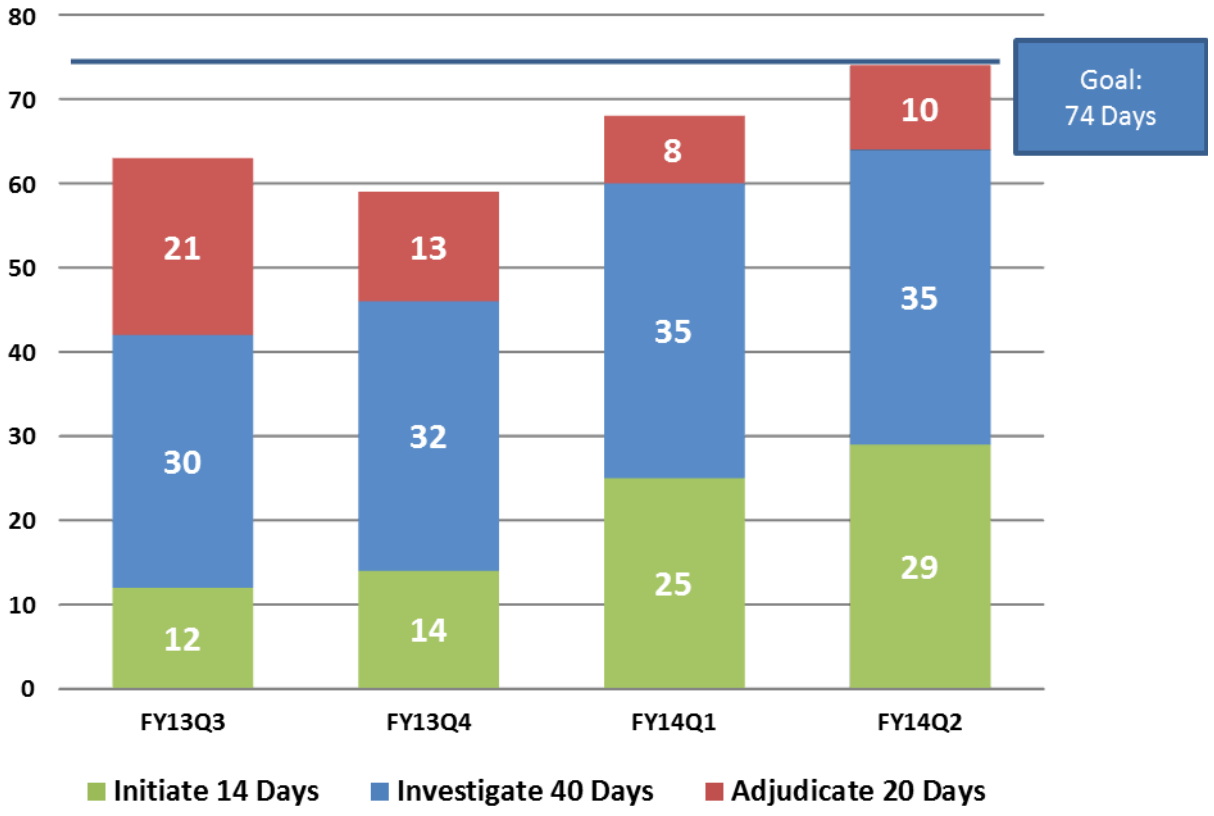
Average Days of Fastest 90% of Reported Clearance Decisions Made



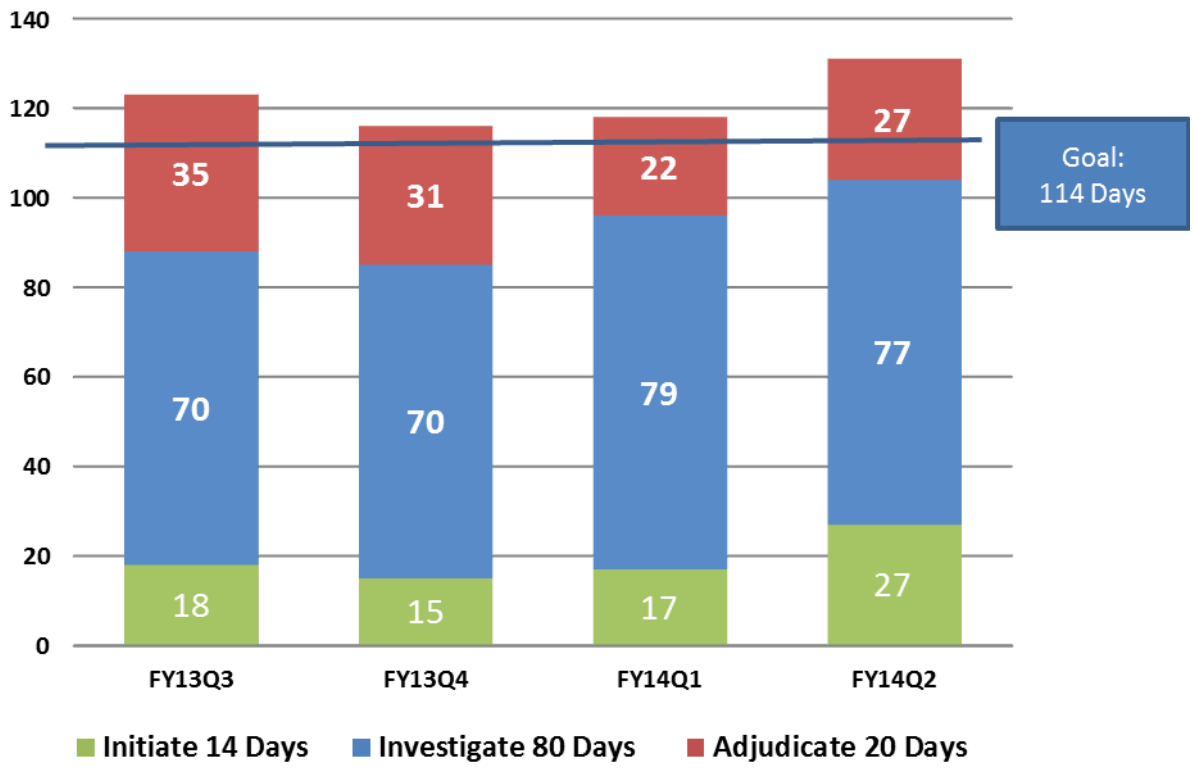
	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 3rd Q FY13	8,883	20,981	12,385
Adjudication actions taken – 4th Q FY13	9,268	20,165	18,807
Adjudication actions taken – 1st Q FY14	5,802	13,858	12,918
Adjudication actions taken – 2nd Q FY14	6,306	17,594	15,363

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

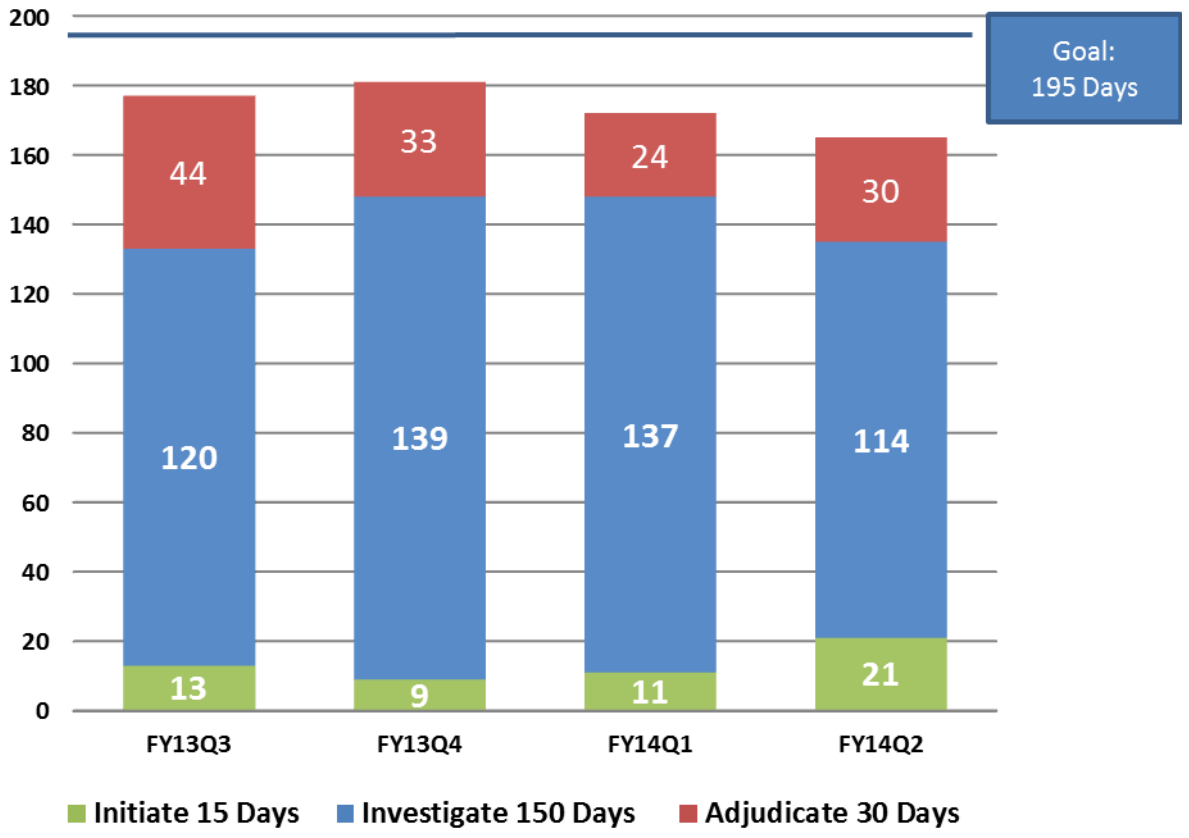
IC and DoD Industry Secret Clearances



IC and DoD Industry
Top Secret Clearances



IC and DoD Industry
Periodic Reinvestigations



2012 Intelligence Authorization Act Report on Security Clearance Determinations

Format used in 2012:

Table 1C
Total: Tables 1A and 1B

Employee Type	As of 10/1/12:		As of 10/1/13:	
	Conf/Secret	Top Secret	Conf/Secret	Top Secret
Government	2,757,333	791,200	2,886,106	851,920
Contractor	582,524	483,263	558,626	497,683
Other	167,925	135,506	175,859	180,185
Sub-Total:	3,507,782	1,409,969	3,620,591	1,529,788
Total:	4,917,751		5,150,379	

Further detail in 2013:

Table 1A
Eligibility (In access)

Employee Type	As of 10/1/12:		As of 10/1/13:	
	Conf/Secret	Top Secret	Conf/Secret	Top Secret
Government	1,283,287	625,727	1,204,416	646,527
Contractor	497,634	444,928	467,909	452,102
Other	136,163	131,302	144,512	176,511
Sub-Total:	1,917,084	1,201,957	1,816,837	1,275,140
Total:	3,119,041		3,091,977	

Table 1B
Eligibility (Not in access)

Employee Type	As of 10/1/12:		As of 10/1/13:	
	Conf/Secret	Top Secret	Conf/Secret	Top Secret
Government	1,474,046	165,473	1,681,690	205,393
Contractor	84,890	38,335	90,717	45,581
Other	31,762	4,204	31,347	3,674
Sub-Total:	1,590,698	208,012	1,803,754	254,648
Total:	1,798,710		2,058,402	

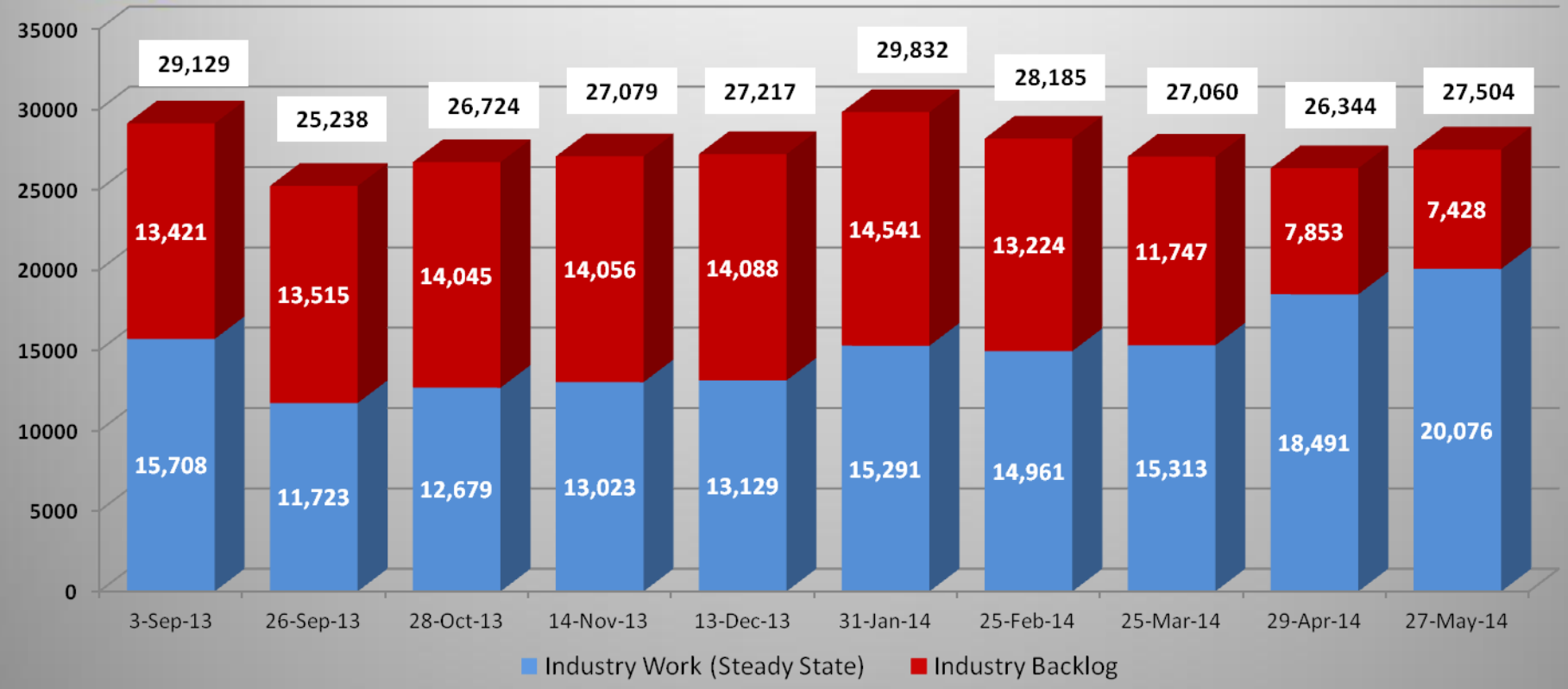
Contact information:
Christy Wilder
571-204-6502 (W)
93-58834 (S)

Attachment #6

NCMS

DoD Consolidated Adjudications Facility Update

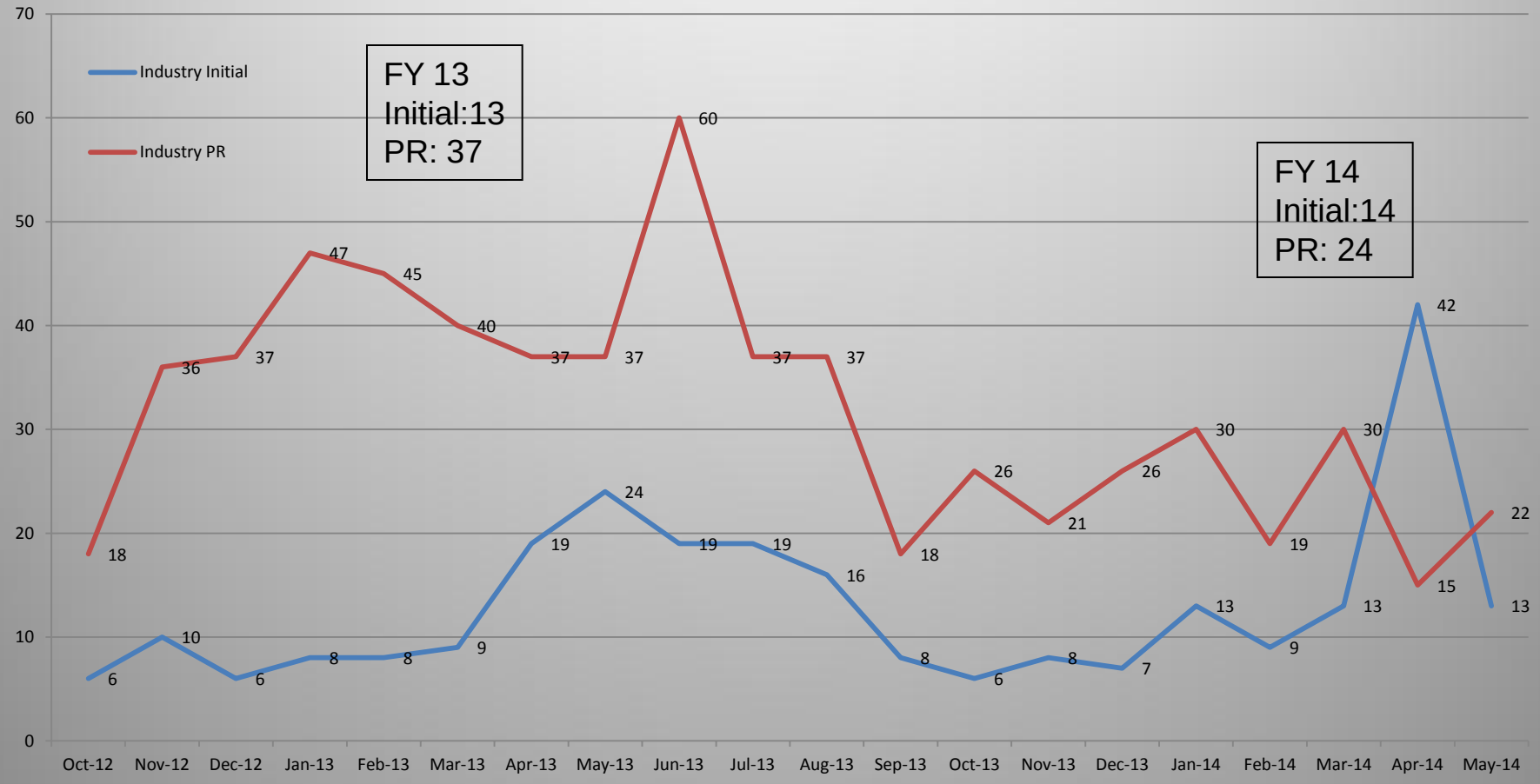
DoD Consolidated Adjudications Facility (CAF)
Pending Industry Workload



- 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
- Current path eliminates IND backlog NET 2015

Month	NISP Backlog	Annual NISP Receipt	Backlog % of Total NISP
April 13	14,702		8.1%
May 14	7,428		4.1%
	-7,274	~ 180,000	

Industry
Intelligence Reform and Terrorism Prevention Act Performance



- **Timeliness to fluctuate/increase during FY14-15**
- **Overall DoD CAF timeliness edged up in FY14 as well**
- **Focus on inherited backlog impacts timelines**

Cases Sent to DOHA FY13…To Present

- **SORs referred to DOHA for legal review:**
  - 4,423 cases were referred to DOHA for legal review
  - average number of days case remained at DOHA for legal review was 37 days
  - average time it took for the DoD CAF to issue a SOR after a case was returned from legal review was 13 days
  - average time it took to receive a response to an SOR from the applicant was 45 days

DoD Consolidated Adjudications Facility (CAF) Summary and Takeaways:

- **IRTPA**
  - > 96% of Industry cases are adjudicated in < 30 days
- **DoD CAF Caseload Inventory**
  - DoD CAF to improve timeliness and eliminate backlog via:
    - Improved Processes
    - Standardized Productivity
    - New Efficiencies--e.g., flexibility vice specialization of adjudicators
    - Collaborative behavior at levels
- **DoD CAF Director Assessment:**
  - Projection to fully eliminate industrial case backlog is NET late FY15
  - We should maintain full IRTPA compliance, but overall timeliness for “Initials” may fluctuate as we adjudicate more & older backlog cases
  - Given fiscal challenges, CAF Adjudicators are succeeding better than expected

Attachment #7

DEFENSE OFFICE OF HEARINGS & APPEALS

Changes to the Industrial Security Clearance Process

NISPPAC at NCMS
19 June 2014

What's New:

DOHA's adjudicators moved to ODA&M in 2012, along with DISCO's adjudicators, to become part of the DoD Consolidated Adjudications Facility. Despite what may be listed for many cases in JPAS, all industrial security clearance adjudications are now with the DoD CAF.

Now only due process cases are with DOHA. As of June 6, DOHA has on hand 520 for SOR review, 239 for hearing, 113 for a decision on a written record and 40 AJ decisions on appeal with the Appeal Board. DOHA has less than a thousand industrial cases on hand in total and no backlog.

Issues not resolved in the investigation, such as financial issues, can usually be resolved with more information developed from the subject. So a best practice for the time when the employee submits the SF 86 or eQIP with issues identified is to be sure to provide as much mitigating information about those issues as possible at the earliest possible stage in the process.

CAF Consolidation:

DOHA's adjudicators moved under ODA&M on October 21, 2012, along with DISCO's adjudicators, to become part of the DoD CAF.

On May 3, 2012, the Deputy Secretary of Defense directed a central DoD Consolidated Adjudications Facility (CAF) be established under the authority, direction, and control of the Director, Administration and Management (DA&M). On that date, the Deputy Secretary of Defense directed the complete consolidation of the functions, resources and assets of the Army Central Clearance Facility, Department of the Navy CAF, Air Force CAF, Joint Staff CAF, Washington Headquarters (WHS) CAF, Defense Industrial Security Clearance Office (DISCO), and the personnel security adjudication function of the Defense Office of Hearings and Appeals (DOHA) at Fort Meade, Maryland, into this new DoD CAF organization.

All industrial adjudicative-level actions will appear as DoD CAF. DOHA actions are now only in due process cases.

Adjudication & Due Process:

- Preliminary Adjudicative Process
  - –Largest portion of cases never go to due process, as adjudicators can make decision to grant clearance at earliest possible time.
  - –The adjudicators apply Federal Adjudicative Guidelines and may grant the clearance or either issue interrogatories (written questions) to the individual or request a further investigation, if potentially disqualifying issues are not resolved by the investigation. The adjudicator does not deny or revoke the clearance, but issues a Statement of Reasons (SOR) if unable to grant the clearance. The SOR is the start of due process.

- Due Process Hearings & Decisions on the Written Record

  Required before denial or revocation, but SOR can be withdrawn and a favorable decision made after review of the Answer.

Basis of Personnel Security Clearance Due Process:

Greene v. McElroy 360 U.S. 474 (1959), E.O. 10865 (1960), *Navy v. Egan* 484 U.S. 518 (1988), E.O. 12968 (1995), and E.O. 13467(2008).

Executive Order 10865 specifically provides the procedural protections for individuals that the Supreme Court had found lacking in “a hearing which failed to comport with our traditional ideas of fair procedure.”

So now industrial contractors get detailed notice of the Government’s concerns, the opportunity to respond to that notice, the opportunity to appear personally and to present relevant documents and to present and cross-examine witnesses. Executive Orders 12968 and 13467 do not diminish or otherwise affect the denial and revocation procedures provided to individuals covered by Executive Order 10865.

Executive Order 10865:

With certain very narrow exceptions, each individual must receive:

•(1) A written statement of reasons (SOR) which shall be as comprehensive and detailed as the national security permits.

•(2) A reasonable opportunity to reply in writing to the SOR.

•(3) An opportunity to appear personally … for the purpose of supporting eligibility … and to present evidence.

•(4) A reasonable time to prepare for that appearance.

•(5) An opportunity to be represented by counsel.

•(6) An opportunity to cross-examine persons who have made oral or written statements adverse to the individual on a controverted issue.

•(7) A written notice of the final decision in his case which, if adverse, shall specify whether [the decisionmaker] found for or against [the individual] with respect to each allegation in the statement of reasons.

DoD Directive 5220.6:

Executive Order 10865 is implemented by DoD Directive 5220.6.

With few exceptions, most industry due process cases come to DOHA.

When the industry employee receives a written statement of reasons (SOR) they are also sent a copy of the Adjudicative Guidelines and a copy of DoD Directive 5220.6, so the individual knows the standards.

Once they have answered the SOR, they will also get copies of any and all documents that the Government is relying on as a basis for the proposed denial or revocation of their security clearance.

It is never too early to start providing potentially mitigating information.

Visit the DOHA Web Site:

- Feel free to direct an individual with questions to the Defense Office of Hearings and Appeals web site address:

- *http://www.dod.mil.dodgc.doha*

- This site provides information about DOHA programs and can answer many questions. All Administrative Judge and Appeal Board Decisions since 1 November 1996 are published on the DOHA website in a redacted format.

- ***If*** DOHA has their case, any individual can call DOHA at 1-866-231-3153 or e-mail us to ask about a case at DOHA: dohastatus@osdgc.osd.mil

Attachment #8

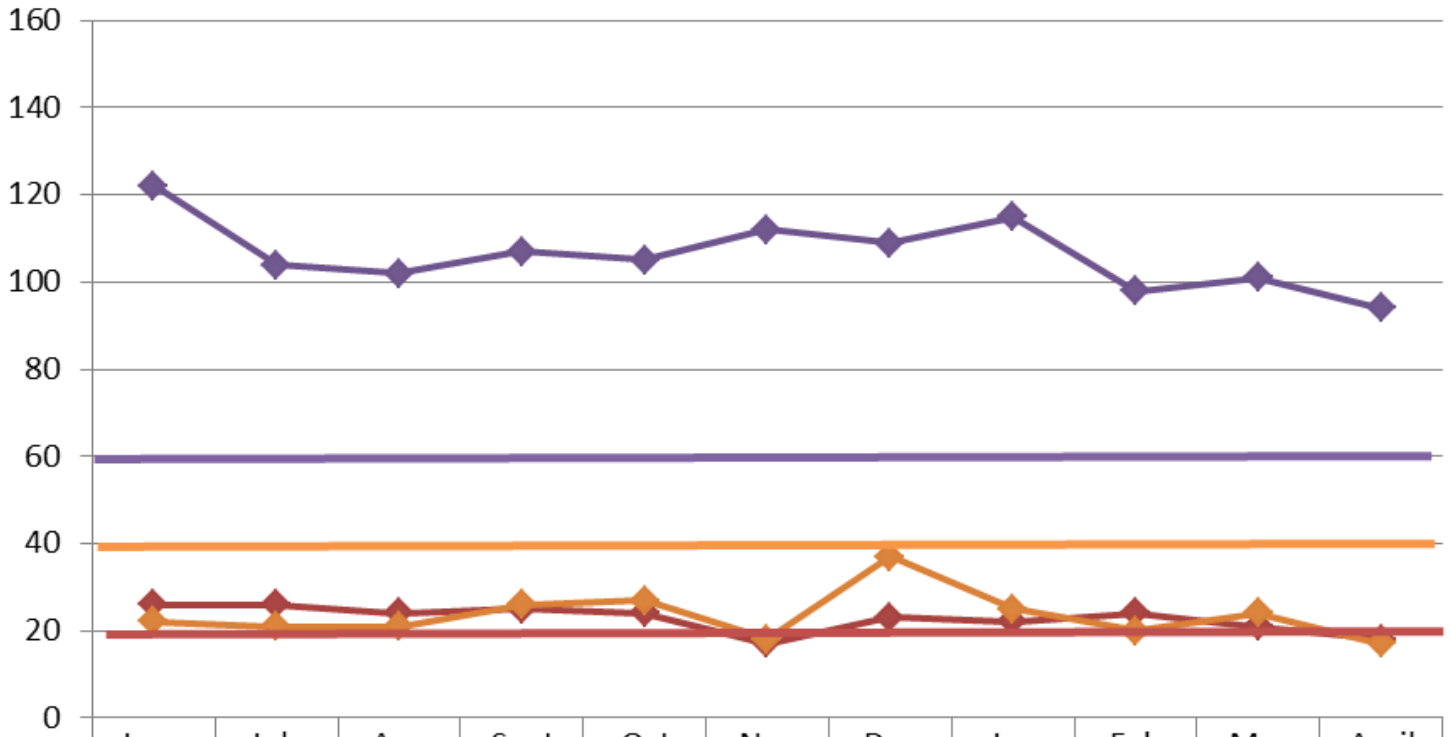
NISPPAC C&A Working Group Update for the Committee

May 2014

Working Group Initiatives

- ISFO Process Manual
  - Effective May 2014
  - Configuration Management Procedure under Development
- New System Security Plan template
  - Released in May 2014
- Baseline Technical Security Configuration of Microsoft Windows 7 and Microsoft Server 2008 R2
  - Released July 2013
- In process of identifying compliance tools for future consideration & evaluation

DSS ODAA Approval Timeliness



	June	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	April
IATO Timeliness	26	26	24	25	24	17	23	22	24	21	18
IATO Amount	155	223	145	170	219	200	213	156	179	213	204
ATO Timeliness	122	104	102	107	105	112	109	115	98	101	94
Reg ATO Amount	107	139	183	127	111	139	168	190	171	212	191
SATO Timeliness	22	21	21	26	27	18	37	25	20	24	17
SATO Amount	109	94	132	114	107	146	104	104	151	148	128

Takeaways:

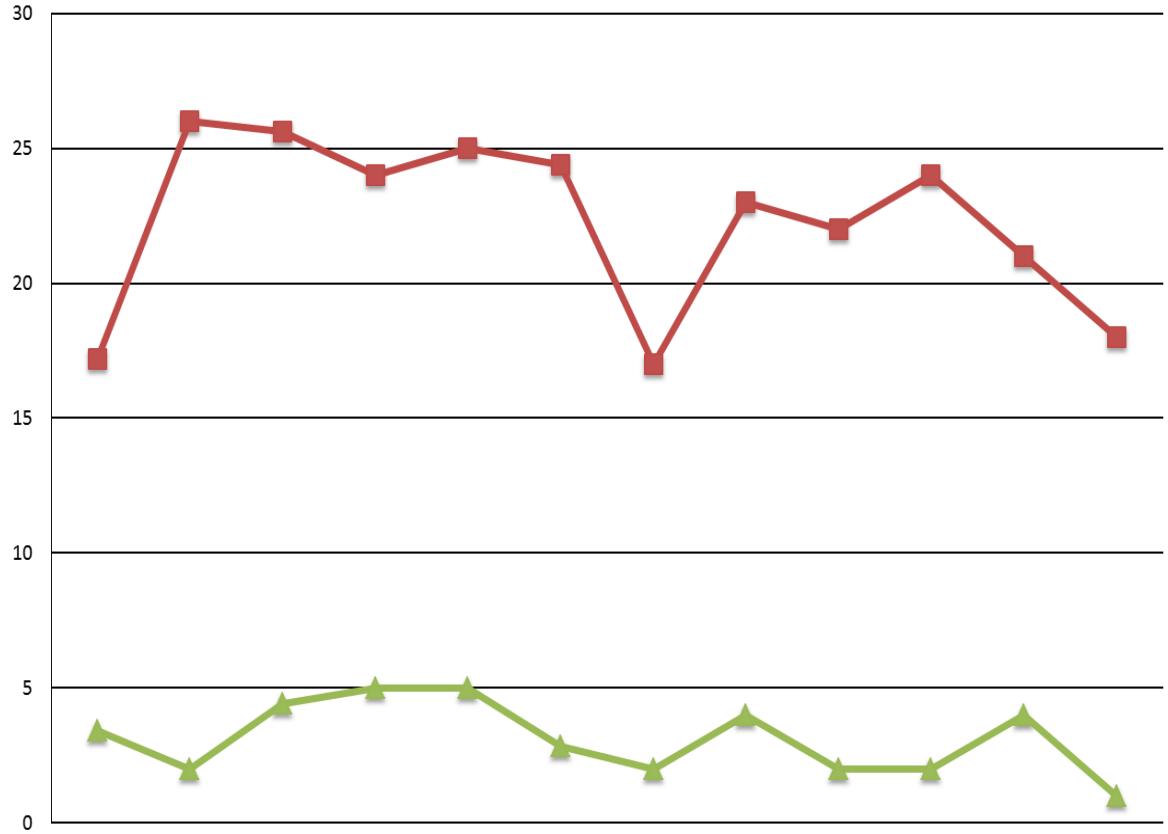
- Security Plans are Being Processed and Reviewed in a Timely Manner
  - Most Common Deficiencies in SSPs Include Missing Attachments and Documentation not being tailored to the System

- Onsite Validations are Being Completed in a Timely Manner
  - Most Common Vulnerabilities Identified During System Validation Includes Auditing Controls and Not Protecting Security Relevant Objects

- Focus to Process Straight to ATO (Where Practical) to Reduce Risk and Increase Efficiency

Back-Up Slides

Security Plan Review Results from May 2013- April 2014



	May-13	Jun-13	Jul-13	Aug-13	Sep-13	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14
Total IATOs	189	155	223	145	170	219	200	213	156	179	213	204
Industry Response Time to DSS Questions, Comments	3	2	4	5	5	3	2	4	2	2	4	1
# Second IATOs	12	12	28	13	14	21	14	19	13	5	9	5
Time from DSS Receipt of plans to Granting of IATOs	17	26	26	24	25	24	17	23	22	24	21	18

4112 SSPs were reviewed

2266 IATOs were issued

Avg. 22 days to issue an IATO

1462 SATO were processed

23 days to issue a SATO.

1015 of the SSPs (25%) required some level of correction

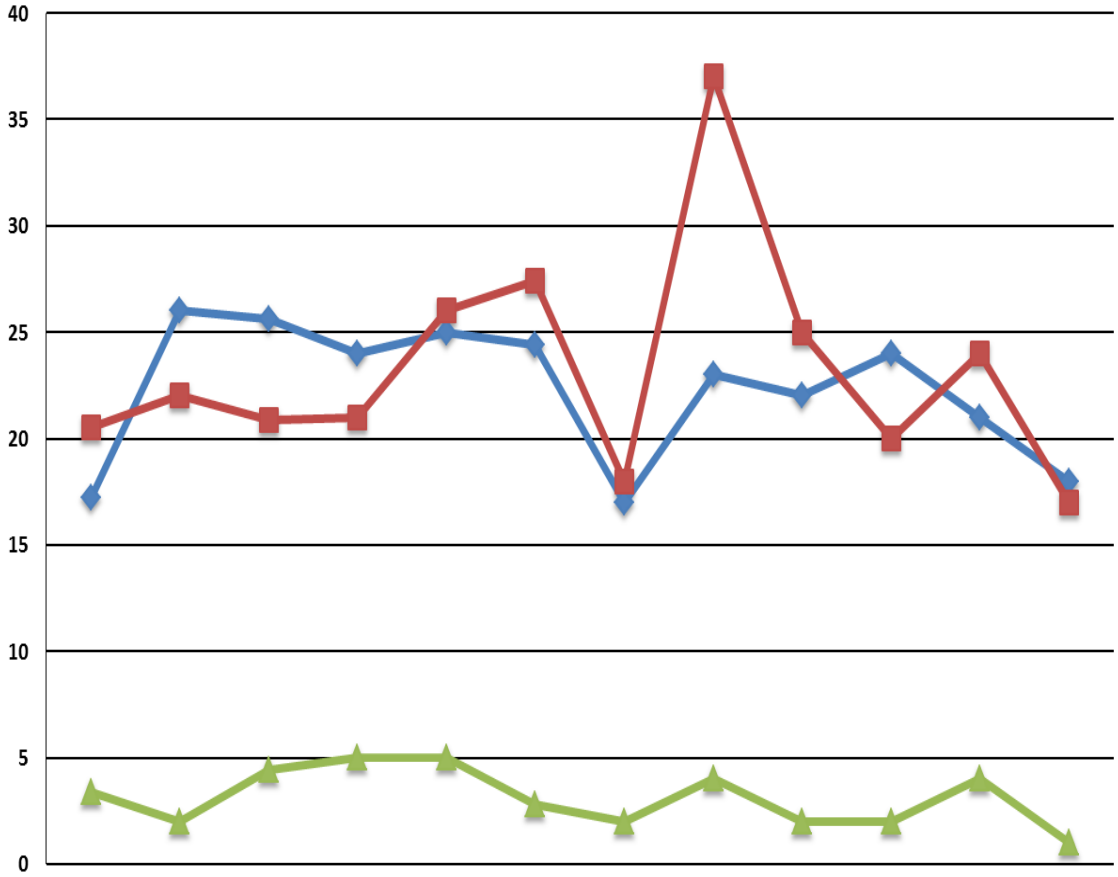
- 618 of the SSPs (15%) were granted IATO with corrections required.

- 100 of the SSPs (2%) that went SATO required some level of correction.

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

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

Security Plan Review Results from May 2013- April 2014



	May-13	Jun-13	Jul-13	Aug-13	Sep-13	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14
Time from DSS Reciept of plans to Granting of IATOs	17	26	26	24	25	24	17	23	22	24	21	18
Time from DSS Reciept of plans to Granting of SATOs	20	22	21	21	26	27	18	37	25	20	24	17
Industry Response Time to DSS Questions, Comments	3	2	4	5	5	3	2	4	2	2	4	1
Second IATOs	12	12	28	13	14	21	14	19	13	5	9	5

4112 System security plans (SSPs) were accepted and reviewed during the preceding 12 months.

2266 Interim approvals to operate (IATOs) were issued during the preceding 12 month period, it took an average of 22 days to issue an IATO after a plan was submitted.

1462 “Straight to ATO (SATO)” were processed during the preceding 12 months, it took an average of 23 days to issue the ATO.

1015 of the SSPs (25%) required some level of correction prior to conducting the onsite validation.

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

100 of the SSPs (2%) that went SATO required some level of correction.

Denials: 297 of the SSPs (7%) were received and reviewed, but denied IATO until corrections were made to the plan.

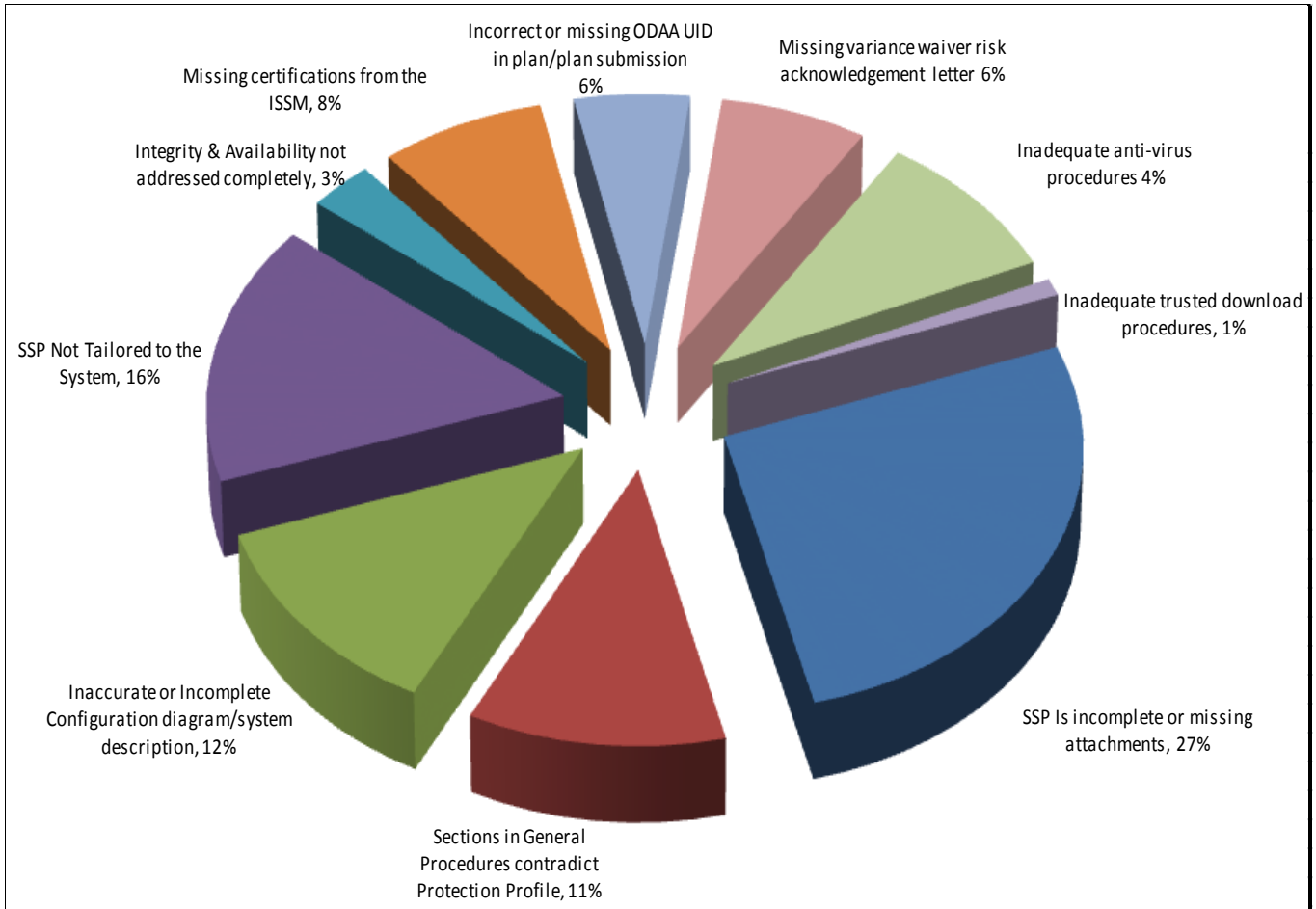
Rejections: 87 of the SSPs (2%) were not submitted in accordance with requirements and were not entered into the ODAA process. These SSPs were returned to the ISSM with guidance for submitting properly and processed upon resubmission.

Last Months Snapshot: April 2014

204 IATOs were granted with an average turnaround time of 18 days

128 SATOs were granted with an average turnaround time of 17 days

Common Deficiencies in Security Plans from May 2013- April 2014

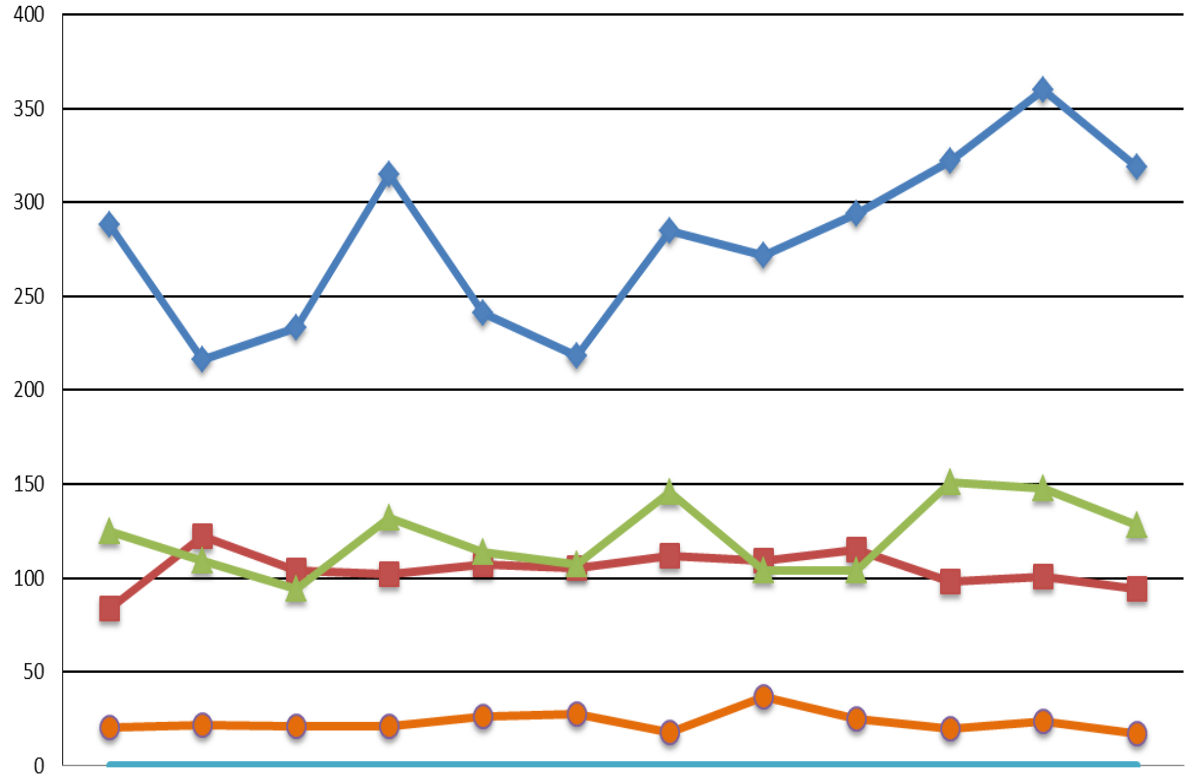


	May-13	Jun-13	Jul-13	Aug-13	Sep-13	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14
# Deficiencies	124	180	217	168	239	178	148	137	197	146	178	179
# Plans w/ Deficiencies	81	81	115	92	112	101	83	90	76	89	92	90
# Plans Reviewed	343	302	354	309	328	364	376	338	282	357	396	363
Avg Deficiency per Plan	0.36	0.60	0.61	0.54	0.73	0.49	0.39	0.41	0.70	0.41	0.45	0.49
Denials	16	30	29	29	31	29	19	16	17	22	31	28
Rejections	13	8	8	3	13	9	11	5	5	5	4	3

Top 10 Deficiencies

1. SSP Is incomplete or missing attachments
2. SSP Not Tailored to the System
3. Inaccurate or Incomplete Configuration diagram or system description
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. Inadequate anti-virus procedures
9. Integrity & Availability not addressed completely
10. Inadequate trusted download procedures

On Site Review Results from May 2013- April 2014



	May-13	Jun-13	Jul-13	Aug-13	Sep-13	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14
Total ATOs	288	216	233	315	241	218	285	272	294	322	360	319
Avg Days to Reg ATO	84	122	104	102	107	105	112	109	115	98	101	94
Total SATOs	125	109	94	132	114	107	146	104	104	151	148	128
Avg Days to SATO	20	22	21	21	26	27	18	37	25	20	24	17
% SATO's	43%	50%	40%	42%	47%	49%	51%	38%	35%	47%	41%	40%

During the Past 12 Months:

3363 ATOs

Avg 104 Days from IATO to ATO

1462 SATOs

Avg 23 days for SATOs

43% of all ATOs were SATO

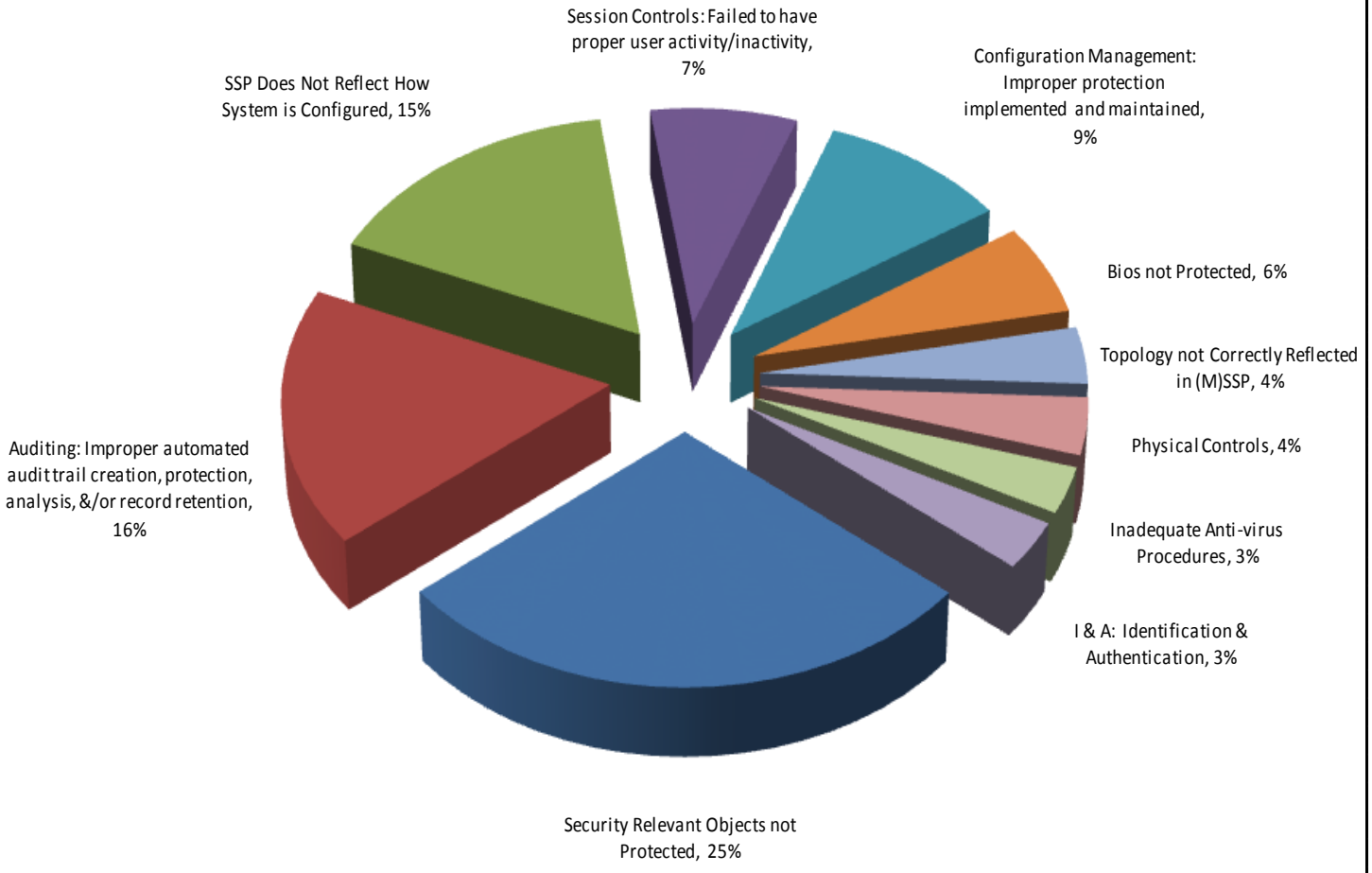
3224 System Validations

- 2398 systems (74%) had no vulnerabilities identified.

- 762 systems (24%) had minor vulnerabilities identified that were corrected while onsite.

- 64 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 2013- April 2014



	May-13	Jun-13	Jul-13	Aug-13	Sep-13	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14
# Vulnerabilities	108	70	95	77	105	133	66	86	102	114	133	96
# Onsites w/ vulnerabilities	54	54	67	69	74	74	45	70	70	78	90	81
# Onsites	280	203	234	309	235	204	267	263	283	309	342	295
Avg Vulnerability per Onsite	0.39	0.34	0.41	0.25	0.45	0.65	0.25	0.33	0.36	0.37	0.39	0.33

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

Attachment #9

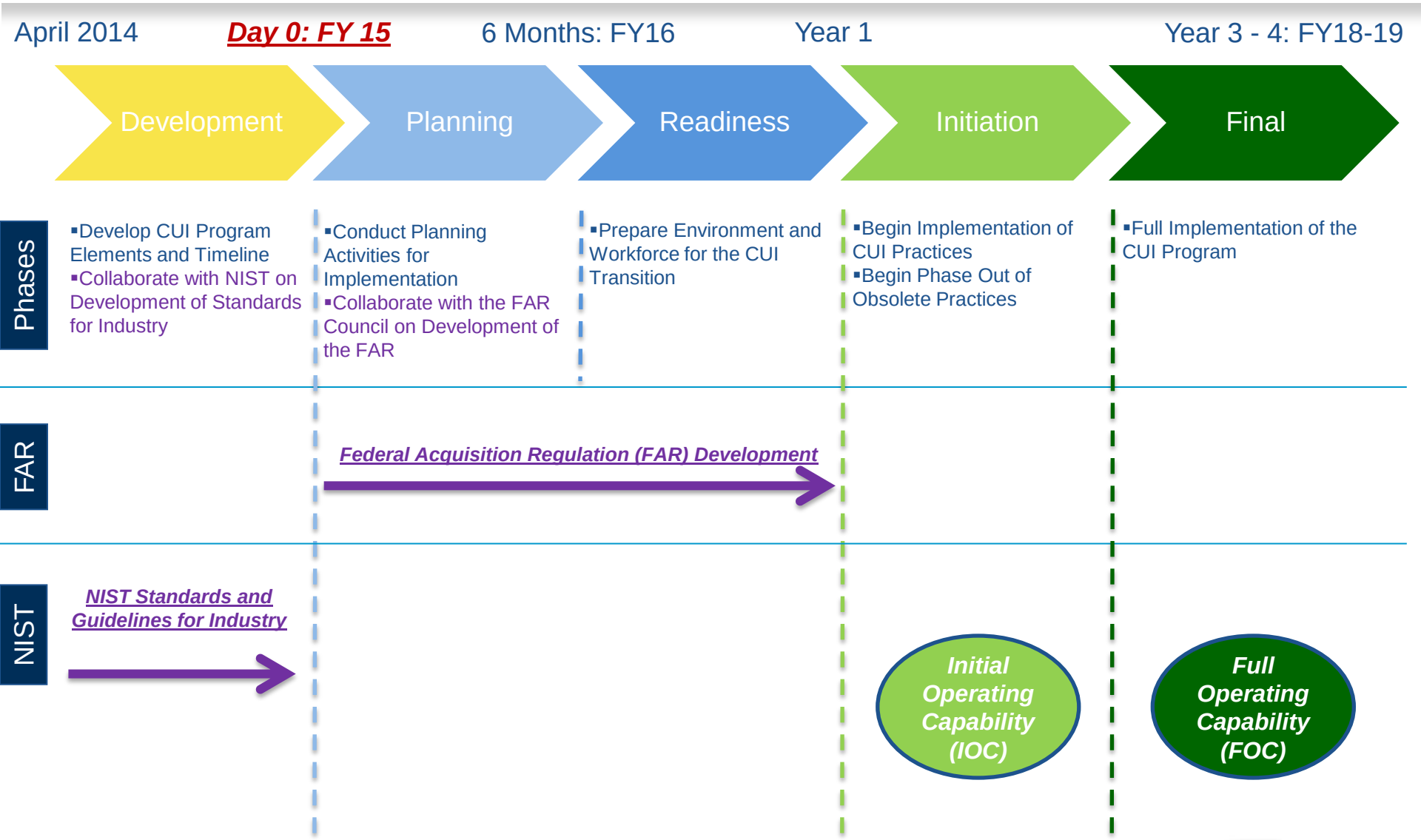
NISPPAC CUI Working Group

- Separate presentations made to CSAs and MOU NISPPAC Industry Members
- Topics covered were proposed approaches to oversight, IT requirements, and a Federal Acquisitions Regulation clause
- Series of meetings involving CSAs and Industry members will focus individually on the topic areas above with the aim of obtaining input and recommendations

NISPPAC CUI Working Group (cont'd)

- Federal Acquisition Regulation (FAR)-based solution for conveying CUI Program and Oversight Requirements.
  - Model based on self-certification and selective validation, as established by the Executive Agent (EA).
  - Validation activities are conducted by the CUI EA and the Government Contracting Agency (GCA) .
- Use of already existing central repository for capturing self-certification - System for Award Management (SAM)
  - The primary Government repository for prospective Federal awardee and Federal awardee information and the centralized Government system for certain contracting, grants, and other assistance-related processes.

CUI Phased Implementation - FAR & NIST



Attachment #10

Executive Branch Insider Threat Programs

Information Security Oversight Office

Protect • Inform • Assess

Alegra E. Woodard
Operations & Industrial Security
Information Assurance Specialist - CISSP

June 19, 2014

Executive Order 13587 Background

Unlawful disclosure of classified information by WikiLeaks in the summer of 2010

EO 13587 Oct 2011

The committee recommended government-wide actions to reduce the risk of a future breach

Senior Information Sharing and Safeguarding Steering Committee

Insider Threat Task Force

National Policy Nov 2012

Insider Threat Minimum Standards

Designate an insider threat program senior official(s);

Information integration, analysis and response;

Insider threat program personnel;

Access to information;

Monitoring user activity on networks;

Employee training and awareness.

National Security System Priorities

Removable Media – Limit the number of users with removable media permissions and strengthen accountability for their use.

Insider Threat Programs – *Integrate specialized abilities, tools, and techniques to deter, detect, disrupt the insider threat, and provide training.*

Reduced Anonymity – Strengthen verification of the identity of individuals logging on to classified systems, and enable tracking.

Access Control – Implement standardized and interoperable access control systems to enforce access privileges at the network, application, and data levels.

Enterprise Audit – Integrate specialized abilities, tools, and techniques to deter, detect, disrupt the insider threat, and provide training and assistance to agencies to help them meet national policy and minimum standards requirements in this area.

Program Establishment

Designate an insider threat program senior official(s);

Issue an insider threat policy signed by your D/A head; and

Submit to D/A leadership an insider threat program implementation plan that addresses how D/As intend to meet the requirements set forth in the minimum standards.

ISOO
Information Security Oversight Office

U.S. Department of Defense
Defense Security Service

NITTF
National Insider Threat Task Force

National Insider Threat Policy and Minimum Standards

Industry Implementation

32 CFR 2004 Revision	NISPOM DoD 5220.22-M (2006) *Conforming Change #2*

MAY 2013

ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

QUESTIONS?

Contact Information

Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, N.W., Room 502C
Washington, DC 20408-0001

(202) 357-5351 (voice)
(202) 357-5908 (fax)
alegra.woodard@nara.gov

Attachment #11

National Industrial Security Program (NISP) Contract Classification System (NCCS) Update

June 2014

DD Form 254

- **FAR: requirement to be included in every contract requiring access to classified information**
- **Developed by the Government Contracting Activity/Program**
- **Establishes the information protection requirements and scope of access by the contractor**
  - Includes information about the program and types of information to which contractor will have access
  - Used by the contractor to establish their NISP security program
  - Used by DSS to determine the scope of oversight
- **Prime contractors required to include in subcontracts requiring access to classified information**

Current State Problem to Solve…

- **No central repository in DoD or the Executive Branch**
- **Paper or PDF DD Form 254**
- **Large volume across the Executive Branch**
- **No automated distribution system**
- **No way to know that the right people have the information to do their job**
- **No easy way to analyze the information collected on the form:**
  - Security across contractors
  - Security across supply chain
  - Foreign ownership, control, or influence issues
  - Government information location in industry

Federal Enterprise Solution: NCCS

- Eliminate paper and manual process
- Provide NISP community a single web-based system to receive, change, and keep up-to-date contractor security requirements
- Define workflows and manage different user access based on roles and responsibilities
- Provide analytical capability across government programs and companies to identify specific relationships and trends
- Provide linkages to existing automated systems
- Identify prime and subcontractor relationships
- Support audit and oversight activities
- Support conducting damage assessments
- Facilitate threat information sharing with industry

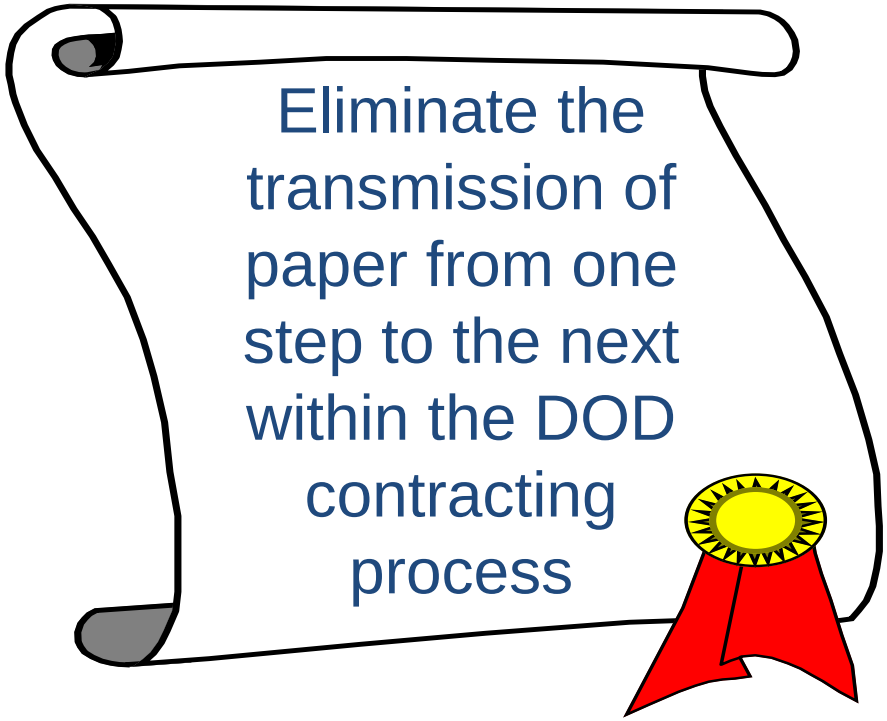
Wide Area WorkFlow (WAWF) Overview

D. Bruce Propert
Office of the Under Secretary of Defense for Acquisition, Technology and Logistics
Defense Procurement and Acquisition Policy
Program Development and Implementation

Why was WAWF developed?

- *Problem:* Paper acceptance & payment processes generated high interest penalties due to lost or misplaced receiving reports
- *Objective:* Create an electronic commerce environment using existing tools and systems
- *Schedule:* Initial Operational Capability 2002, Full Operational Capability 2003

DoD Paperless Contracting Initiative



FY13 WAWF Volume

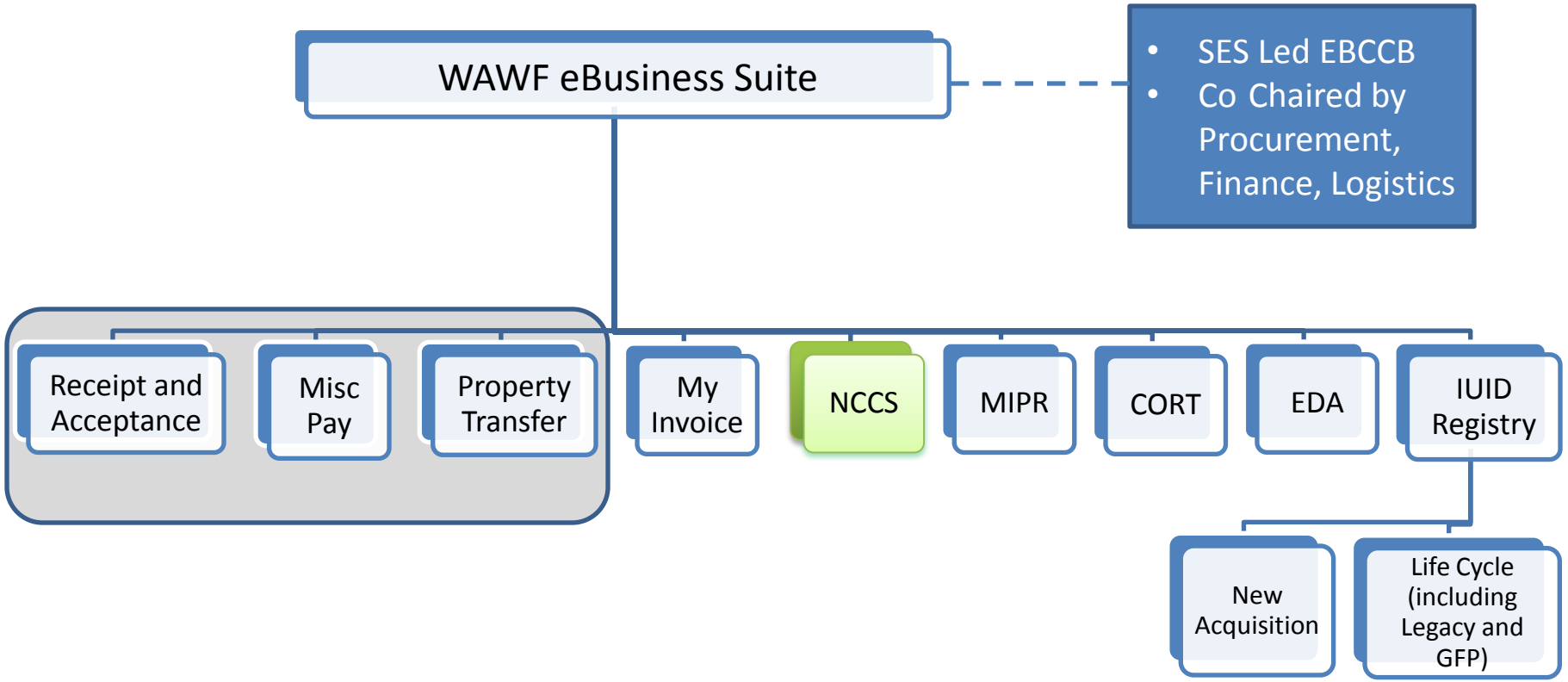
- **In FY13, the US Federal Government reported spending a total of $461B on contracts: $308B in DoD and $153B in civilian agencies.**
  - **DoD accounts for approximately 67% of total and approximately 90% of DoD is processed using WAWF.**
- **Total of 580 K WAWF Users including EDA, CORT, and WAWF**
  - **304.5 K Government users***
  - **8K Government Support Contractors**
  - **267.8K Contractor users (143 K Companies)**
- **Invoices (total FY13)**
  - **3.9 Million Transactions**
  - **$309 Billion**
- **Receiving Reports and Transfer of Property Documents**
  - **1.9 Million Transactions**
  - **$116 Billion**
- **Grants and Miscellaneous Payments**
  - **127,805 Invoices**
  - **$3.3 M**

Overall WAWF Benefits - DoD

- DFARS 252.232-7003 Electronic Submission of Payment Requests and Receiving Reports designated WAWF the sole enterprise solution
- Using WAWF has significantly improved the overall receipt, acceptance, and payment process, resulting in:
  - Cost avoidance in Prompt Payment Act (PPA) interest penalties of $90M per year;
  - Elimination of approximately 50,000 lost documents per year;
  - Approximately 50-80% reduction in invoice cycle time;
  - Elimination of the manual entry of approximately one million documents per year;
  - Approximately 70% reduction in cost for DFAS Contract Pay to process invoices
- Receipt, acceptance, and invoicing are integrated
- Acceptance can be performed at item level
- Supports property accountability

As an Enterprise DoD solution for invoicing and receipt/acceptance, WAWF is contributing to greater efficiency and user adoption.

WAWF Ecosystem



- GS 15 led Operational Requirements Committees (ORC) for each major component of WAWF
- NCCS would be independent ORC reporting to EBCCB


WAWF
Wide Area Workflow

NCCS Project Status

- USD(AT&L)/DPAP co-development with DSS to build and integrate NCCS into Wide Area WorkFlow (WAWF)
  - WAWF 5.7 release – April 2015
  - WAWF 5.8 release – approx Oct 2015

BACKUP INFORMATION

5.7.0 WAWF Release Schedule

✓ Requirements Wring Out	18 - 20 Mar 2014
✓ Software Requirements Review (SRR)	29 Apr – 1 May 2014
• Preliminary Design Review (PDR)	17 – 19 Jun 2014
• Critical Design Review (CDR)	19 – 21 Aug 2014
• Build 1 / Engineering Drop Due	25 Nov 2014
• JITC SIT/FSIT	1 - 19 Dec 2014
• SIT/FSIT Wrap Up	23 Dec 2014
• Build 2 / Engineering Drop Due	20 Jan 2015
• OAT I TRR	22 Jan 2015
• OAT I (Columbus, OH)	26 Jan – 6 Feb 2015
• OAT I Wrap Up	10 Feb 2015
• Build 3/ Engineering Drop Due	3 Mar 2015
• OAT II TRR	5 Mar 2015
• OAT II (Columbus, OH)	9 – 20 Mar 2015
• OAT II Wrap Up (Go/No-Go Decision)	24 Mar 2015
• Deployment Weekend	10 – 12 Apr 2015

PCLWG Backup Data

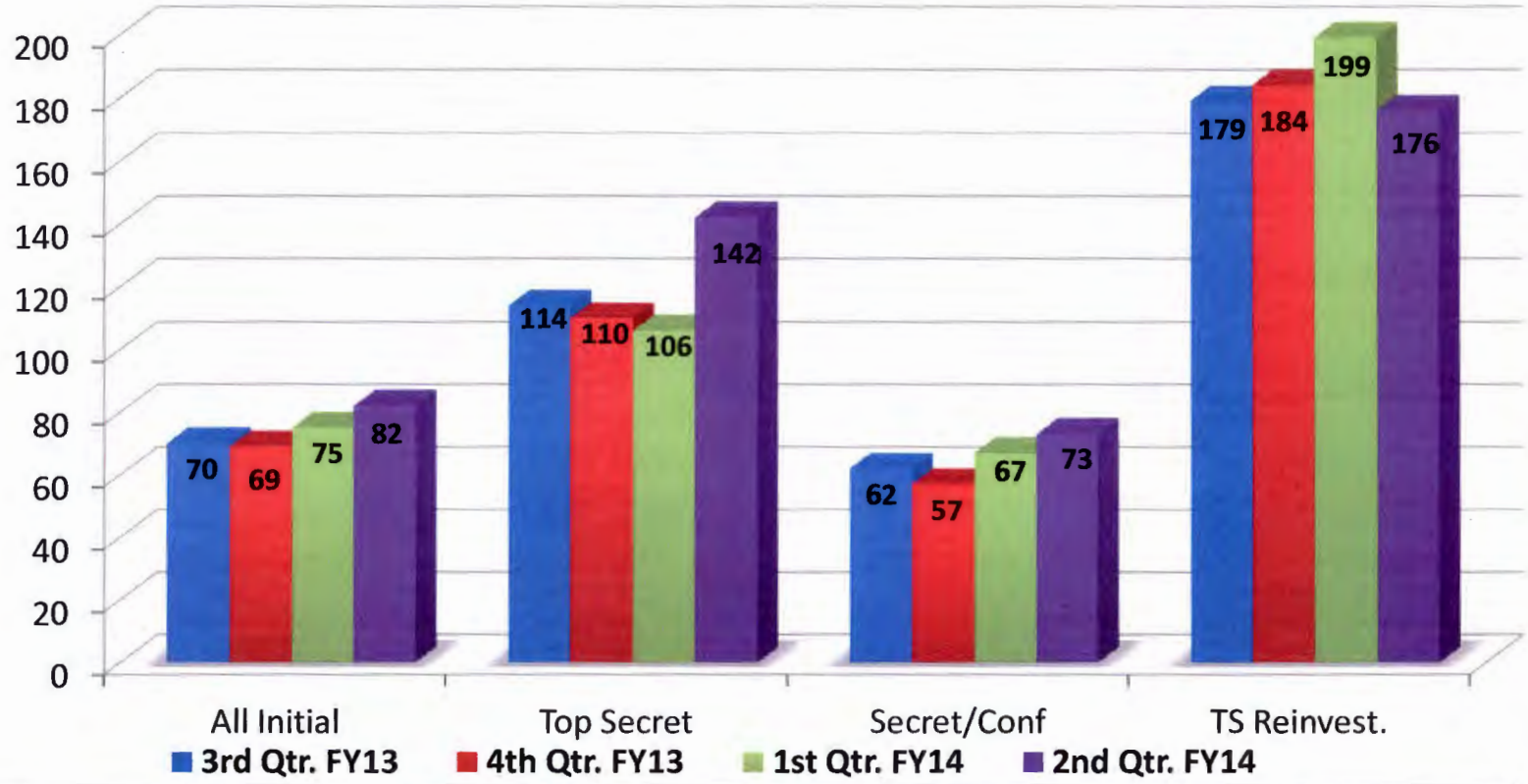
a New Day for Federal Service

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

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

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

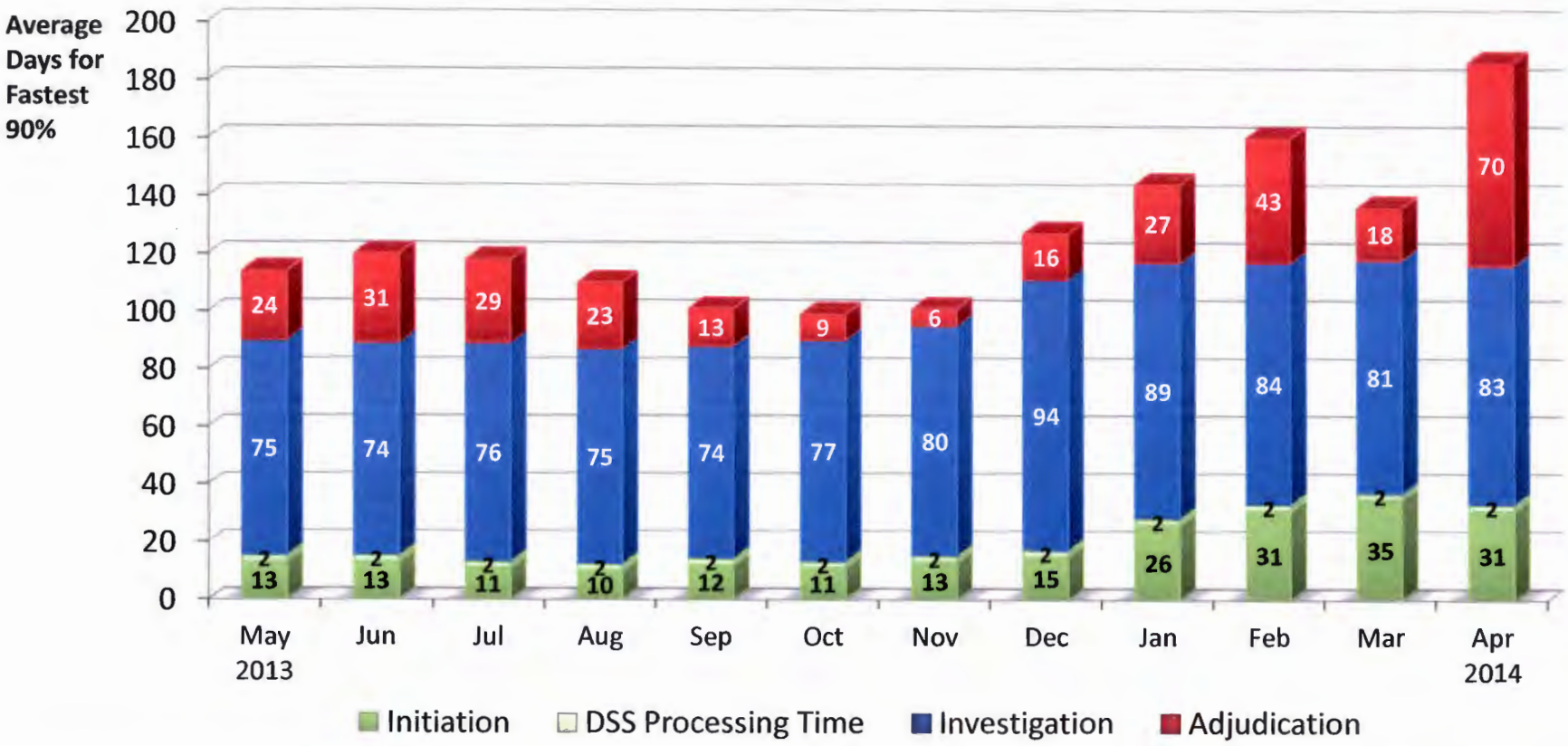
Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 3rd Q FY13	24,033	4,182	19,851	10,199
Adjudication actions taken – 4th Q FY13	25,264	5,898	19,366	16,632
Adjudication actions taken – 1st Q FY14	16,574	3,369	13,205	9,062
Adjudication actions taken – 2nd Q FY14	20,571	3,132	17,439	11,154

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

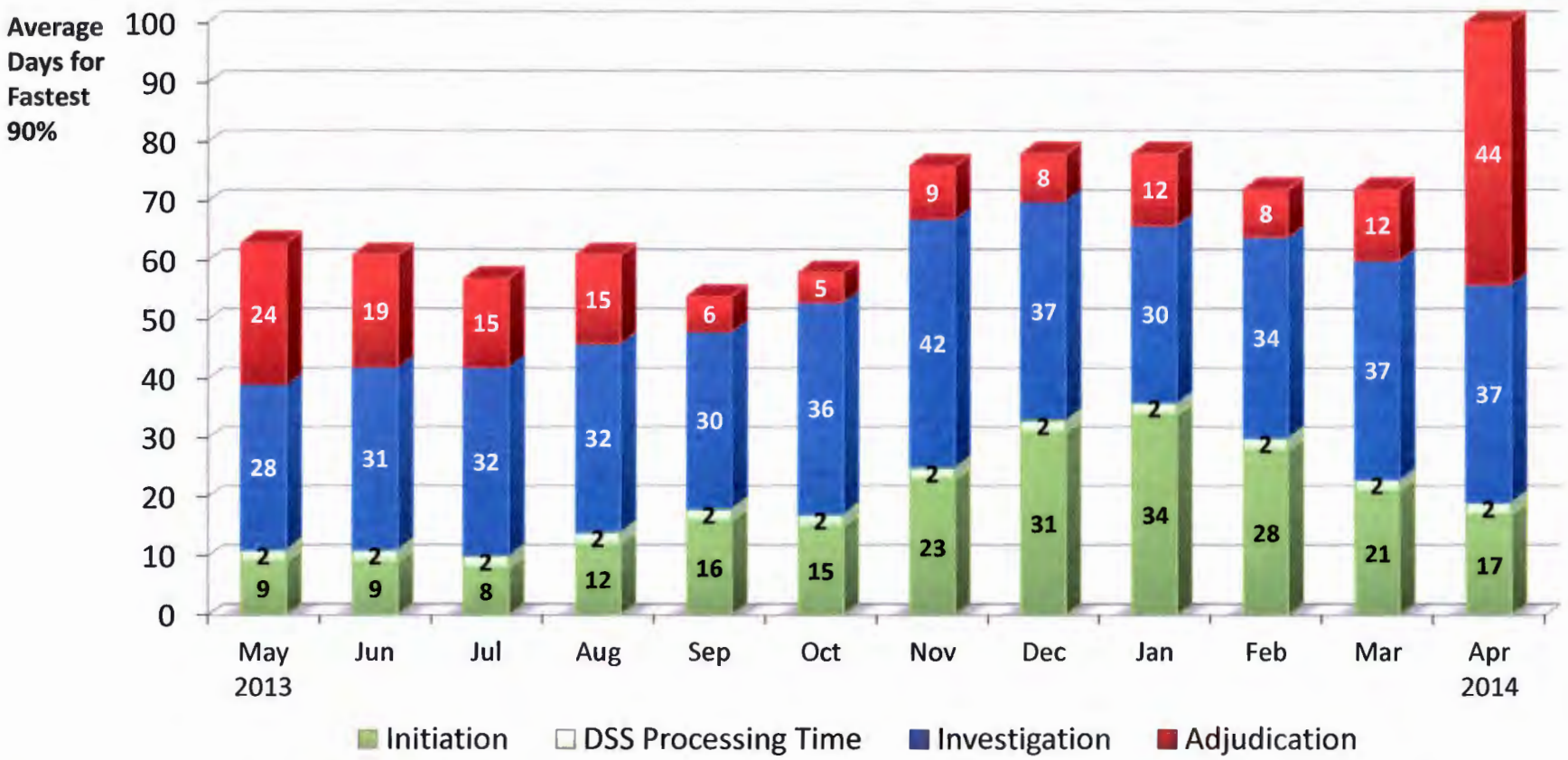
Industry's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



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

	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014	Feb 2014	Mar 2014	Apr 2014
100% of Reported Adjudications	1,182	1,368	2,283	1,407	2,219	1,360	1,080	940	759	777	1,603	961
Average Days for fastest 90%	114 days	120 days	118 days	110 days	101 days	99 days	101 days	127 days	144 days	160 days	136 days	186 days

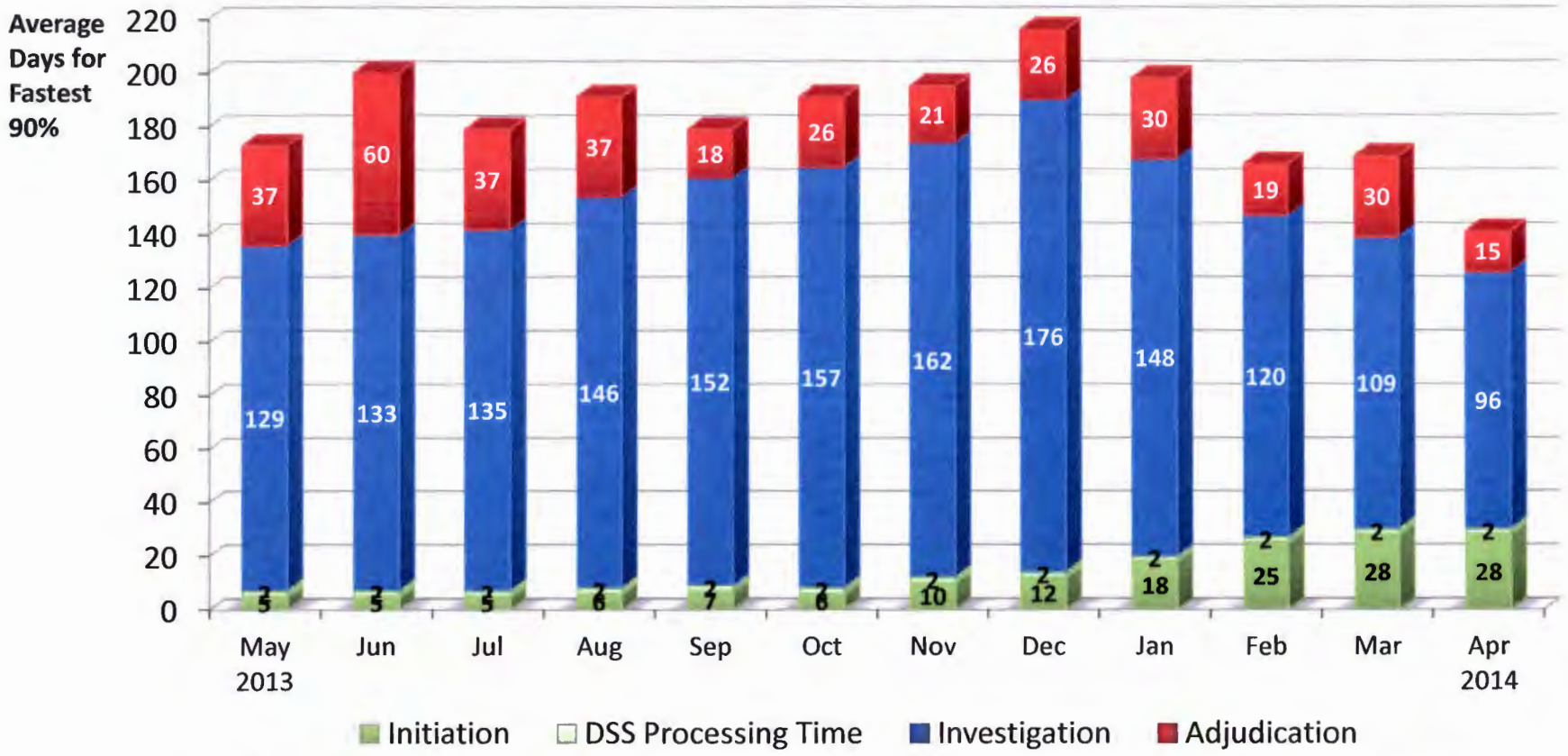
Industry's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



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

	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014	Feb 2014	Mar 2014	Apr 2014
100% of Reported Adjudications	7,515	6,015	5,836	7,404	6,144	4,640	3,080	6,440	5,319	6,644	5,485	6,996
Average Days for fastest 90%	63 days	61 days	57 days	61 days	54 days	58 days	76 days	78 days	78 days	72 days	72 days	100 days

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



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

	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014	Feb 2014	Mar 2014	Apr 2014
100% of Reported Adjudications	3,667	2,324	4,205	7,515	4,934	3,354	3,422	2,301	3,392	4,222	3,551	4,731
Average Days for fastest 90%	173 days	200 days	179 days	191 days	179 days	191 days	195 days	216 days	198 days	166 days	169 days	141 days

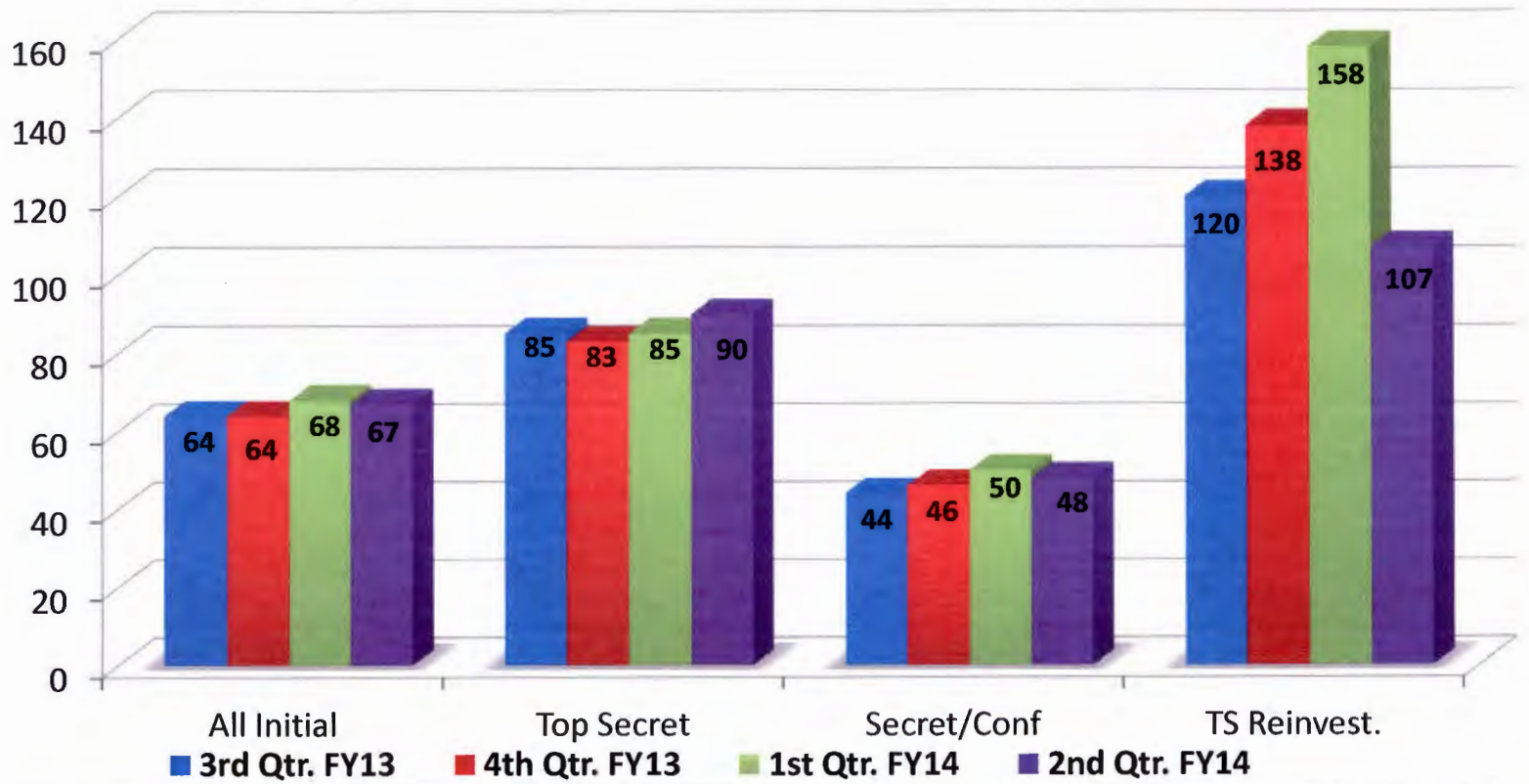
a New Day for Federal Service

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

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

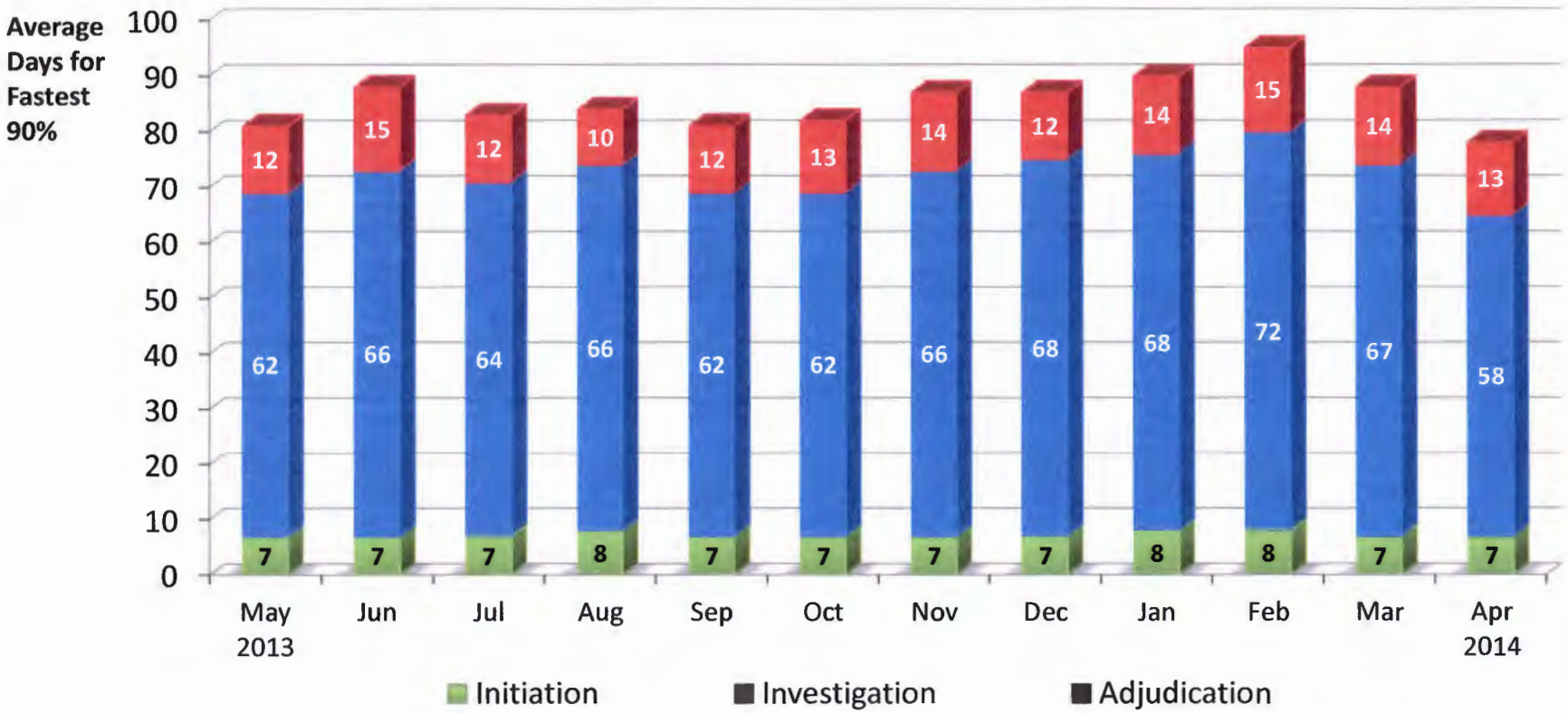
Timeliness Performance Metrics for DOE's Personnel Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 3rd Q FY13	1,896	979	917	2,961
Adjudication actions taken – 4th Q FY13	1,535	758	777	3,743
Adjudication actions taken – 1st Q FY14	1,412	773	639	2,774
Adjudication actions taken – 2nd Q FY14	1,547	724	823	2,578

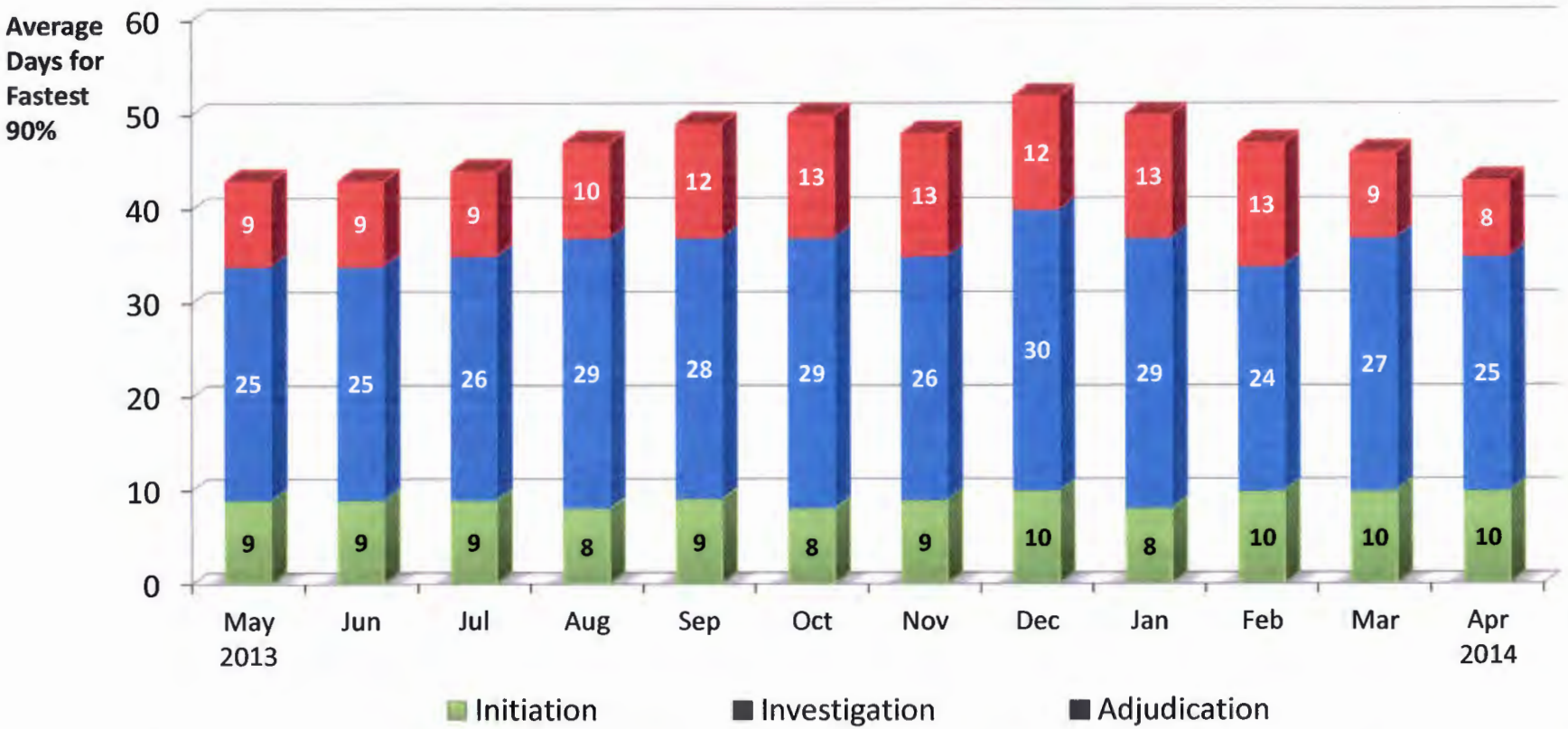
DOE's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



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

	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014	Feb 2014	Mar 2014	Apr 2014
100% of Reported Adjudications	323	274	266	249	231	315	208	234	249	221	239	219
Average Days for fastest 90%	81 days	88 days	83 days	84 days	81 days	82 days	87 days	87 days	90 days	95 days	88 days	78 days

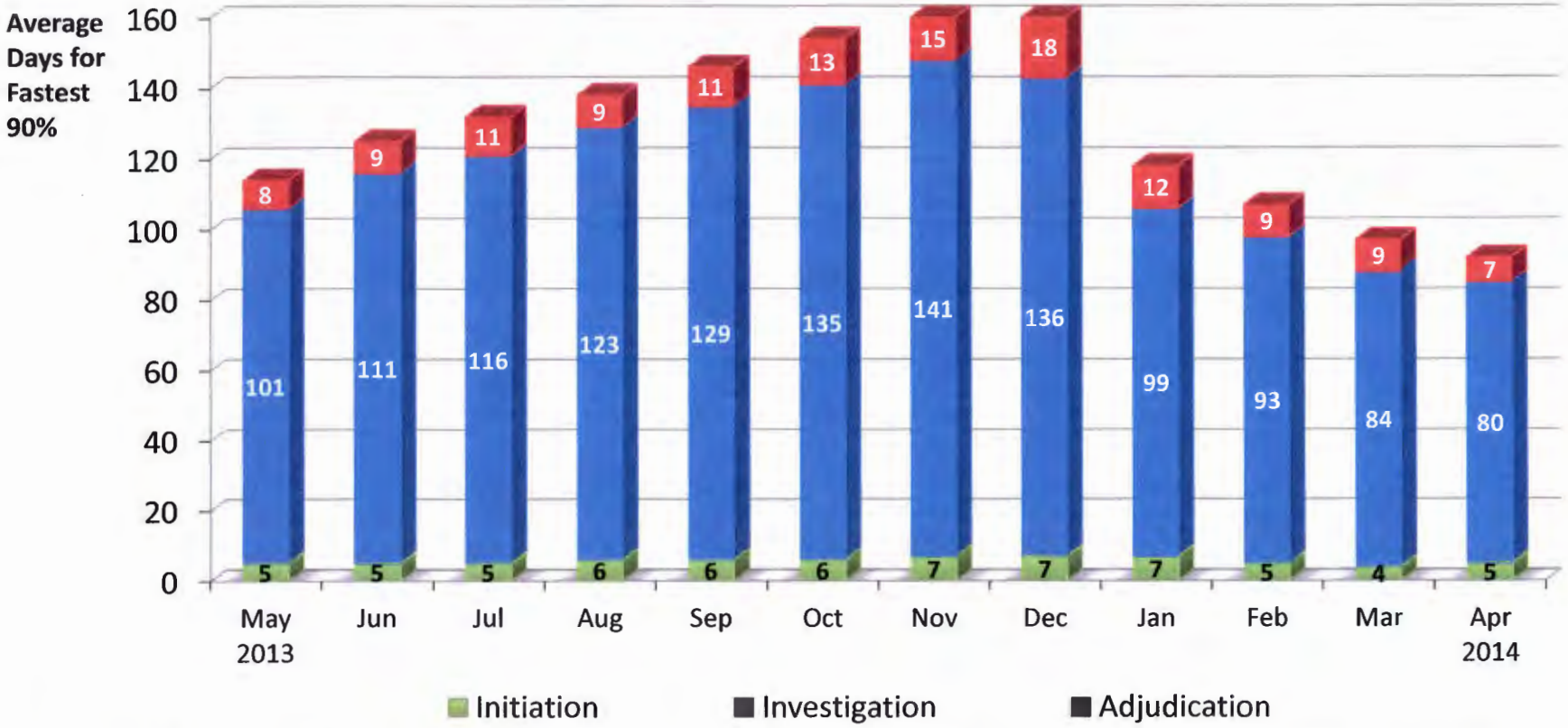
DOE's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



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

	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014	Feb 2014	Mar 2014	Apr 2014
100% of Reported Adjudications	321	233	286	278	197	222	161	201	221	280	263	289
Average Days for fastest 90%	43 days	43 days	44 days	47 days	49 days	50 days	48 days	52 days	50 days	47 days	46 days	43 days

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



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

	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014	Feb 2014	Mar 2014	Apr 2014
100% of Reported Adjudications	773	1,011	1,184	1,392	1,148	1,097	882	717	734	970	861	860
Average Days for fastest 90%	114 days	125 days	132 days	138 days	146 days	154 days	163 days	161 days	118 days	107 days	97 days	92 days

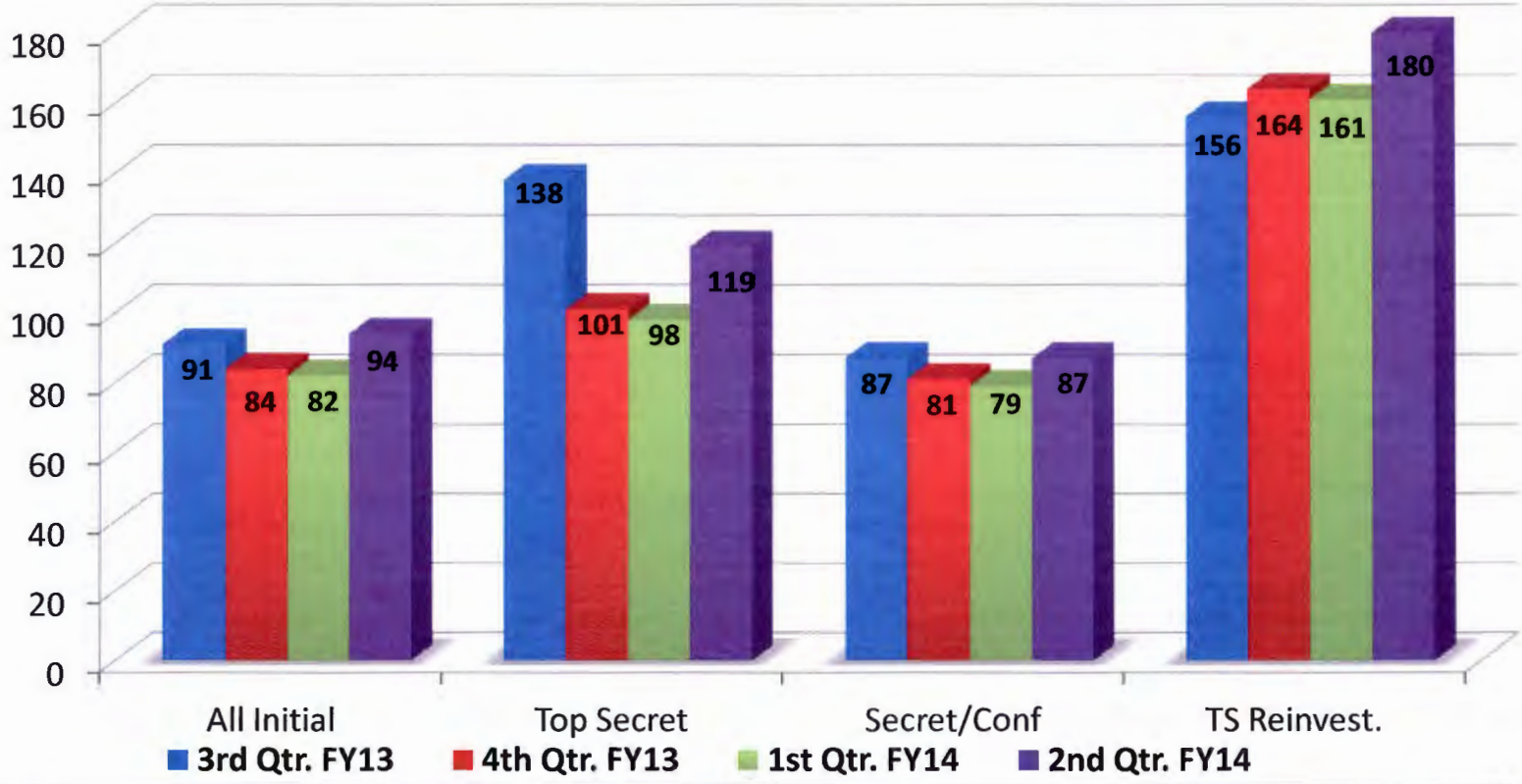
a New Day for Federal Service

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

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

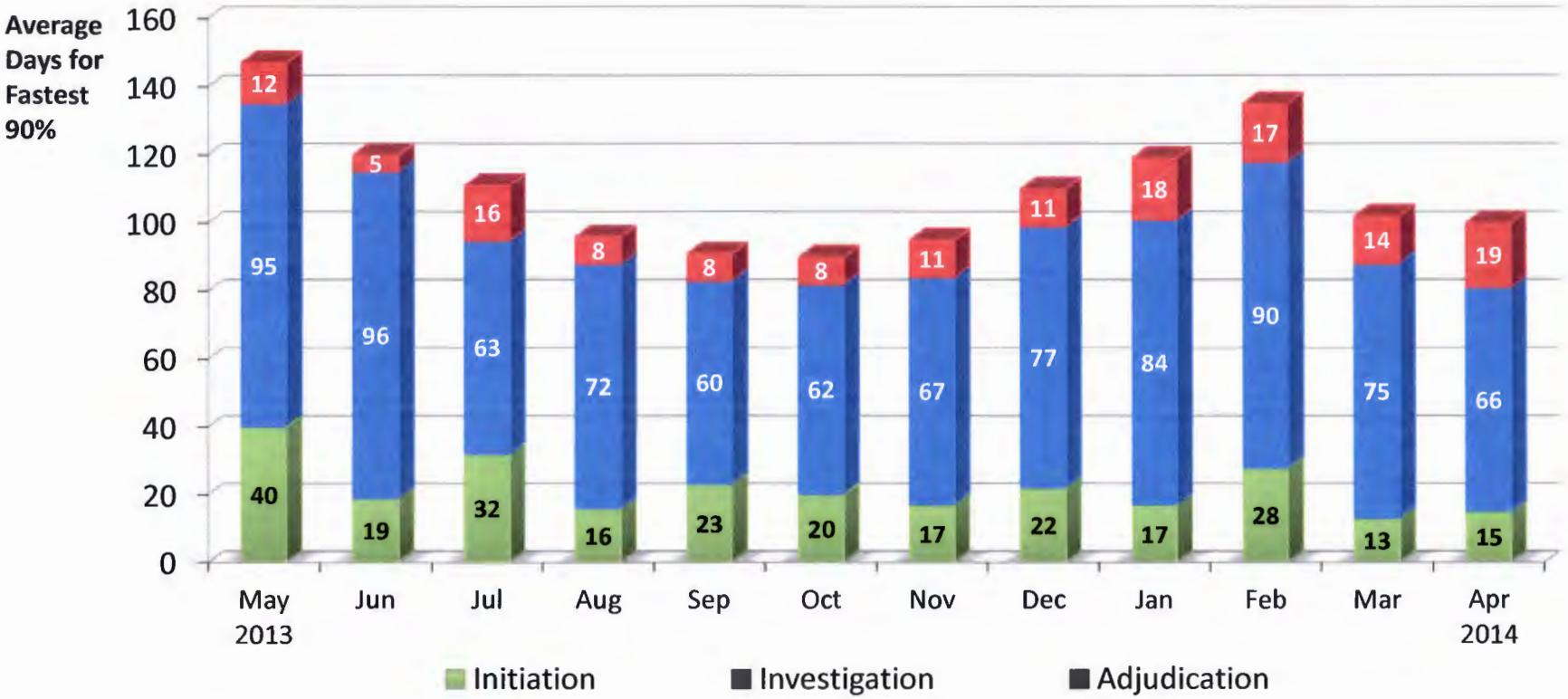
Timeliness Performance Metrics for NRC's Personnel Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 3rd Q FY13	254	22	232	22
Adjudication actions taken – 4th Q FY13	265	35	230	49
Adjudication actions taken – 1st Q FY14	169	28	141	98
Adjudication actions taken – 2nd Q FY14	208	53	155	52

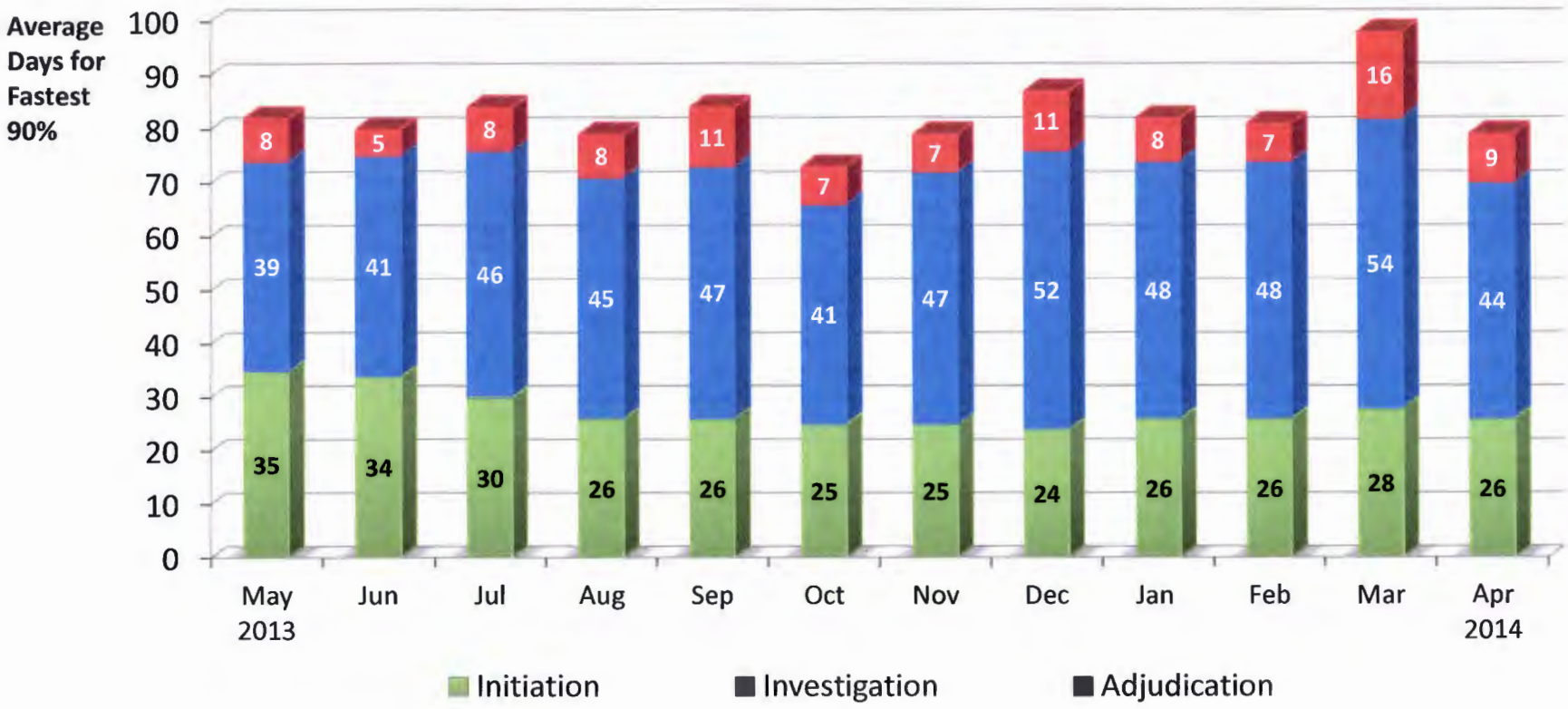
NRC's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



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

	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014	Feb 2014	Mar 2014	Apr 2014
100% of Reported Adjudications	11	4	15	10	10	7	11	10	26	11	16	16
Average Days for fastest 90%	147 days	120 days	111 days	96 days	91 days	90 days	95 days	110 days	119 days	135 days	102 days	100 days

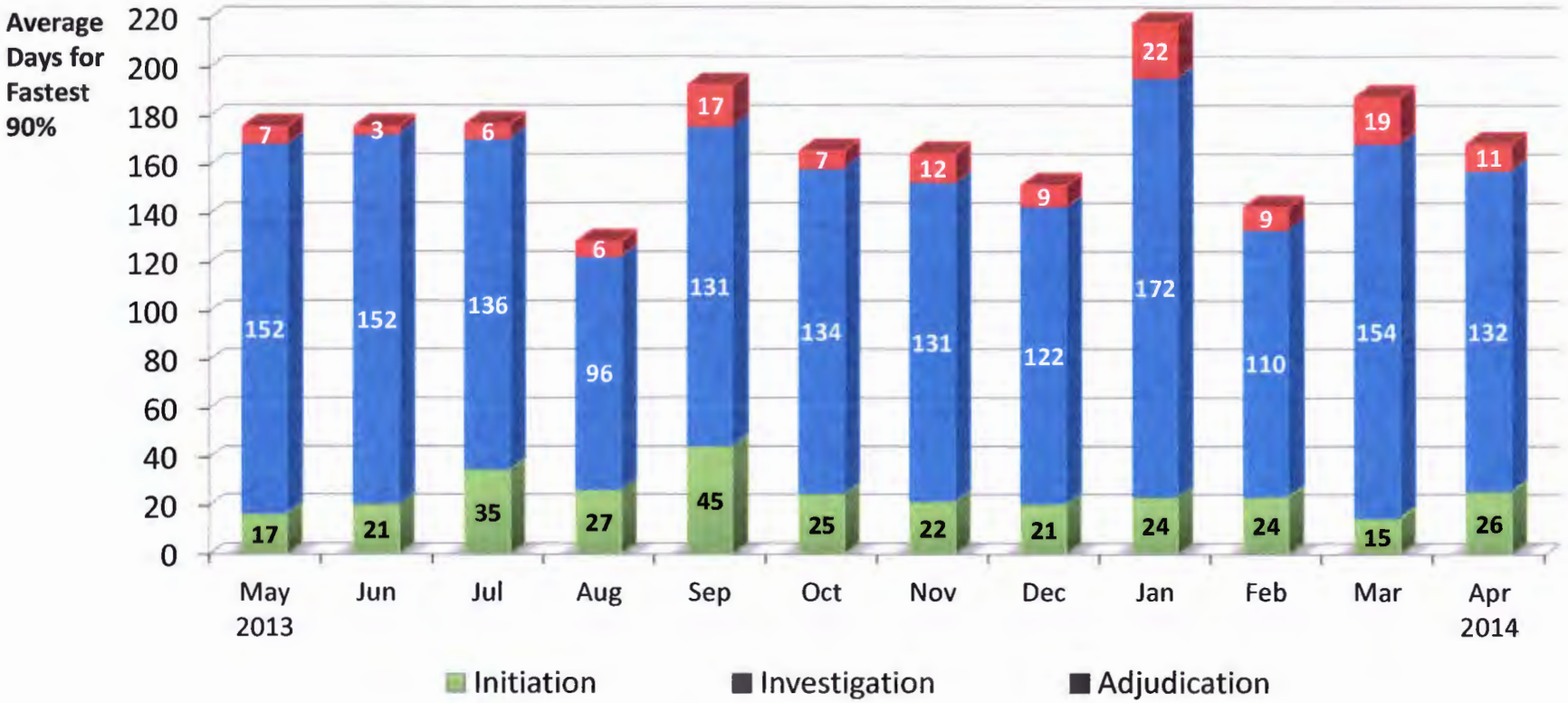
NRC's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



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

	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014	Feb 2014	Mar 2014	Apr 2014
100% of Reported Adjudications	82	87	94	79	58	59	35	47	40	55	60	52
Average Days for fastest 90%	82 days	80 days	84 days	79 days	84 days	73 days	79 days	87 days	82 days	81 days	98 days	79 days

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



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

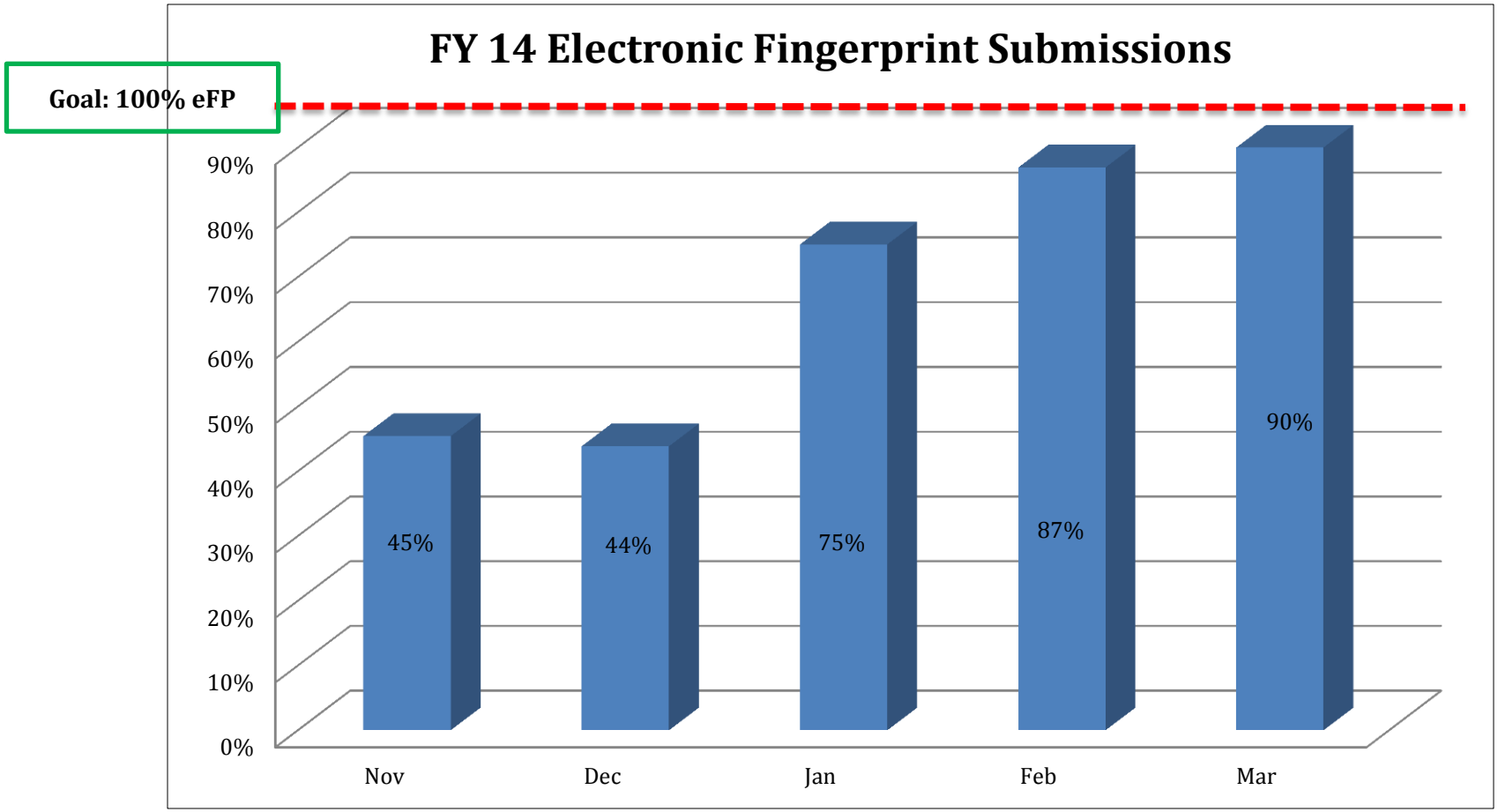
	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014	Feb 2014	Mar 2014	Apr 2014
100% of Reported Adjudications	4	7	14	17	18	40	27	31	17	26	9	24
Average Days for fastest 90%	176 days	176 days	177 days	129 days	193 days	166 days	165 days	152 days	218 days	143 days	188 days	169 days

Personnel Security Management Office for Industry (PSMO-I) Update

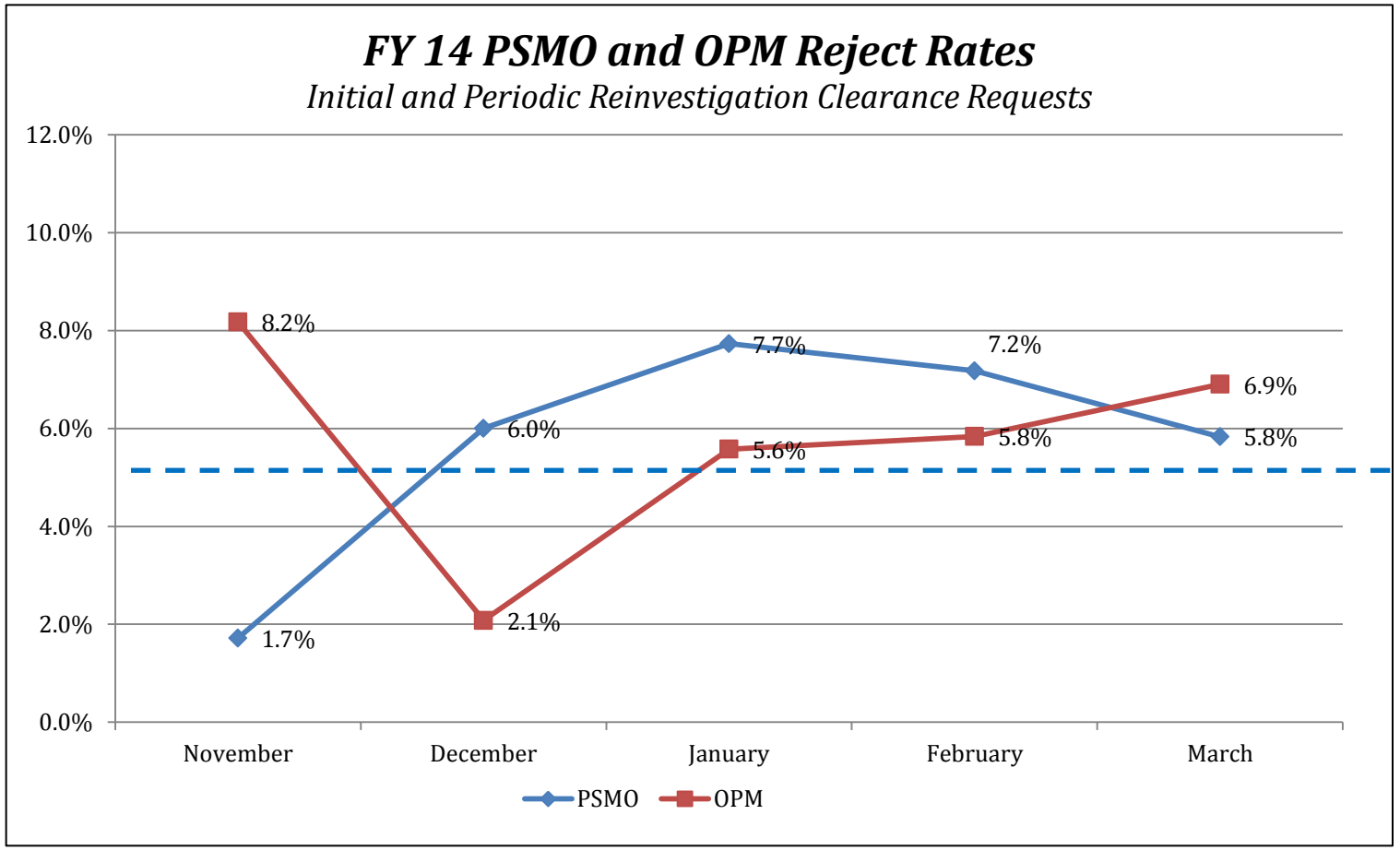
2014

Presented by:
Laura Hickman

eFP Submissions



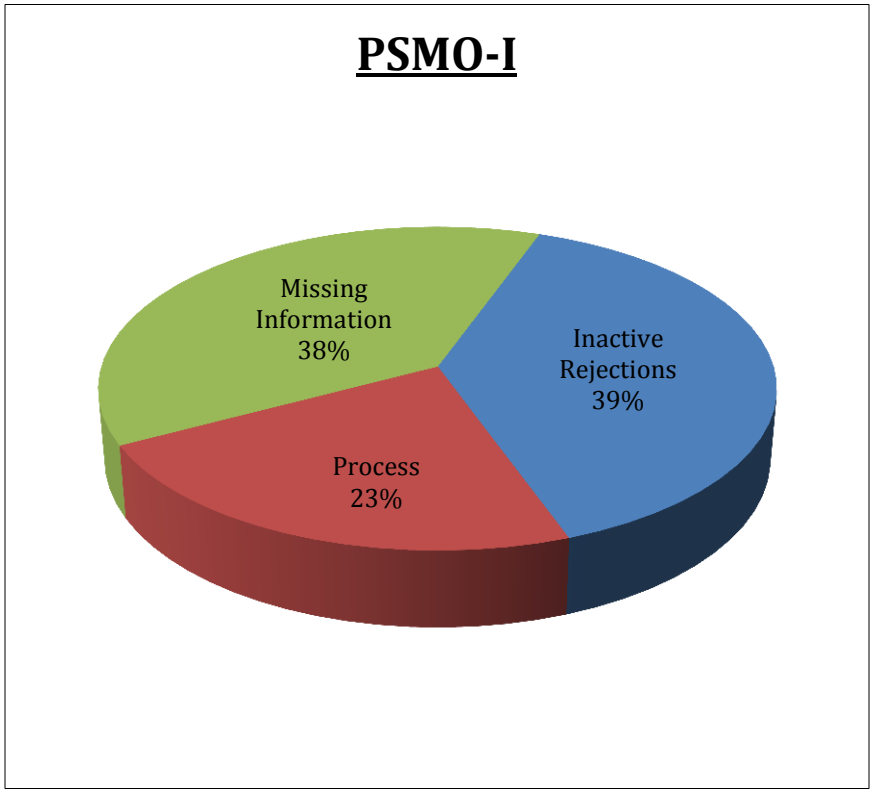
e-QIP Rejection Rates – FY14

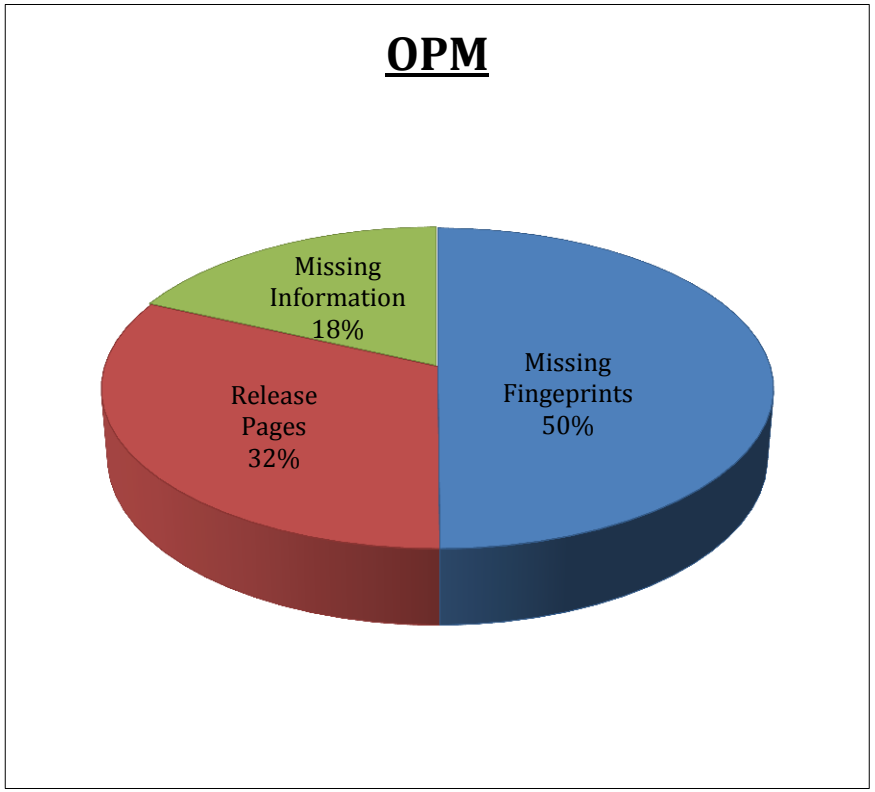


e-QIP Rejection Reasons – FY14

FY 14 PSMO and OPM Reject Reasons

Initial and Periodic Reinvestigation Clearance Requests





Process - Rejections or stoppages that occur because there wasn't a need for the submission. Typically regarding PR's submitted when they're still in scope or an investigation request that was submitted but a valid reciprocal action could be made instead.

Inactive Rejections –Rejections that took place for release pages as well as access vs. eligibility reasons. PSMO-I is no longer rejecting