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

The NISPPAC held its 47th meeting on Wednesday, March 19, 2014, at 10:00 a.m. at the National Archives and Records Administration (NARA), 700 Pennsylvania Avenue, NW, Washington, DC 20408. John Fitzpatrick, Director, Information Security Oversight Office (ISOO) chaired the meeting. Minutes of this meeting were certified on May 30, 2014.

I. Welcome and Administrative Matters

Mr. Fitzpatrick welcomed the attendees, and after introductions, reminded everyone that NISPPAC meetings are recorded events. He then asked Greg Pannoni, the NISPPAC Designated Federal Official (DFO), to review the Committee's old business. (See Attachment 1 for a list of those in attendance.)

II. Old Business

Mr. Pannoni reviewed the four Action Items from the November 14, 2013 NISPPAC meeting. He reported that the briefing to update the Committee on Executive Order (E.O.) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," which had been postponed at the November 17, 2013 meeting would be presented at the meeting. Next, he stated that Pat Viscuso, ISOO, would provide an update on Controlled Unclassified Information (CUI). Next, he noted that ISOO served on OMB's Suitability and Security Clearance Process Review and was asked to represent NISP issues in the review's work with respect to clearances and the clearance process. He reminded everyone of the recent plethora of activity at the highest levels of the government as a result of the Washington Navy Yard shooting and recent unauthorized disclosures. He noted that the results of those studies were released the previous day would get continued attention through implementation of recommendations. Finally, Mr. Pannoni informed the membership that a representative from the Office of the Director of National Intelligence (ODNI), the Security Executive Agent with responsibility over security and public trust clearance processing, would provide a presentation on the Continuous Evaluation (CE) Program. (See Attachment 2 for a list of Action Items).

III. Reports and Updates

(A) Department of Defense (DoD) Update:

Valerie Heil, Office of the Under Secretary of Defense for Intelligence (OUSD(I)) announced that the Secretary of Defense released the final recommendations (see http://www.defense.gov) from the security standards review process regarding the Washington Navy Yard shootings. She described the four key recommendations as (1) implementation of the CE program as an OUSDI(I) and Office of Personnel Management (OPM) coordinated effort to provide automated records checks of personnel with access to DoD facilities and/or classified information, (2)

establishment of a DoD insider threat management and analysis center, (3) centralization of authority, accountability, and programmatic integration under OUSD(I), and (4) expeditious deployment of resources required in behalf of the identity management enterprise services architecture. Next, she noted that the National Industrial Security Program Operating Manual (NISPOM) conforming change #2 was in DoD formal coordination process is nearing completion, and that the changes will include the requirements for insider threat minimum standards, as well as proposed text related to Section 941 (cyber incident reporting) of the FY 2013 National Defense Authorization Act. Further, she reminded the Committee that the NISPOM Working Group's Chapter 8 initiative has also been included in the proposed update. In addition, she explained that DoD hopes to have the final status change update by the next NISPPAC meeting, and reminded industry that once the conforming change is published they will have six months for implementation. Finally, she described OUSD(I)'s establishment of new minimum requirements for the issue of an interim eligibility to access Secret (S) and Confidential (C) information, and that these requirements include a review of the fingerprint check before the Defense Security Service (DSS) can grant the interim clearance. OUSD(I) has given DSS 30 days from the time they certify completion of the testing phase to declare its functionality and to advise industry on the use of the new criterion.

The Chair then spoke to the serious incidents that precipitated these reviews, stating that not only the tragedy at the Washington Navy Yard but also the significant unauthorized disclosures the government has been dealing with since WikiLeaks have resulted in continuing and escalating attention on making fundamental changes in the personnel security process. Further, he noted that the link between personnel security and the government's need to reform its practices to ensure the protection of both the workforce and national security information, now places significant focus at the top levels of government that it has rarely been seen before. In addition, he suggested that announcements both from DoD and the Office of Management and Budget's (OMB) government-wide review were going to sustain those topics at the senior government level of attention for a long time. Continuing, he noted that even as the area of unauthorized disclosures activity is somewhat less publicized than the Navy Yard incident, there will be a complete integration with these concerns, and that the National Security Council is now putting increased attention not only on things cyber and things related to information assurance on classified systems but also on strengthening personnel security management practices and integrating both management decisions and awareness of personnel security importance and the processes that serve personnel security. Finally, he pointed out that the agencies responsible for making these enterprise level and executive branch level changes are all the ones you would expect, and that we in federal, civilian, and military services will need to extend our efforts to all aspects of state, local, tribal and private sector sharing. He opined that in a forum like the NISPPAC we must continue and even strengthen the relationships established around the NISP to put the focus on the industry experience and the impact to the government-industry partnership that these changes will bring. However, he advised that we must understand that the drive for these changes happens and is being worked outside of the NISP channels, and that our focus will be to bring it together, whether through CE or insider threat or changes to policy, increased across-channel attention to the goals implicit in these initiatives. In addition, he suggested that we must take advantage of the opportunity to be heard regarding how it all affects us, and that even though we do not yet have answers to all our questions, we must begin the conversation, and be patient as the government sorts out the many moving pieces. He noted that

in the days following the announcement of the initiatives outlined in the OMB release, the primary focus will be first on congressional interaction and answering the needs that happen there, and that this partnership must continue to bring questions forward, but with the understanding that everything will now be colored by the impact of these initiatives.

(B) DSS Update:

Stan Sims, DSS, reviewed the results of the recent government and industry stakeholders' meetings and noted that there was a general interest in a review of DSS' oversight processes and procedures and specific interest on the PCL process. He noted that the stakeholders have been having extensive discussions on the Defense Federal Acquisition Regulation Supplement's (DFARS) clause on the safeguarding and protection of DoD unclassified technical information, and that they welcomed Ms. Kristen Baldwin's, DoD's Office of Acquisition, Technology, and Logistics (AT&L), update regarding the ongoing actions related to that clause, as well as the efforts of the DoD data vulnerability tiger team in developing an implementation plan for the clause's execution. He pointed out that Industry, represented by Mr. Tony Ingenito, had an opportunity to ask questions, voice concerns, and discuss the items of information that they need in order to execute the provisions of the clause. Next, he noted progress with regard to the ongoing revisions to the National Interest Determination process, and that it will then be fully coordinated, once it completes DoD legal review. He then presented updates regarding other DSS initiatives affecting Industry stakeholders in which he described efforts to assist in the oversight of the National Industrial Security Program (NISP) objectives, the Command Cyber Readiness Inspection process, as well as some ongoing education and training initiatives. He highlighted that the DSS recently added several important toolkits to their website (www.dss.mil), to include the Facility Security Officer's (FSO) toolkit, which he described as a single point, role-based resource developed in support of industry partnerships. He noted that DSS has increased the use of webinars as a vehicle to share knowledge with cleared industry partners, as well as implemented additional automation initiatives, such as the automation of the DD Form 254 and the subsequent collaboration with AT&L to host the product on their server. Finally, he described the ongoing efforts to automate the Industrial Security Facilities Database, which is used by both federal government and our industry partners.

(C) Combined Industry Presentation:

Tony Ingenito, Industry, began (see Attachment 3) by expressing industry concerns regarding insider threat requirements under E.O. 13587, and stated that industry continues to remains in touch with as many organizations as possible in order to stress their perspectives on the imperative for consistent requirements across all the user agencies. He added that industry and the Central Intelligence Agency have reviewed their insider threat programs and reached consensus on contractual requirements. Also, this stresses consistent process application, and ensures that industry can surface areas of concern that could represent potential problems. He reminded the Committee that he has previously discussed two-person integrity (TPI) concerns relative to affordability and the lack of risk mitigation, and that there has been no indication that organizations will be abandoning TPI below the Sensitive Compartmented Information level. Regarding CUI, industry still eagerly awaits program and policy updates, especially as we continue to see premature and inconsistent application. Again he stressed industry's plea for

cross-agency standardization in order to protect of this critical material in a cost-effective manner, and he remarked positively on Ms. Baldwin's close scrutiny of their concerns. He pointed out that while the initial DFAR changes will be applied to new contracts, that there has been some e-mail traffic suggesting broader implementation. In terms of information technology security, he described actions and overall policy as remaining consistent, but suggested that some controls continue to be interpreted differently by various programs and agencies which in turn created multiple approval and tracking problems. In the case of DoD policies, industry foresees many new things on the horizon, even as they continue to function under a series of interim instructions. Therefore, they are looking forward to getting everything finalized so as to eliminate so much implementation latitude. With regards the work of the Personnel Security Clearance Working Group (PSCWG), he noted efforts to move beyond simple metrics tracking, and to focus on sequestration recovery plans, and out of scope periodic reviews. He reported that the stakeholders had broached that subject at the last meeting, and that the government has renewed its interest in working with industry, and have even reached out to both the DoD Central Adjudication Facility (CAF) and the Personnel Security Management Office (PSMO) to help industry work some high priority problem cases. He noted that as the Enhanced Security Clearance Act is now law, industry should be able to assist with an implementation plan that achieves consistency among all industry partners. He asserted that industry still has concerns, and feels it has made little progress, with regards to Defense Office of Hearings and Appeals (DOHA) caseloads, and particularly in terms of the need for increased exposure and transparency related to caseload volume and age, and noted that Industry's real concern in this arena was that cases have been in the pipeline for up to two years or longer without a ruling, even as the individuals continue to be provided access, which they believe enhances insider threat vulnerability. The DoD CAF agreed to attempt to gather and report such data in the spirit of reducing longstanding cases.

Mr. Ingenito then reviewed the other programs requiring immediate attention from industry resources, specifically the progress made to date on next steps in the NISPOM conforming change process, the continued work on the DD Form 254 automation project, the Special Access Programs Working Group, and the CUI program documentation process. He explained that all were proceeding as anticipated, and that industry was looking forward to being included in the planning and development phases of each. In addition, he called attention to the Windows XP retirement efforts, and especially the continued concerns regarding mitigation. However, he reminded the Committee that there are a number networks and systems that still have to remain on Windows XP because our customer platforms still require its use, and that industry remains concerned that this is a far-reaching and complex process, and fears that even after having been raised the issues to several different levels it appears likely that we are beginning to negatively impact our ability to support the war-fighter in these particular programs. Therefore, industry is anxious to see what we're able to get out of this with regards to mitigation, as well how this impacts across all of our existing programs. He concurred that the recent stakeholders' meeting was of significant value, as industry was able to effectively highlight many of their desires, especially from the enterprise and capability standpoint. He noted that it is refreshing to discover that over 100 DSS representatives played a significant role in establishing user requirements, and that these were consistent with industry's concerns, and that they were pleased with the back and forth flow of dialogue and expect to continue to make good progress. In response to a question from Mr. Pannoni regarding when industry will be allowed to comment on the AT&L

guidance since it will impact future Industry execution of the policy, Ms. Heil noted the policy will be made available to industry once it is published. The Chair suggested that perhaps we need a greater understanding of the acquisition community guidance particulars, and especially those portions which will ultimately migrate through NISP channels to the contractors. Mr. Sims pointed out that Ms. Baldwin had made it clear that once the guidance reaches a certain level her office would try to present industry with some level of awareness as to its content and direction. Jim Shamess, Industry, then asked if it would be appropriate to have an AT&L representative speak directly to the Committee on this and/or similar actions. The Chair responded that at some point such may be advantageous, and that at present the current DoD membership is already involved in working many of these issues and he therefore he recommended that we allow them sufficient opportunity to yield results and then coordinate all the moving parts between the cyber, acquisition, security, and industrial communities. The Chair remarked about his objectives regarding information sharing within this forum, so as to provide as much information as is possible about the complete contractor experience in the personnel security processes, as well as in all the places those processes occur in government and industry together. He noted that we have consistently and regularly heard over the last couple of years from each of the organizations who provide security clearances and who contribute their performance measures and metrics on the established phases of the process, and this has resulted in the opportunity for our membership to examine the particulars, and then to compare these with their own experience. He added that by so doing, we have been able to evolve our process and thus constantly refocus the efforts of our PCLWG. He added his desire was to continue to achieve those goals made possible through the efforts of the PCLWG, but noted that their report format will undergo a profound change between this meeting and the next and move from the "so what" approach that had employed up to now, to one more oriented toward addressing industries primary issues and concerns. He noted that the metrics will continue to be made available through the meeting record. He challenged the PCLWG participants to ensure that they capture this new and desired sense of direction and content.

(D) PCLWG Report

Steve DeMarco, DoD CAF, reported (see Attachment 4) on the CAF's overall performance, and noted that while some fiscal quarters had been fairly stable, others had experienced significant fluctuations. He suggested that these could well be attributed to a combination of budget issues, followed by sequestration and furloughs, DSS's need to temporarily suspend Electronic Questionnaires for Investigations Processing (e-QIP) submissions, and the typical increases during holiday leave. He noted that it was January (2014) before they could begin to achieve their a nine percent reduction in the backlog, which resulted from reallocation of resources, and the introduction of a new DoD operating manual which consolidated our processes from five divisions into one. He noted that they have been training increasing numbers of adjudicators to perform "due process" work. He explained that the CAF has now assigned a "due process" adjudicator to each of our teams, so that when we encounter a case that has specific issues, we can quickly begin to prepare it for submission to DOHA, thus eliminating the addition of another case to the backlog. He noted that they now prioritize their workload in such a way as to assign a group of people on the oldest work, in order to achieve a first in-first out posture. He advised that the DoD CAF presently has approximately 50% of our adjudicators working the "due process" workload, so that they can reduce the backlog as quickly as possible. He noted that the

metrics for the period illustrate that 92% of industry cases are adjudicated within 30 days. In addition, he explained that they have improved productivity by establishing a set level of weekly case processing standards, and that they have enhanced the DOHA outreach methodology, so that together they process greater work flow and do so more efficiently. He stated that the Director's assessment is that they will fully eliminate the industrial backlog prior to the end of fiscal year 2015, and that they will continue to dedicate more and more resources to that goal. He reported that overall the workforce seems to be performing better than expected and anticipated that this will continue, and expressed hoped that these objectives, coupled with a concerted overtime effort now in place will ultimately drive down the workload. In response to a question from Mr. Pannoni, regarding the workload of the DOHA adjudicators, Mr. DeMarco responded that once the due process cases are prepped they are sent DOHA, where a legal counsel determine whether or not they meet the criteria for issuance of a statement of reasons (SOR) and if certified, it is returned to the CAF who sends the SOR to the subject. He explained that once the subject responds, the case is then sent back to DOHA, who will in turn generate a letter of denial, or they will adjudicate the case, so such cases rest in two places simultaneously. The chair then pointed out that the DoD CAF's move to Ft. Meade obviously necessitated some process changes, and ultimately affected what portion goes to DOHA and what part goes to the DoD CAF's, and that there is not a clear understanding of the entire process. He then asked the PCLWG to provide an explanation of what precisely has changed and what is now the status of handling the backlog and the proper accountability for how these things get resolved. He pointed out that the changes and advantages in consolidating procedures in the DoD CAF have already altered everybody's understanding of how the DoD CAF processes its caseload. Mr. Sims reminded the Committee that DSS had taken on this action in yesterday's stakeholder's meeting to work with the DoD CAF to give industry more clarification as to what the backlog really represents.

Chuck Tench, DSS-PSMO, began by explaining that they try to keep two days of inventory on hand at all times, or between1,000 to 1,200 cases (see Attachment 5). He noted that under normal circumstances they acquire approximately 600 investigations a day, and that before the furlough they were at 864 investigations, and or roughly two days in arrears, but then peaked at 13,992 cases after the furlough, the shutdown, and their moratorium on submissions to OPM. He advised that with overtime and 23 employees they were able to substantially cut into that backlog, and currently only have 3,900 investigations in the queue. He noted that the PSMO quality assurance check of the release pages will now revert back to the old process where OPM reviews the pages and directly contact the FSO submitting the package, and that those rejections will be reported through OPM. In addition, he noted that they were shifting some resources between the CAF and DSS which will result in a more collaborative effort and thus relieve some of the CAF's workload. He stated that the key to success here is to provide as much information as is practical, and with as much accuracy as possible, as that will dramatically submissions and investigations timelines. Concerning electronic fingerprint submissions to OPM, he noted they were definitely on an upward trend, with the 75% rate in January, and increasing to 87% in February. Also, he advised that there are going to be changes in the interim clearance process, which will entail a review of the Standard Form 86, and the results of OPM's review of the national databases. He added that they had begun testing OPM's release packages, as well as the testing of the electronic adjudication business rules for electronic interim releases. He noted that the PSMO was planning to model the National Agency Check, Local Agency Check for

electronic adjudication, after they achieve interim ingest into the Clearance Adjudication Tracking System. In addition, PSMO will examine any key management personnel who enter the interim guidelines through the electronic adjudication process, so as to increase process strength and reduce risk. He advised that, there is now a link on the PSMO website that identifies all approved Secure Web Fingerprint Transmission vendors. He noted that of the over 5,000 fingerprints submitted in February only 648 were in hard copy mailed to OPM, and that DOD was slowly but surely reaching the 100% electronic submission target. Finally, he explained the channels of communication that the PSMO office leverages through DSS to industry in order to get the word out to all concerned that there are changes in processes.

Mark Pekrul presented the metrics for the Department of Energy (DOE) (see Attachment 6) and reminded the Committee that the metrics reflected for DOE include both their federal and contractor employees, and that approximately 90,000 individuals are cleared, and roughly 90% of those are contract employees. Further, he added that although DOE does continue to meet its obligations and goals for initial submissions and adjudications, there are slight increases over the last several months due to sequestrations, shutdown, and holidays.

Valerie Kerben, Nuclear Regulatory Commission (NRC) announced that NRC's metrics were performing quite well and especially that those from the second and third quarters would definitely meet all IRTPA goals (see Attachment 7). She reminded the Committee that due to their unique processes it takes NRC slightly longer to initiate cases, but that nevertheless they are meeting submission timeliness objectives, and that their submission reject rate to OPM is always less than 5%, and that they are getting few fingerprint e-QIP kickbacks. In addition, and as in the case with DOE, their cases that are submitted to OPM reflect both federal and contractor employees, as well as their licensee population. Further, she pointed out that NRC has made significant improvements both in submission and adjudication in Secret and Top Secret initial submissions and adjudications, meeting many more goals this year. Also, their Periodic Reinvestigation (PR) program remains strong as well, as they attempt to complete more high risk category personnel. Finally, and as a result of an ODNI initiative, they have revalidated their clearance numbers, resulting in an approximately 20% decrease in Q level clearances, as well as some contractor clearances.

Christy Wilder, ODNI, began with a recap (see Attachment 8) of the timeliness metrics for the Intelligence Community's (IC) fiscal year (FY) 2013 Initial Investigations and PRs. She explained that these figures would drive the information contained in the Intelligence Authorization Act (IAA) reporting requirements as well as the ODNI's agency-specific annual performance letters. She reported that the Secret investigations, including initiations, investigations, and adjudications all met their goals. However, the TS investigations for the same time period did not achieve equal success, as some of the required adjudication times exceeded timeliness goals. She advised that overall it took less than four months from the time the person signed the SF-86 until they were performing the job, and that this represents a dramatic improvement in past year's performance. For PRs the story is much the same as with the TS figures where we again encounter timeliness problems only in the adjudication part of the process. Also, as in the case of the initial PR figures, we enjoyed overall success, in that it took less than five months to conduct a PR, which is well within the goal. Next, she explained that the Report on Security Clearance Determinations, a requirement of the IAA, is not yet approved for briefing to the NISPPAC, as it has not yet been released to Congress, and that she hoped to

brief it at the June meeting. The Chair asked that the ODNI representative to send ISOO a link to the report's contents should it become available prior to the next NISPPAC meeting, so that we could distribute the particulars to our membership. She then remarked on the previously issued executive correspondence requiring agencies to validate their clearances, stating that this initiative has already met with some considerable success, as over 70% of the agencies have already completed validation and responded to the ODNI, and that those who have not yet reported have been approved for extensions. Finally, Ms. Wilder summed up some of the initiatives, in addition to timeliness factors, being worked by the ODNI. She stated that they are now beginning to focus on other areas needing improvement, specifically quality, reciprocity, and out-of-scope PRs. To that end, she reported that the reciprocity study begun approximately one year ago was now in its final stages of completion, and that they would soon have a new metrics framework for identification of reciprocal actions, as well as measurement totals by which agencies assess and improve upon them. Regarding out-of-scope PRs, the ODNI remains extremely concerned with their volume, as well as how they can be measured, and believes that the new CE initiative may be the long-sought-for-answer.

(E) The Continuous Evaluation (CE) Program

Brian Kelly, ODNI, briefed the CE program (see Attachment 9), explaining that E.O. 13467, **"**Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," defines the CE process as "reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility." In addition, he noted that E.O. 12968, "Access to Classified Information,"(as amended by E.O. 13467) states that "any individual who has been determined to be eligible for or who currently has access to classified information shall be subject to continuous evaluation under standards (including, but not limited to, the frequency of such evaluation) as determined by the DNI,", and that the Federal Investigative Standards (issued jointly by the DNI and the Director of OPM in September 2012), "requires that a continuous evaluation program be in place for all individuals cleared to Tier 5 (individuals eligible for access to TS or TS/SCI information, or eligible to hold a sensitive position)." He further described the process as an attempt to bridge the gap between the initial security investigation and the five- or 10-year PR. He described the benefits of the new initiative as the ability to know more about an individual, which helps management to better assess risk factors and that agencies will be more amenable to issues of reciprocity, as they will know that information associated with background investigations and access are both current and comprehensive. He noted that there has also been much discussion about whether or not, in light of the ongoing nature of CE, a PR is still necessary. He explained that certain kinds of investigative information, such as TS/SCI level information, are available only through the PR process which produces an updated SF-86, as well as a new personal security interview. He explained that CE will also assist in workforce management by identifying trends in individuals who are developing poor financial responsibility, and act as a tool to prevent or modify undesirable behaviors. He explained that they are going to develop, a government-wide monitoring program that extends to all people (military, civilian, government, and contractor

personnel) who hold, or would hold a security clearance. He noted that CE will be phased in over a period of three years with the first goal to develop initial operating capability by the end of FY 2014, which will involve a small set of agencies at the TS/SCI level IC agencies (high risk population), and embrace a limited number of data sets, so as to build the foundation for a much more extensive program. He explained that it will be fully implemented by the end of 2016, and that the rate of implementation from agency to agency will ultimately depend on a number of factors, not the least of which being how an agency identifies its highest risk people, and/or the number of people and resources that can be allocated to resolving timelines issues. He noted that they will need to develop a risk-based algorithm in order to identify what the target population should be, so as to ensure that we reach the most high risk candidates. He observed that another obvious benefit of the CE program, and one that was practically impossible before wherein we would lose contact with personnel who have had a mobile or fragmented career path, is that we will be able to capture an individual's performance statistics and behavioral trends from job to job, which will dramatically enhance any number of types of information sharing.

Mr. Kelly noted that CE will ultimately provide another way to combat the insider threat, because it will rapidly improve the ability to document and monitor travel, finance, and criminal conduct behaviors, while building greater trust in our workforce. In response to questions from Leonard Moss and Kurt Poulsen, Industry, regarding accessing databases for information regarding CE activities, he responded that there are plans for a single database that would permit an agency to capture information that has been flagged for its needs. He explained that the size of the database is not a barrier to either access or reliability, as each agency will own the information relative to its population, and that the flagged information will enter the database from both unclassified and classified sources where it will be sanitized, and then be made available in an unclassified format. Ultimately, some data will be supplemented by other classified data. In short, he explained that the system will perform as an identification and flagging tool only, and that it will remain the prerogative of each agency to capture and process the information into its own case management system. He noted that there will be a feedback loop showing which issue(s) has been identified and resolved, as well as a way to supplement the database with the agency's own investigative data. The Chair repeated Mr. Kelly's initial warning that the system is yet in the early stages of development. He reminded the membership that they should read the recently released OMB report, and particularly the recommendations in Section A that describe what CE is intended to produce and how it will increase the information available to be used in decision making, and Section C that describes the information technology architecture that is to be developed and integrated across all agencies.

(F) E.O. 13587 Update

The Chair introduced Ray Sexton, explaining that he was from the Office of the Program Manager for the Information Sharing Environment, which is the home for the Classified Information Sharing and Safeguarding Office (CISSO), the interagency coordination entity for all things related to E.O. 13587. Mr. Sexton began (see Attachment 10) by reviewing the CISSO's five original priority areas: controlling removable media, the identification of ways in which management might reduce anonymity and increase user attribution, building a more robust insider threat program, enhancing access controls, and improving enterprise audit capabilities. He described extensive modifications being made to the key five priorities as a result of the

recent massive leaks of extremely sensitive classified information. He cited as examples: that the control of removable media had been moved to a maintenance mode, and that identity management, had become the Senior Information Sharing and Safeguarding Steering Committee's (SISSSC) top priority. He noted that the SISSSC is trying to integrate all the efforts into one, which has become their primary focus for the foreseeable future. He remarked that this affects our industry partners because of the enhanced emphasis being placed on CE. He estimated that the increased scrutiny on maintaining personnel security will result in a sixth priority of Continuous Monitoring and Diagnostics (CMD), with the ultimate goal to diminish the delta between detection and action. The chair summed up the process as the rapid development of a far-reaching capacity that scrutinizes systemic maintenance and activity through continuous user monitoring. He noted that chief information officers will now be able to generate an automated capability to monitor and report information assurance status, as well as providing a link to insider threat needs, much in the same way as envisioned in the Federal Information Security Management Act. Mr. Sexton added that in fact there has been some confusion between the objectives of CE and continuous monitoring, and the hope is that CDM will eliminate this dichotomy. He noted that the recent CISSP's report to the President, on the policies and safeguarding processes, included 61 long-term and short-term recommendations. He advised that the 61 recommendations ranged from short-term objectives such as discovering privileged users and verifying their clearances to long-term initiatives such as Cross-Agency Priority objectives, Credential and Access Management, spear phishing, and CDM objectives. The chair added that Tab A of the White House Tasking initiative contained a specific callout to the NISP process, stating that anything touching the cleared contractor community will come through ISOO and the Cognizant Security Authorities in much the same way as with the NISPOM conforming changes.

Mr. Sexton noted that some other proposals are geared towards reducing the number of privileged users, minimizing the number of roles an individual is permitted to have, and/or what types of roles might an individual be permitted to assign to himself, and that some of these issues might need to be addressed by a committee like the NISPPAC. He opined that the recent Navy Yard incident prompted a 120-day review of security clearance suitability issues, and resulted in more emphasis being placed upon CE, and that in view of the fact that a number of these recent security-related breaches involved cleared contractors, there is now increased vigilance towards industrial security clearance processes. He reported that the President's Review Group on Intelligence and Communications Technologies, considered a sliding scale of security versus privacy and made some 55 recommendations, of which 38 were approved and that from that number, the Steering Committee is charged with the execution of approximately 10 recommendations from the White House tasking. Mr. Sexton noted that in the interest of constant budget reform, every participant in this vast process is making daily efforts towards streamlining safeguarding and security reporting, in order to reduce the number and frequency of agency and departmental data calls, and that the CISSO staff developed the Key Information Sharing and Safeguarding Indicators as a self-reporting tool in an attempt to combine these two requirements into one integrated effort. Vince Jarvie, Industry, asked whether anyone had considered the civil liberties side of the hiring question, and pointed out that many times industry personnel who have been judged unsuitable for a clearance because they represent a high security risk, are still approved for employment due to civil liberty issues. The Chair advised that it was a complex area, and that there are an entirely different set of rules in the federal

regulatory scheme for how government agency heads deal with their authority to bring personnel into the workforce, and that balancing Human Resources versus security interests is always difficult to achieve. He noted that those in government and industry who work in the NISP environment must provide as much information as is legal so that senior leadership is equipped with as much as can be known and applied toward making such decisions, and that a central theme in the 45-day report to the President clearly sends the message that department and agency heads must do a better job of balancing personnel security issues with mission issues at large. Mr. Sexton added that the issue is indeed a critical one, and that in the annual report to the President on information safeguarding, one of the key points is that we can develop all the electronics we want, add in all the continuous monitoring we can manage, and yet the question is still reduced to leadership, management, training, and culture, which are all human factors. Further, he noted that while the five priorities, are driven by technological factors, the human factors must be resolved by the responsible department and agency heads. The Chair added that in the context of the NISP, a perfect example of this attitude is the change offered in the conforming change process that proposes the notion of a senior agency official or company official to be the nexus for insider threat., similar to the process within the government where we have designated senior agency officials and they have this very clear chain from the President, to the department, to the agency head, and on down to the policy level, and we are now trying to build that chain and make it as clear as possible in the NISP and within the NISPOM.

(G) CUI Update

Pat Viscuso, ISOO, provided an update on CUI policy status, supplemental guidance status, and plans for its phased implementation (see Attachment11). He reminded the Committee that over the past year the CUI Advisory Council has been working on establishing the policy for safeguarding sensitive but unclassified information in accordance with law, regulation, and government-wide policy. He suggested that this primary objective had now been accomplished in that there are now standards established for safeguarding, dissemination, marking, and decontrol, and that these objectives have been encapsulated in two basic products. The first product is a high level policy guidance document which we are will ultimately incorporate into the Code of Federal Regulations (CFR). He explained that this was achieved through an agreement reached with the OMB's Office of Information and Regulatory Affairs (OIRA), which will open an interagency coordination process from April to July 2014, followed by a public comment process from July to November, and concluding with an adjudicated comments phase. He noted that once this process is complete, the CUI Executive Agent will initiate a supplementary guidance process, which will consist of consultations with the Council through which we will issue the actual marking, safeguarding, misuse, dissemination, and decontrol guidance. He noted that the CUI Council has been able to comment on the marking handbook, which covers such topics as commingling with classified portion marking, markings' appearance, placement, etc. The Chair reiterated that from a regulatory standpoint the higher level document is more appropriate guidance for the CFR and the supplementary guidance would be written in a way that could be more practically applied as the high-level implementer. For example, anyone familiar with ISOO's handbook on marking classification information will quickly recognize its new cousin, the CUI marking handbook, and that when this manual is ready we will make it available for perusal prior to the official comment period. Dr. Viscuso reminded the Committee that E.O. 13556, "Controlled Unclassified Information," calls for a phased

implementation process, and that ISOO is in consultation with affected agencies and OMB to complete the four phases of the implementation process: planning, readiness, initiation and full implementation. He noted that ISOO has received a variety of comments regarding the timeline and that ISOO is in consultation with OIRA on the implementation of the timelines within the Executive Branch. The Chair suggested that it was perhaps time for the NISP to develop an approach to implementing CUI which takes into account that the non-NISP parts of companies are going to have to deal with the bulk of the information and so our discussion should center on what components of NISP oversight might industry adapt and which might it differentiate itself from. He reminded the Committee that this is the approach we have already initiated in previous discussions, both from the industry side as well as the government side, and now it is time to get feedback from our partners. He suggested that the NISP partnership consider standing up a CUI Working Group along the lines of the other NISPPAC working groups. He asked for feedback from the membership on the actionability and value in pursuing such an endeavor.

IV. New Business

(A) Professional Certification Programs

Denise Humphrey, DSS, presented a briefing on the DoD Security Professional Education Development (SPeD) Program (see Attachment 12). She described SPeD as an initiative to professionalize the security workforce, and to ensure that there is a common set of competencies among security practitioners that promotes interoperability, facilitates professional development and training, and develops a workforce of certified security professionals. She explained that SPeD development is nearly completed and that they have completed the competencies inherent in the initial sequential professional certifications: the Security Fundamentals Professional Certification (SFPC), the Security Asset Protection Professional Certification (SAPPC), and the Security Program Integration Professional Certification (SPIPC). She described the SFPC as providing a recognized and reliable indication of a security practitioner's understanding of the basic concepts, principles, and practices needed to successfully perform functions, implement programs, and pursue missions to protect DoD assets, and noted that the SFPC must be conferred prior to receiving another core certification. She explained that the SAPPC provides a recognizable and reliable indication of a security practitioner's ability to apply foundational concepts, principles, and practices needed to successfully perform functions, implement programs, and pursue missions to protect DoD assets, and that SPIPC provides a recognizable and reliable indication of a security practitioner's understanding and ability to apply risk management and security program management concepts, principles, and practices. She pointed out that SPeD was tailored towards the application of government rules for government operations, and that it would be equally valuable for participation by our industrial partners who work with DoD programs and/or on military installations, who are often required to follow not only the NISPOM but also the rules within government workplaces. She noted that SPeD is designed to fill the void between what's commercially available and what we need for efficient and effective governmental operations. She explained that the Center for Development of Security Excellence (CDSE) has developed other specialty credentials such as the Adjudicator Professional Certification, Due Process Adjudicator Professional Credential Certification, Physical Security Certification, Industrial Security Oversight Certification, and Special Programs Security Certification. Finally, she noted that the CDSE was responsible for the management of

the SPeD initiative, and that their materials would provide information on how to reach them, as well as a list of authorized testing centers. She noted that the programs are free, and that one need only to establish an account in the CDSE's Security Training, Education, and Professional Portal (www.cdse.edu/stepp) to participate.

V. Closing Remarks and Adjournment

The chair noted that the next NISPPAC meeting will be held on June 19, 2014, from 10:00 a.m. to noon, at the conclusion of the NCMS's Annual Seminar at the Gaylord Convention Center, National Harbor, MD. He then reminded everyone that the budget circumstance for the Federal government, and NARA, remains as is the recent past, so our inability to reimburse for travel and other costs will continue as before. Finally, he noted that the target date for the third meeting in 2014 is November 19th at NARA. There being no further business, the meeting adjourned at 12:20 p.m.

Attachment #1

Attachment 1

NISPPAC MEETING ATTENDEES/ABSENTEES

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

• John Fitzpatrick,	Information Security Oversight Office	Chairman
• Greg Pannoni,	Information Security Oversight Office	Designated Federal Officer
• Stan Sims	Defense Security Service	Member/Presenter
• Ryan McCausland	Department of the Air Force	Member
• Dennis Hanratty	National Security Agency	Member
• Eric Dorsey	Department of Commerce	Member
• Richard Donovan	Department of Energy	Member
• Kim Baugher	Department of State	Member
• Anna Harrison	Department of Justice	Member
• Kathy Healy	National Aeronautics & Space Administration	Member
• Dan Cardenas	Nuclear Regulatory Commission	Member
• Anthony Ingenito	Industry	Member
• William Davidson	Industry	Member
• Phillip Robinson	Industry	Member
• Michael Witt	Industry	Member*
• Steven Kipp	Industry	Member
• J.C. Dodson	Industry/ MOU Representative	Member
• Stephen Ulate	Department of the Navy	Alternate
• Drew Winneberger	Defense Security Service	Alternate
• Lisa Desmond	Department of the Army	Alternate
• Michael Hawk	Department of State	Alternate
• Mark Pekrul	Department of Energy	Alternate/Presenter
• Valerie Kerben	Nuclear Regulatory Commission	Alternate/Presenter
• Kathleen Branch	Defense Security Service	Alternate
• George Ladner	Central Intelligence Agency	Alternate
• Richard Hohman	Office of the Director of National Intelligence	Alternate
• Valerie Heil	Department of Defense	Presenter
• Christy Wilder	Office of the Director of National Intelligence	Presenter
• Brian Kelly	Office of the Director of National Intelligence	Presenter
• Ray Sexton	ODNI PM-ISE	Presenter
• Steve DeMarco,	Department of Defense	Presenter
• Chuck Tench	Defense Security Service	Presenter
• Denise Humphrey	Defense Security Service	Presenter
• Ruth Olsen	Office of the Director of National Intelligence	Attendee
• Lisa Loss	Office of Personnel Management	Attendee
• Dan Purtill	Department of Defense	Attendee
• Tracy Brown	Defense Security Service	Attendee
• Chris Corbin	Department of the Air Force	Attendee
• Michelle Murdoch	Central Intelligence Agency	Attendee
• Karen Duprey	MOU Representative	Attendee

• Mark Rush	MOU Representative	Attendee
• Kirk Poulsen	MOU Representative	Attendee
• Robert Harney	MOU Representative	Attendee
• Leonard Moss, Jr.	MOU Representative	Attendee
• James Shamess	MOU Representative	Attendee
• Jay Buffington	Defense Security Service	Attendee
• Keith Minard	Defense Security Service	Attendee
• Christine Beauregard	Defense Security Service	Attendee
• Keith Minard	Defense Security Service	Attendee
• Jeff Moon	National Security Agency	Attendee
• Ron Jackson	Department of Treasury.	Attendee
• Mark Nolan	Department of the Army	Attendee
• Jason Shay	Nuclear Regulatory Commission	Attendee
• Mitch Lawrence	Industry	Attendee
• Jim Euton	Industry	Attendee
• Scott Conway	Industry	Attendee
• Steve Abounader	Industry	Attendee
• Michelle Sutphin	Industry	Attendee
• Aprille Abbott	Industry	Attendee
• Vince Jarvie	Industry	Attendee
• Shawn Daley	Industry	Attendee
• Priscilla Matos	Industry	Attendee
• Richard Weaver	Industry	Attendee
• Glenn Gates	Industry.	Attendee
• Dave Davis	Industry	Attendee
• Doug Hudson	Industry	Attendee
• Mark Theby	Industry	Attendee
• David Best	Information Security Oversight Office	Staff
• Alegra Woodard	Information Security Oversight Office	Staff
• Robert Tringali	Information Security Oversight Office	Staff
• Joseph Taylor	Information Security Oversight Office	Staff

* Attended via teleconferencing

.

Attachment #2

Action Items from March 19, 2014 NISPPAC Meeting

1. The Office of the Undersecretary of Defense for Intelligence will report to the NISPPAC when the Procedures, Guidance and Information (PGI) for the safeguarding and protection of unclassified technical information, is approved by the Defense Acquisition Regulation (DAR) Council, and will provide instructions on how to access the posting on the DAR PGI website and the link to the Defense Federal Acquisition Regulation .

2. The Chair instructed the PCLWG to:

A) Come up with a new format for presenting issues and areas of interest regarding industry's personnel security clearance processes, while providing the usual performance those metrics in an informal manner.

B) Provide the NISPPAC with an explanation of the changes in the DOD CAF processes relating to their accountability, processing and adjudication of the backlog of cases at the Defense Office of Hearings and Appeals (DOHA).

3. ODNI will present the results of the Intelligence Authorization Act (IAA) Report on Security Clearance Determinations to the NISPPAC at the June 2014 meeting

4. The NISPPAC will stand up an ad-hoc CUI Working Group to address industry and government issues and concerns regarding the implementation of CUI within the NISP community.

Attachment #3

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

Industry

19 March 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.
- TPI concerns relative to affordability and lack of risk mitigation if implemented beyond SCI.

Security Policy Update

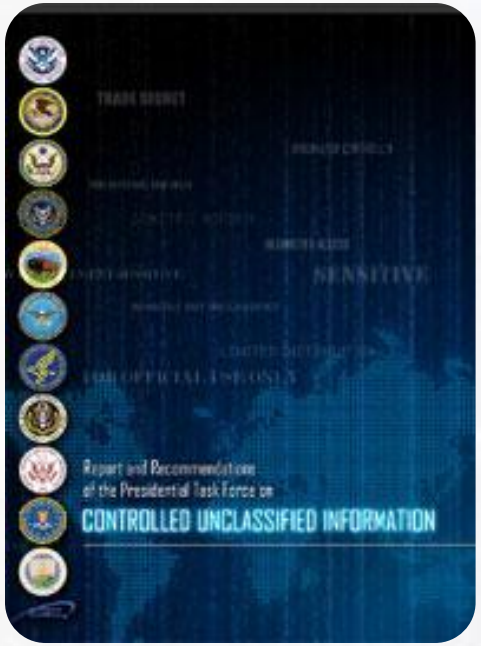
Executive Order #13556

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
  - Standard definitions to be published by NARA via CUI registry
- Pre-mature and inconsistent application and flow down already occurring.

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 and 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 effective implementation plan and identification of CTI is critical to successful implementation.
- Some UA notifications indicated intent to modify existing contract with clause and not fund implementation.

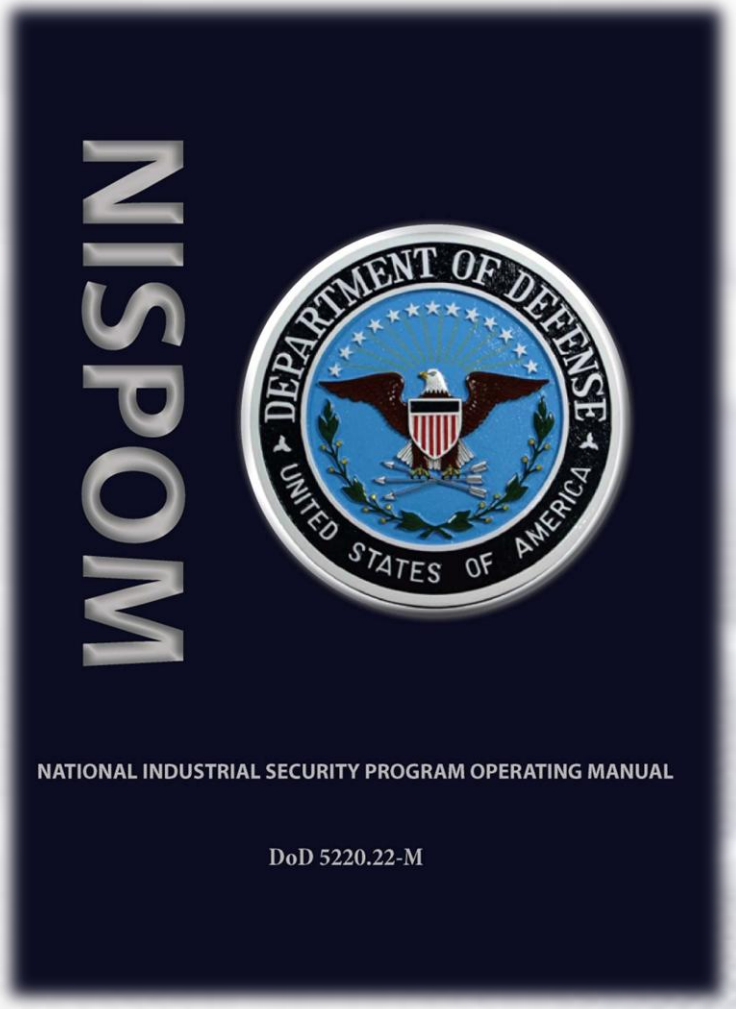
Security Policy Update

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
    - Missile Defense Agency
    - Air Force
    - Defense Information Systems Agency (DISA)

Security Policy Update

Industrial Security Policy Modernization



- National Industrial Security Program Operating Manual revision and update
- Department of Defense Special Access Program Manual development
- Industrial Security Regulation, Volume II update
- Special Access Program (SAP) Supplement being eliminated

National Industrial Security Program

Policy Advisory Committee Working Groups

- Personnel Security
  - Continued effects of Government Sequestration on clearance processing
    - Sequestration recovery plan. Out of scope PR causing issues.
  - Enhanced Security Clearance Act of 2013 impact (Involvement in implementation plan development)
  - Transparency with DOHA caseload and aging of cases
- Automated Information System Certification and Accreditation
  - Question on XP mitigation and impacts across existing programs.

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
  - Automated DD254 System
    - Standing by for ability to beta test
  - Development of National Industrial Security System (NISS)
    - Participating on the system requirements phase
- ISOO sponsored Ad-hoc SAP Working Group
  - Meetings as necessary in 2014
  - SAPCO's and Industry working changes and issues

Additional Significant Activities

- Controlled Unclassified Information
  - Meeting with ISOO and CUI Executive Agent Team on 17 July 2013
  - Excellent exchange on Industry Implementation efficiency options
    - Comments to draft implementation submitted
    - Awaiting further implementation SOP review
- Insider Threat
  - Leverage collective experience and benchmark practices to
    - Support Government policy and tools development for successful operational implementation
    - Meet National Security Insider Threat objectives
      - Provide support to public policy development (e.g., NISPOM Conforming Change #2)
      - Liaison with MOUs, NISPPAC, other ASIS Councils, Government and Commercial Entities (e.g., financial, gaming, medical, and chemical) “Best Practices”
      - TPI concerns relative to affordability and lack of risk mitigation

Attachment #4

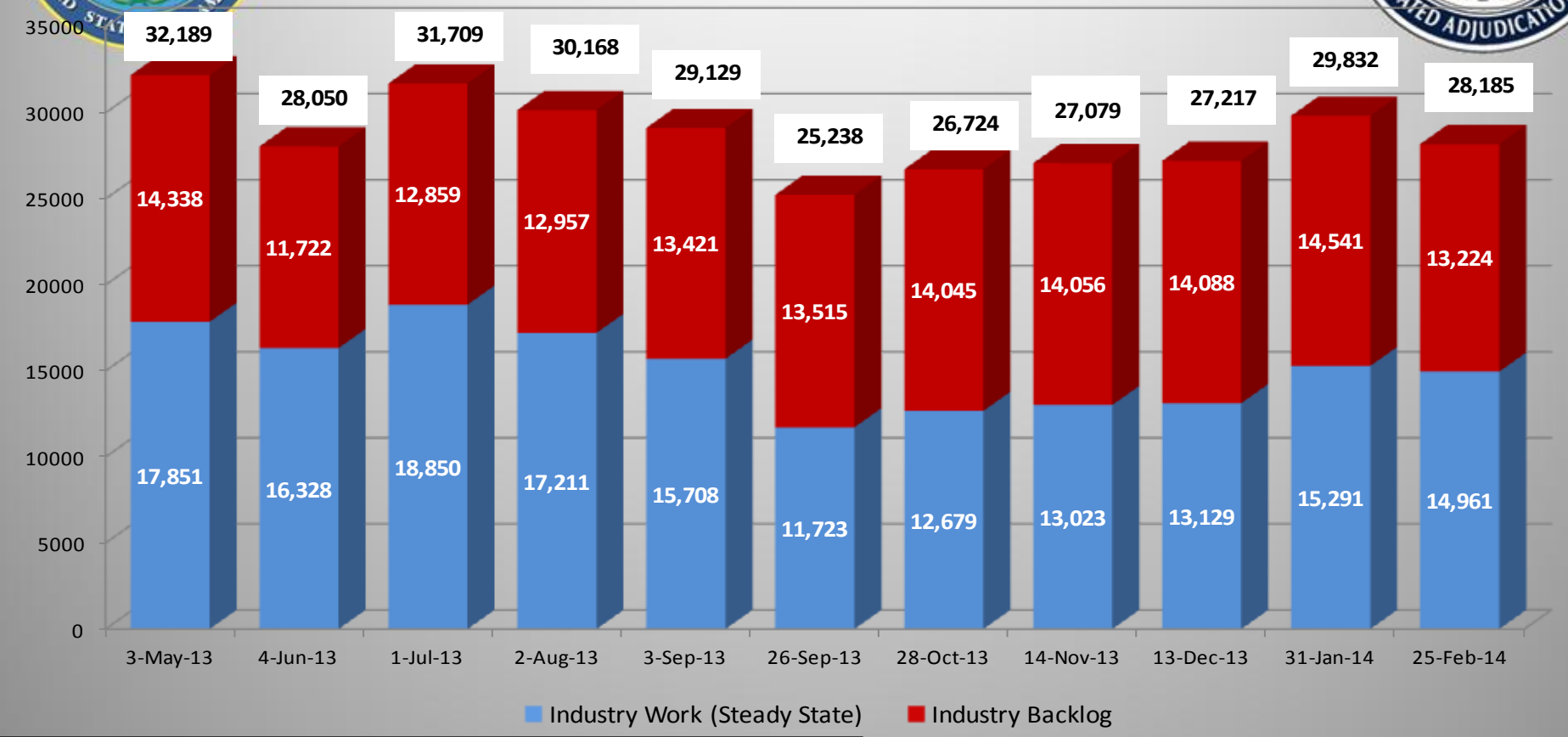
DoD Consolidated Adjudications Facility (CAF) Presentation

to the

The National Industrial Security Program Policy Advisory Committee

March 19, 2014

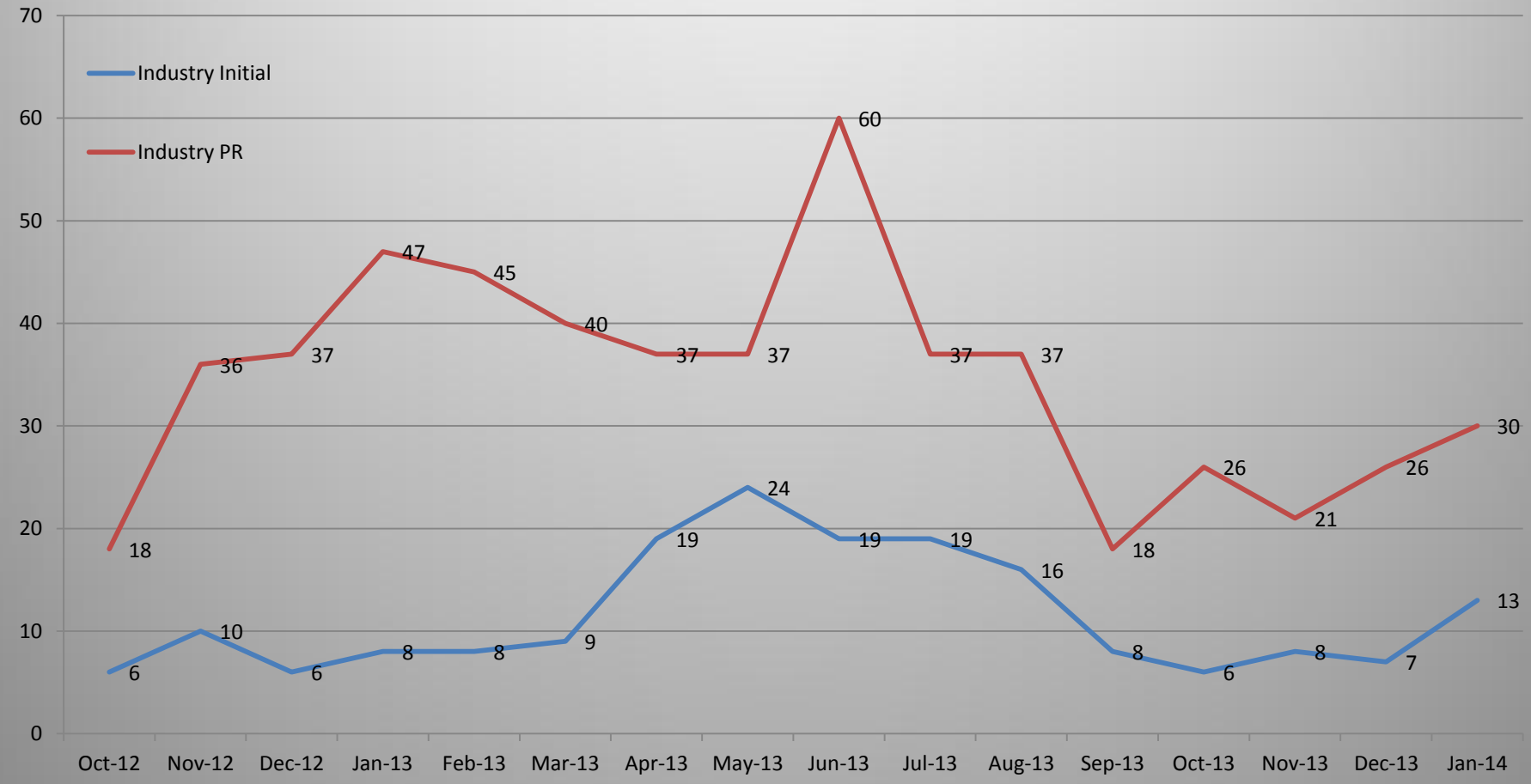
DoD Consolidated Adjudications Facility (CAF)
Pending Industry Workload



- **Backlog increase influenced by:**
  - ✓Holiday leave period
  - ✓46% increase in weekly receipts, 5 Jan- 1 Feb
  - ✓Adjustment to DISCO/DOHA merger and learning DoD CAF SOP
  - ✓DSS submitted suspended PRs from FY13; 12K of 17K released to date
- **W/O OT, (1 Oct-25FEB) negative trend would be 3,772 higher**

Month	NISP Backlog	Annual NISP Receipt	Backlog % of Total NISP
April 13	14,702		8.1%
February 14	13,224		7.3%
	-1,478	~ 180,000	

Industry
Intelligence Reform and Terrorism Prevention Act Performance



- **Efficiencies beginning to be realized by merger of Industry adjudicators**
- **Timeliness to fluctuate/increase during FY14-15**
- **Overall Dod CAF timliness edged up in FY14 as well**

DoD Consolidated Adjudications Facility (CAF) Summary and Takeaways:

- **IRTPA**
  - > 92% 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

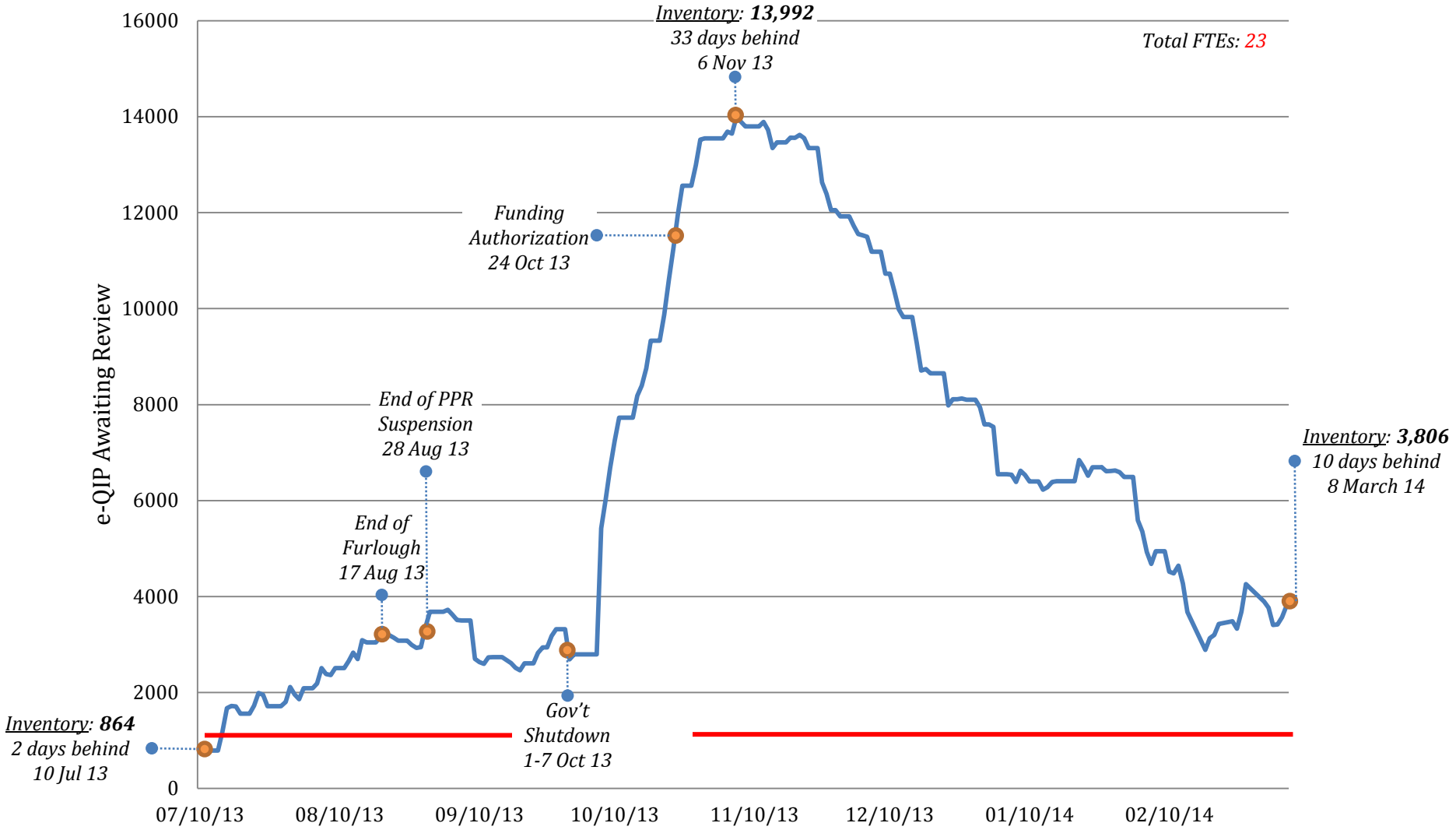
Attachment #5

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

2014

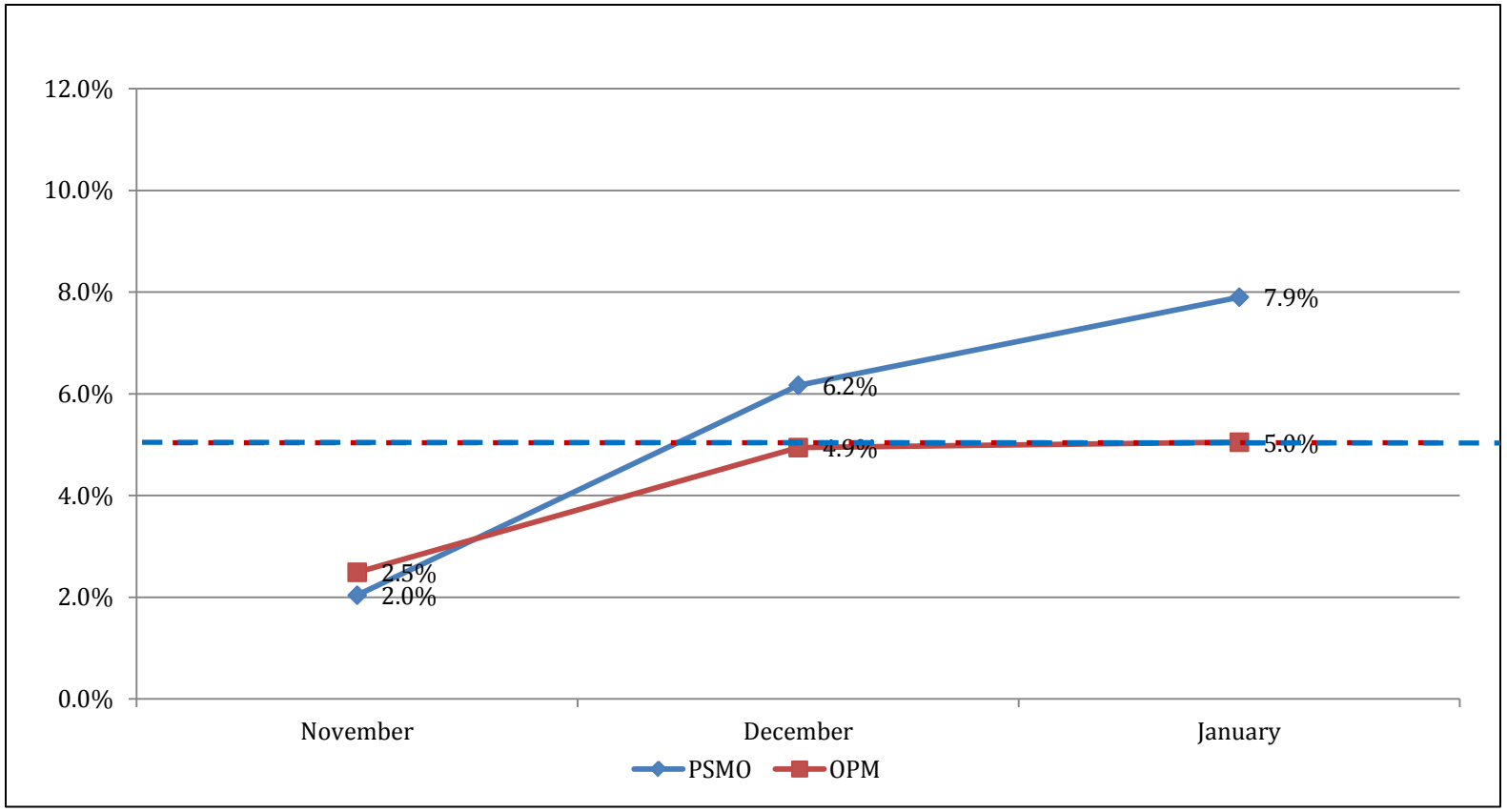
Presented by:
Chuck Tench

e-QIP Inventory Progress



e-QIP Rejection Rates – FY14

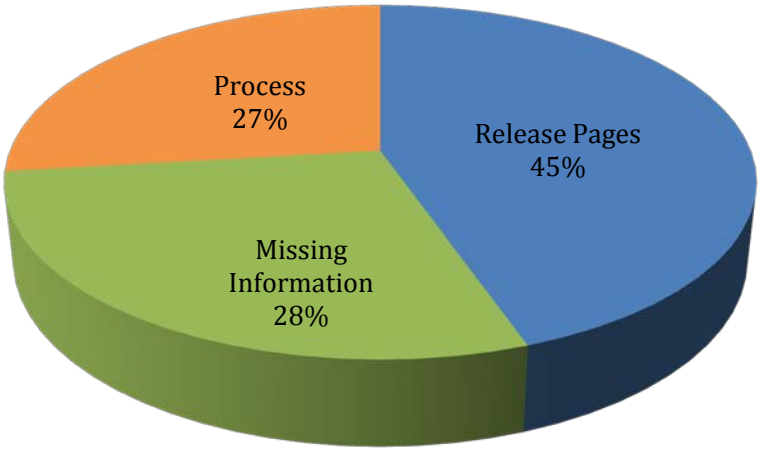
FY 14 PSMO and OPM Reject Rates
Initial and Periodic Reinvestigation Clearance Requests



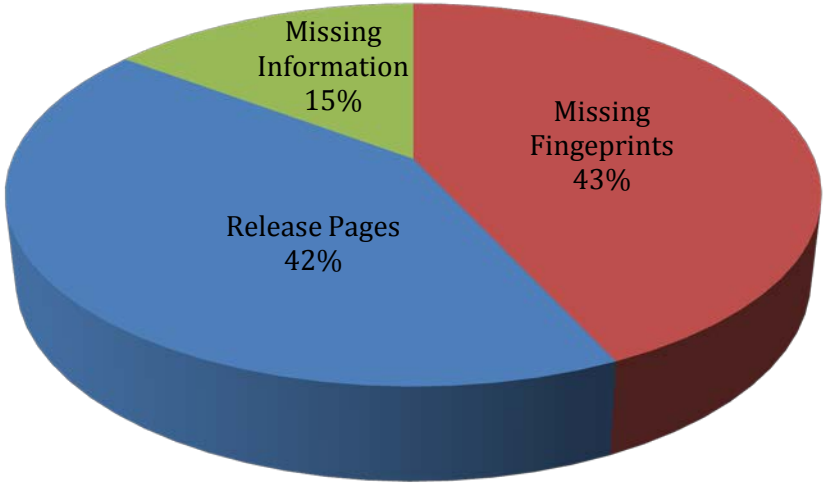
e-QIP Rejection Reasons – FY14

FY 14 PSMO and OPM Reject Reasons
Initial and Periodic Reinvestigation Clearance Requests

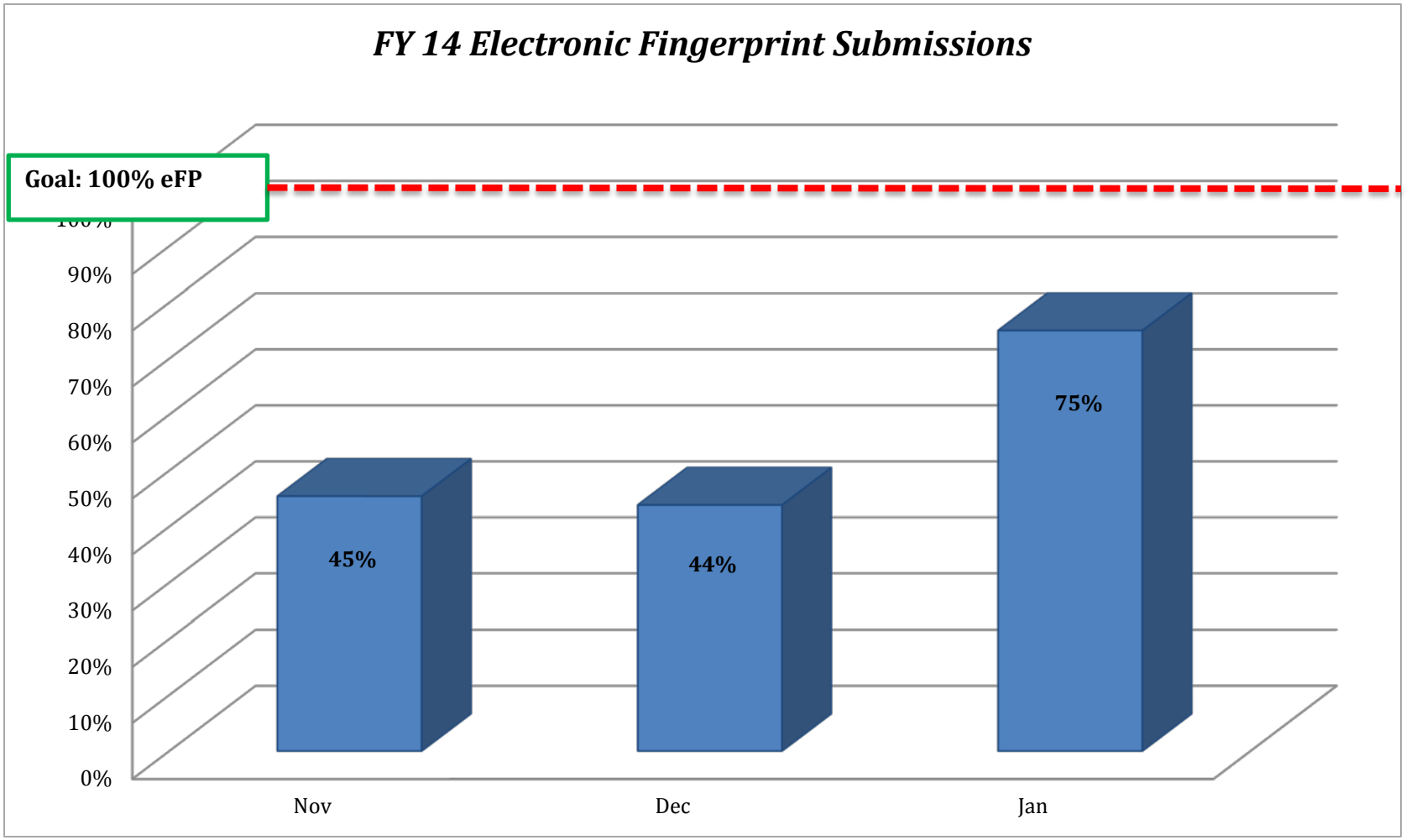
PSMO-I



OPM



eFP Submissions



New Interim Clearance Process

- **Interim Clearance Requirements:**
  - Review SF-86
  - Review National Databases
  - Investigation Scheduled
  - Review FP results
- **Status:**
  - OPM testing e-Delivery of the Advanced NAC with the SF-86
  - DISS PMO working on ingest of OPM product for e-Interim module
  - Next: DSS will dual test manual and automated solution
  - DSS may defer implementation of the favorable fingerprint result criteria for up to 30 days after DSS confirms that the OPM Advance NAC capability is fully functional
  - DSS will also notify contractors when implementation of the criteria for interim eligibility is to begin after confirming the functionality
- **Results:**
  - Interim PCL granted with increased confidence in trusted workforce
  - Reduced Risk

eFP Implementation Options

The **December 2013** deadline for implementing an eFP solution has **passed**. Please review the eFP Implementation Guide to figure out which option is best for your company.

http://www.dss.mil/documents/psmo-i/eFP_Guide_Feb_2014.pdf

Contacts

Email questions:
PSMO-I: AskPSMO-I@dss.mil
SWFT: dmdc.swft@mail.mil

eFP Setup & Submission

- FBI Product List
- FBI Approved Channeler List
- SWFT Approved List
- SWFT - Registration, Access and Testing Procedures
- DMDC-SWFT Homepage
- When submitting eFPs use:
  SOI: DD03
  SON: 346W
  IPAC: DSS-IND

Option 1
Company purchases eFP capture equipment and submits FPs through SWFT

Costs: one time equipment + maintenance

Option 2
Multiple companies share costs to purchase eFP capture equipment and submit FPs through SWFT

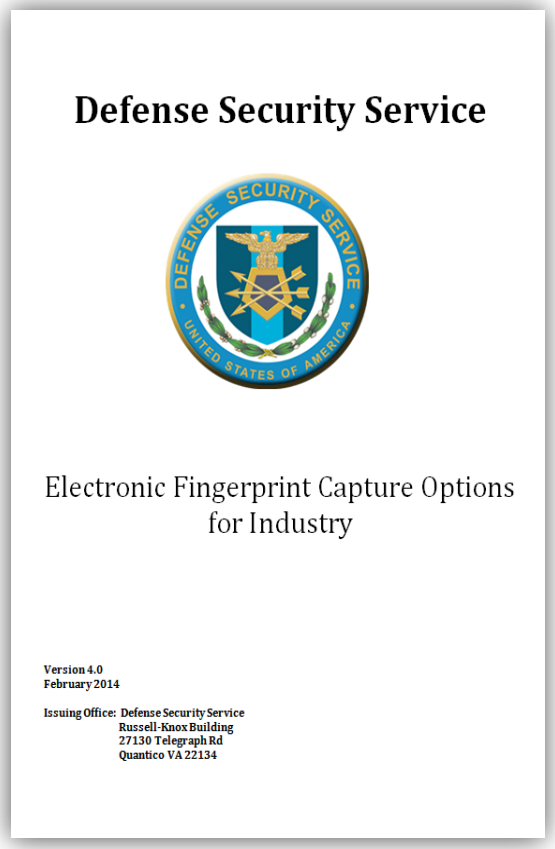
Costs: one time equipment + maintenance

Option 3
Cleared company submits eFPs through SWFT on behalf of other company

Costs: per transaction fee

Option 4
Third Party Vendor provides eFPs to cleared company to submit through SWFT

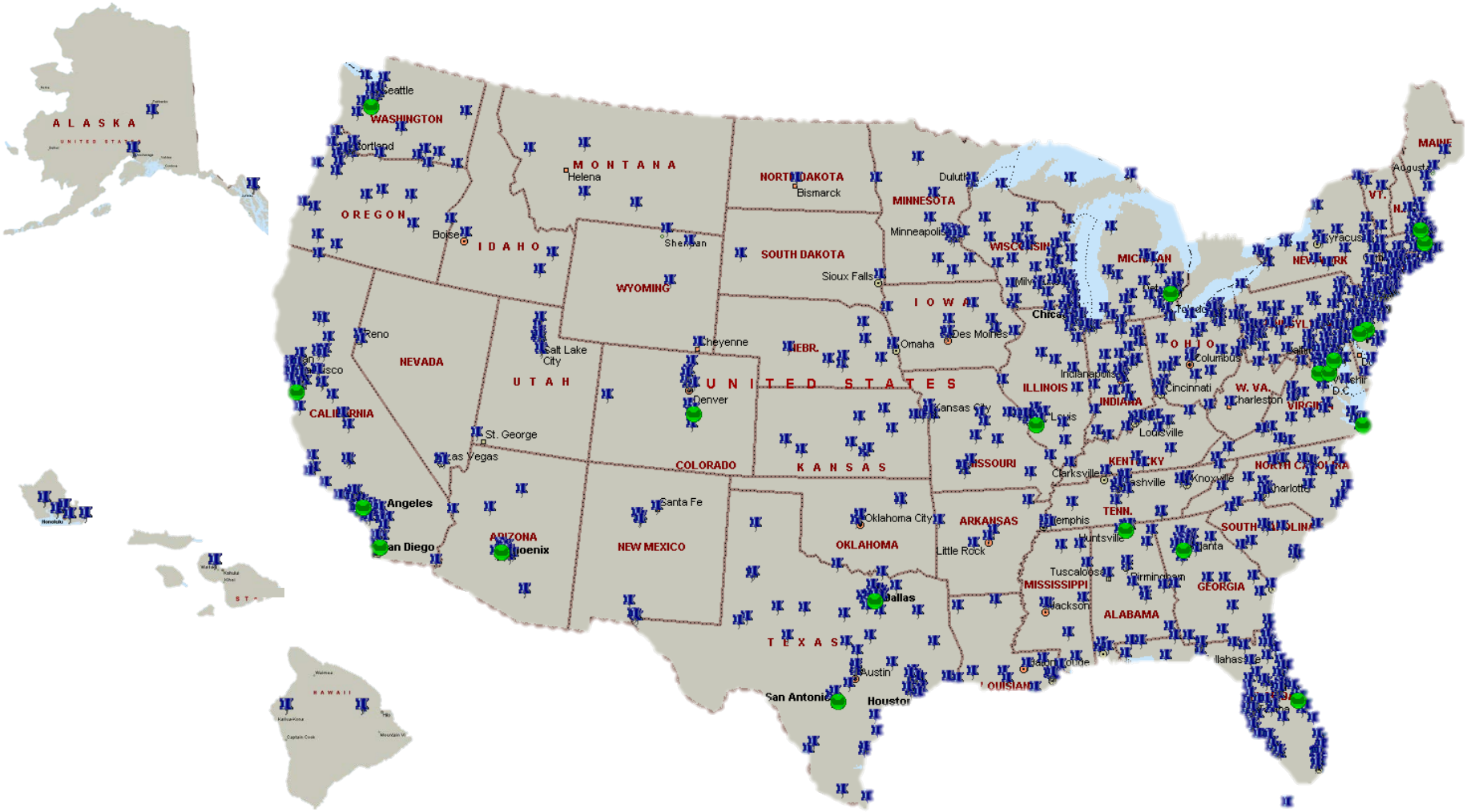
Costs: per transaction fee



Option 5
Government entity supports cleared company to submit eFPs to SWFT or OPM

Costs: none at this time, subject to availability

eFP Coverage Locations



Map Key

Electronic Fingerprint Capture Sites (1076)

DSS Field Office Locations (21) Note: The Field locations are not electronic fingerprint capture sites.

Channels of Communication

NISPPAC
INSA
DSS.mil
ISFD
DMDC PSA
DSS Call Center
Voice of Industry
NCMS Facebook
JPAS Website
ISAC
NCMS Meetings
DSS Webinar
DSS Facebook
ACCESS Magazine
DSS/IO Bulk email
AskPSMO-I Webinar
Briefings to Industry
DMDC Contact Center
JPAS PMO meetings
DSS Twitter
Triage Outreach Program
CDSE Webinar
CDSE Flash Email

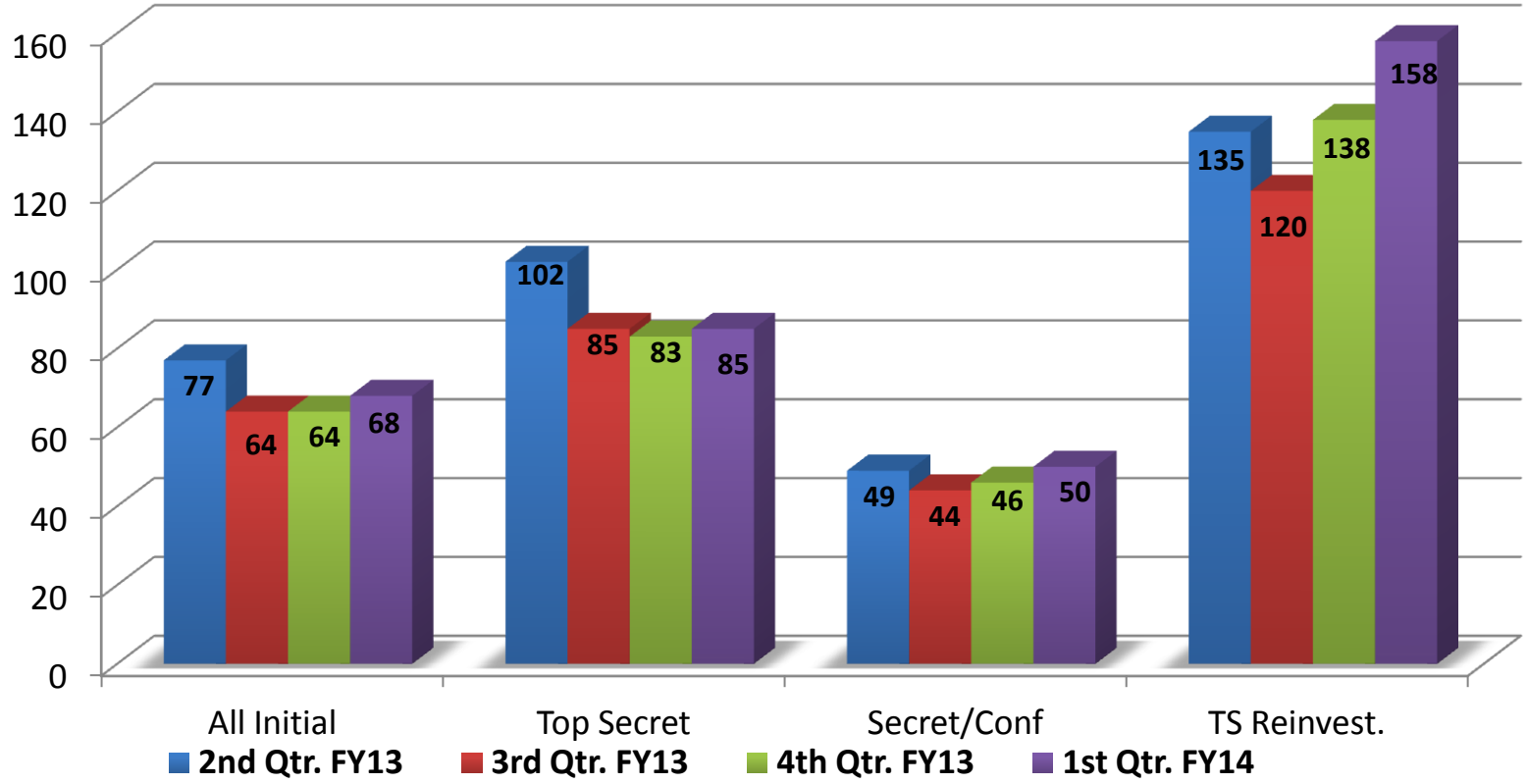
Attachment #6

a New Day for Federal Service

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

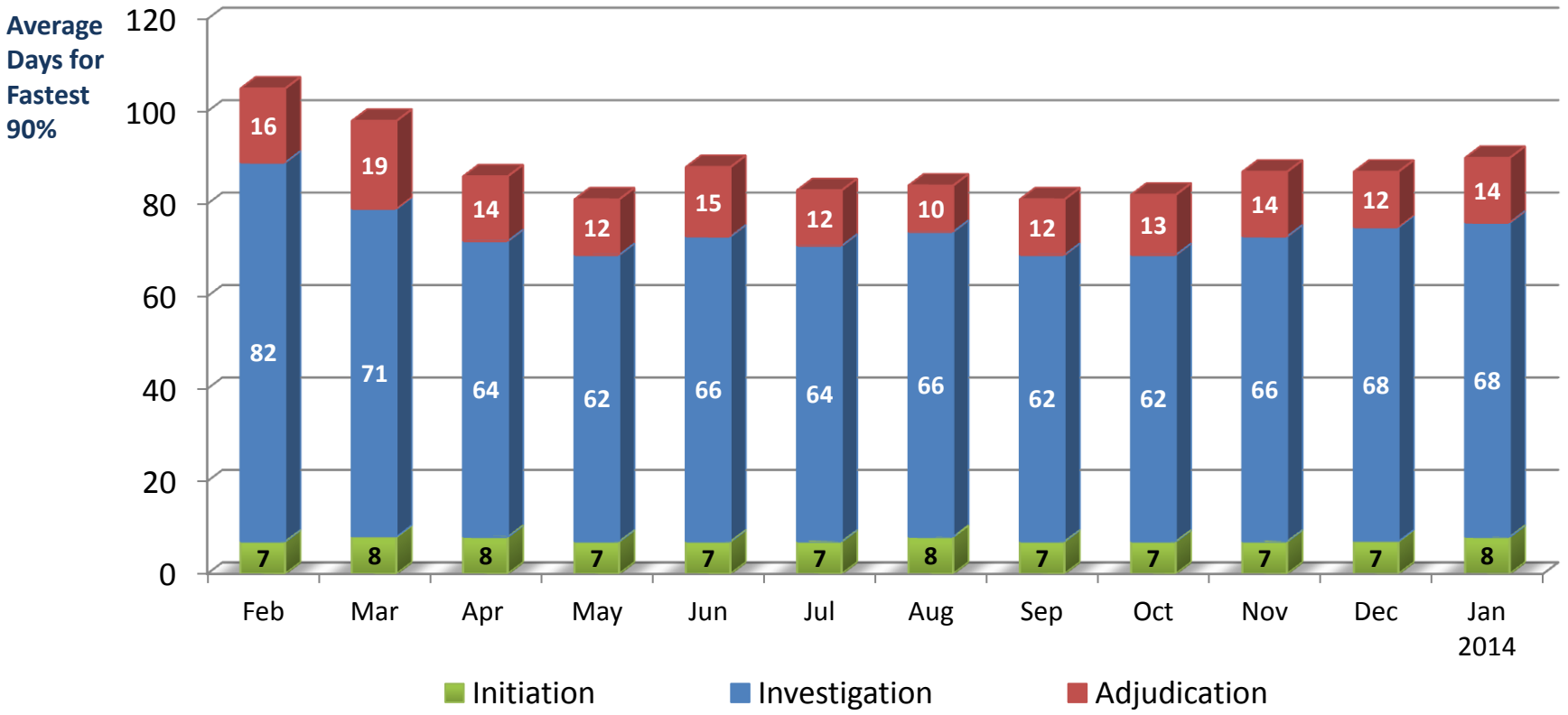
Timeliness Performance Metrics for DOE's Personnel Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 2nd Q FY13	1,679	914	765	1,971
Adjudication actions taken – 3rd Q FY13	1,896	979	917	2,961
Adjudication actions taken – 4th Q FY13	1,535	758	777	3,743
Adjudication actions taken – 1st Q FY14	1,412	773	639	2,774

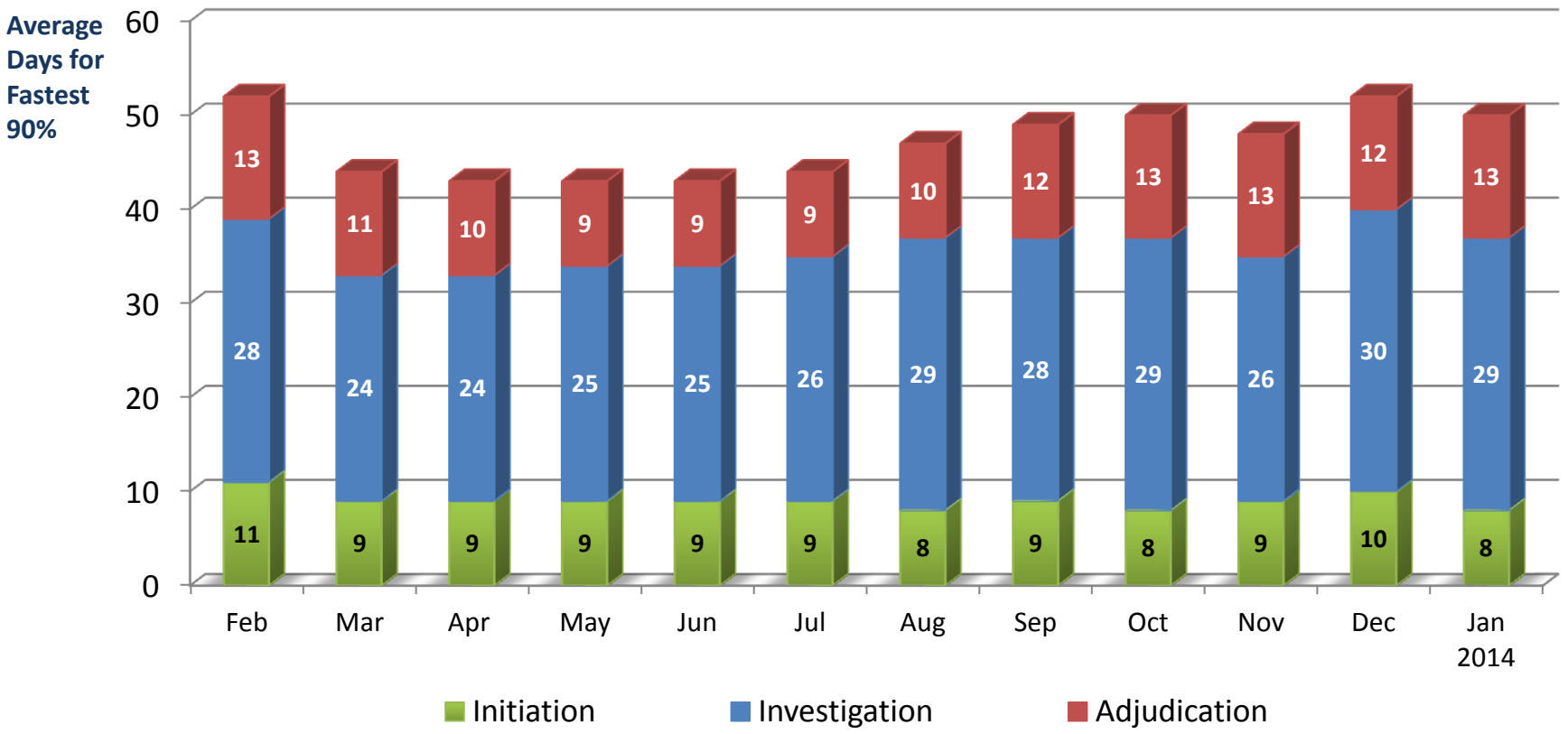
DOE's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



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

	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014
100% of Reported Adjudications	285	311	381	323	274	266	249	231	315	208	234	249
Average Days for fastest 90%	105 days	98 days	86 days	81 days	88 days	83 days	84 days	81 days	82 days	87 days	87 days	90 days

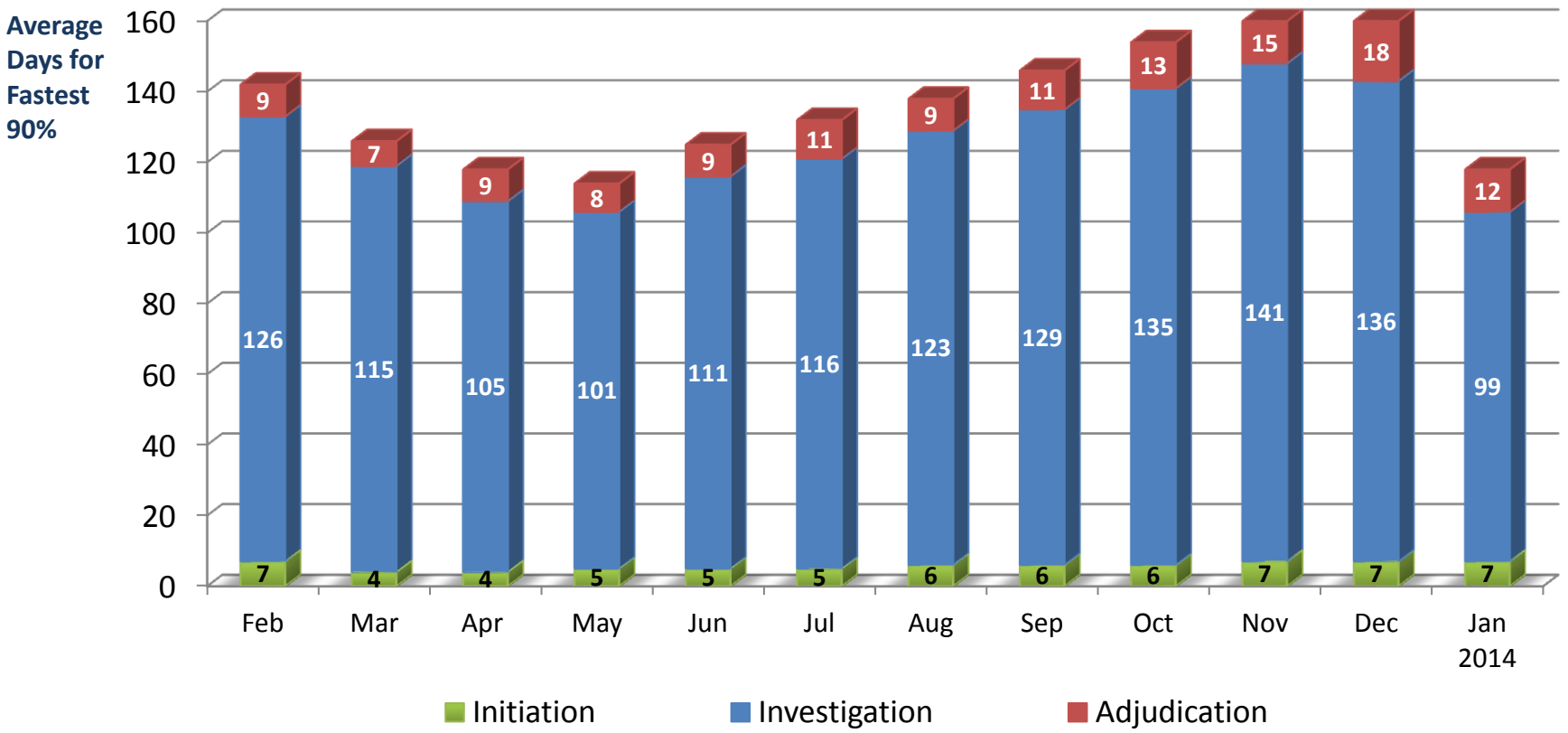
DOE's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



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

	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014
100% of Reported Adjudications	209	285	338	321	233	286	278	197	222	161	201	221
Average Days for fastest 90%	52 days	44 days	43 days	43 days	43 days	44 days	47 days	49 days	50 days	48 days	52 days	50 days

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



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

	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014
100% of Reported Adjudications	580	860	1,159	773	1,011	1,184	1,392	1,148	1,097	882	717	734
Average Days for fastest 90%	142 days	126 days	118 days	114 days	125 days	132 days	138 days	146 days	154 days	163 days	161 days	118 days

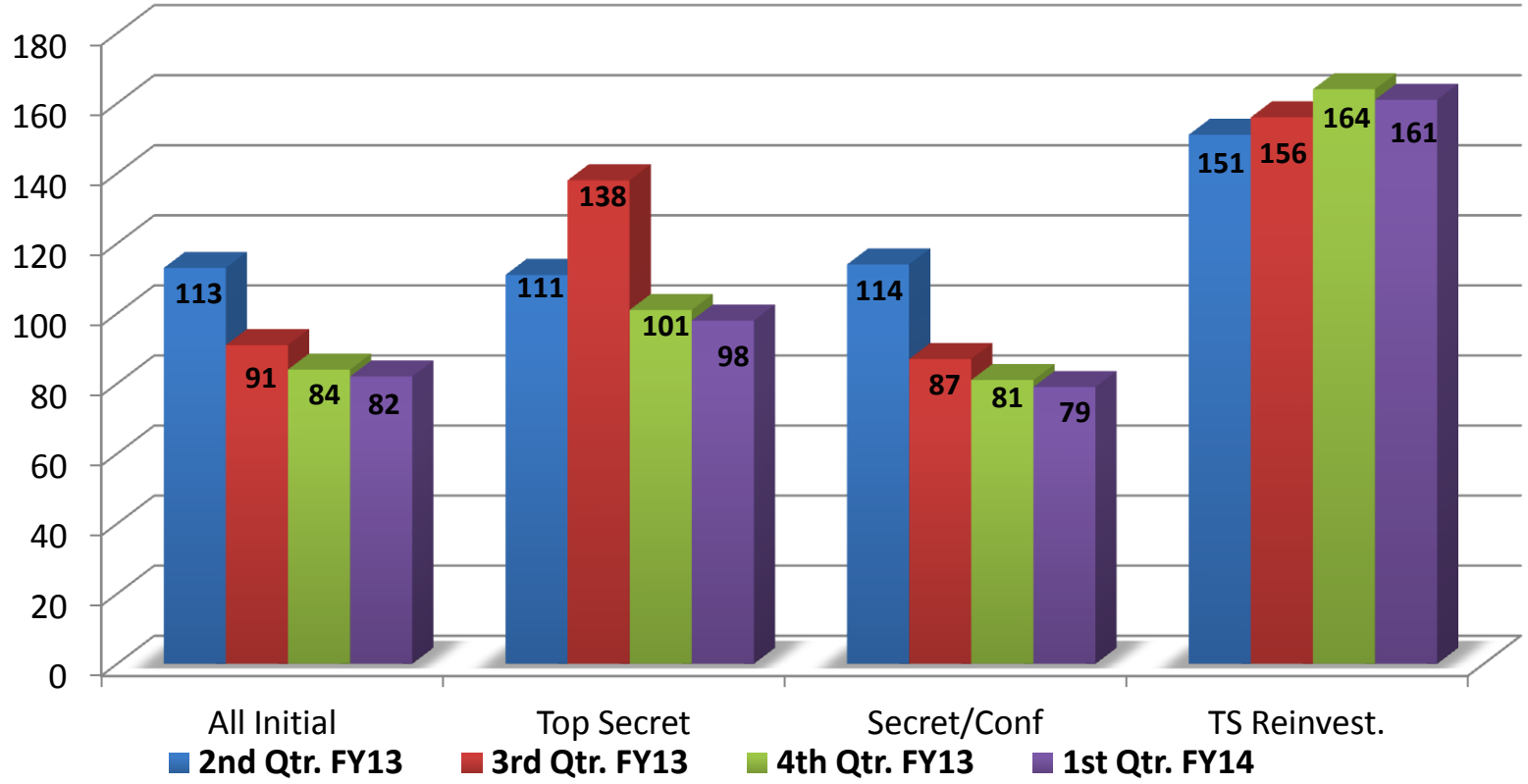
Attachment #7

a New Day for Federal Service

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

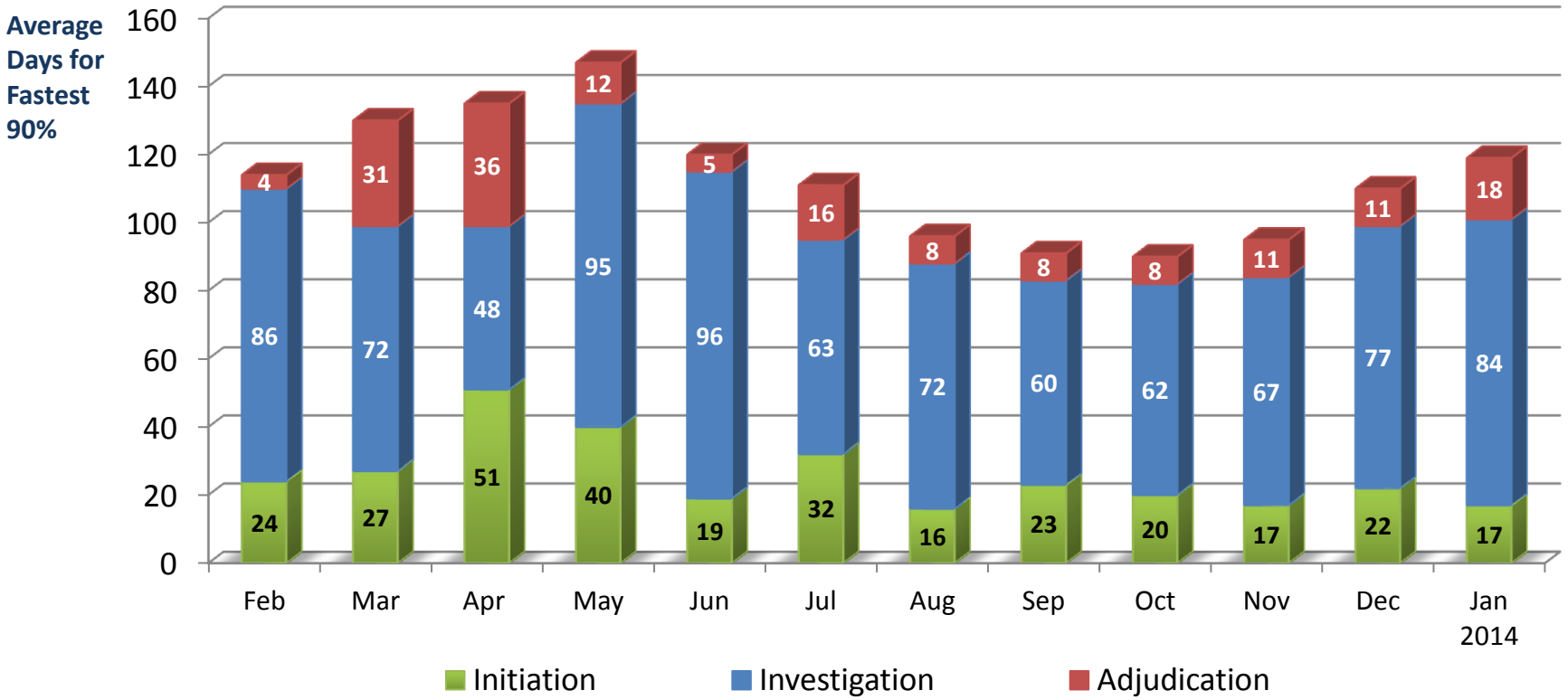
Timeliness Performance Metrics for NRC's Personnel Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 1st Q FY13	227	59	168	25
Adjudication actions taken – 2nd Q FY13	254	22	232	22
Adjudication actions taken – 3rd Q FY13	265	35	230	49
Adjudication actions taken – 1st Q FY14	169	28	141	98

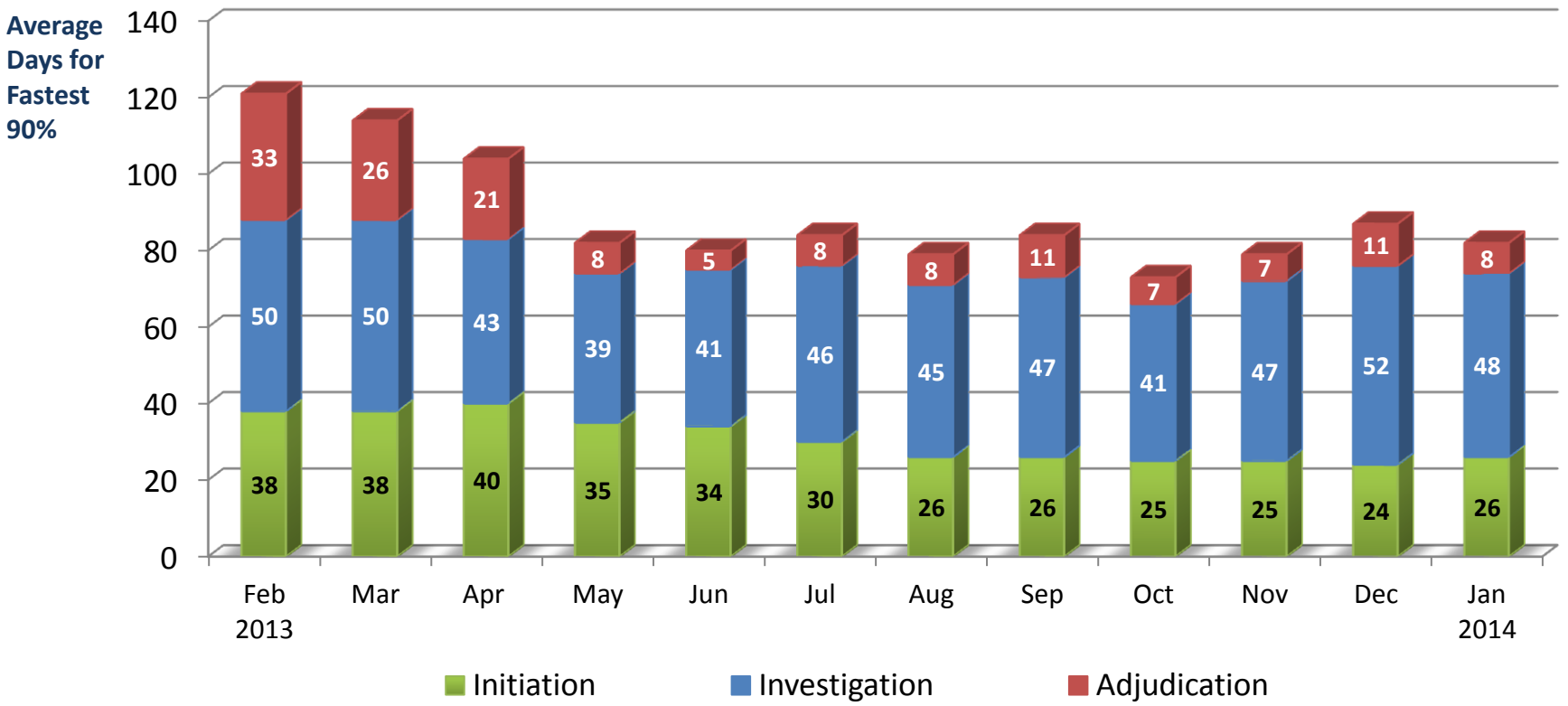
NRC's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



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

	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014
100% of Reported Adjudications	21	22	7	11	4	15	10	10	7	11	10	26
Average Days for fastest 90%	114 days	130 days	135 days	147 days	120 days	111 days	96 days	91 days	90 days	95 days	110 days	119 days

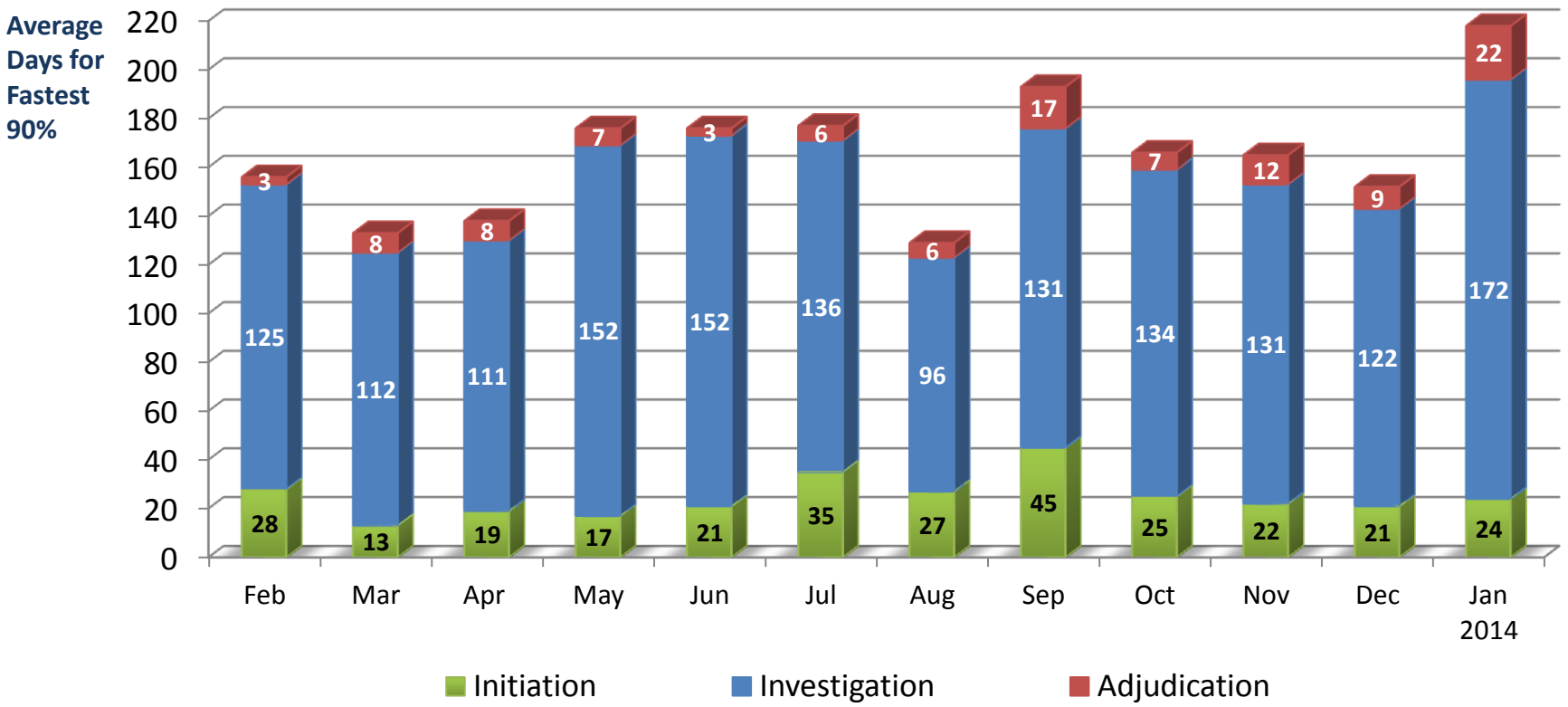
NRC's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



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

	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014
100% of Reported Adjudications	44	69	62	82	87	94	79	58	59	35	47	40
Average Days for fastest 90%	121 days	114 days	104 days	82 days	80 days	84 days	79 days	84 days	73 days	79 days	87 days	82 days

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



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

	Feb 2013	Mar 2013	Apr 2013	May 2013	Jun 2013	Jul 2013	Aug 2013	Sep 2013	Oct 2013	Nov 2013	Dec 2013	Jan 2014
100% of Reported Adjudications	8	11	11	4	7	14	17	18	40	27	31	17
Average Days for fastest 90%	156 days	133 days	138 days	176 days	176 days	177 days	129 days	193 days	166 days	165 days	152 days	218 days

Attachment #8

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

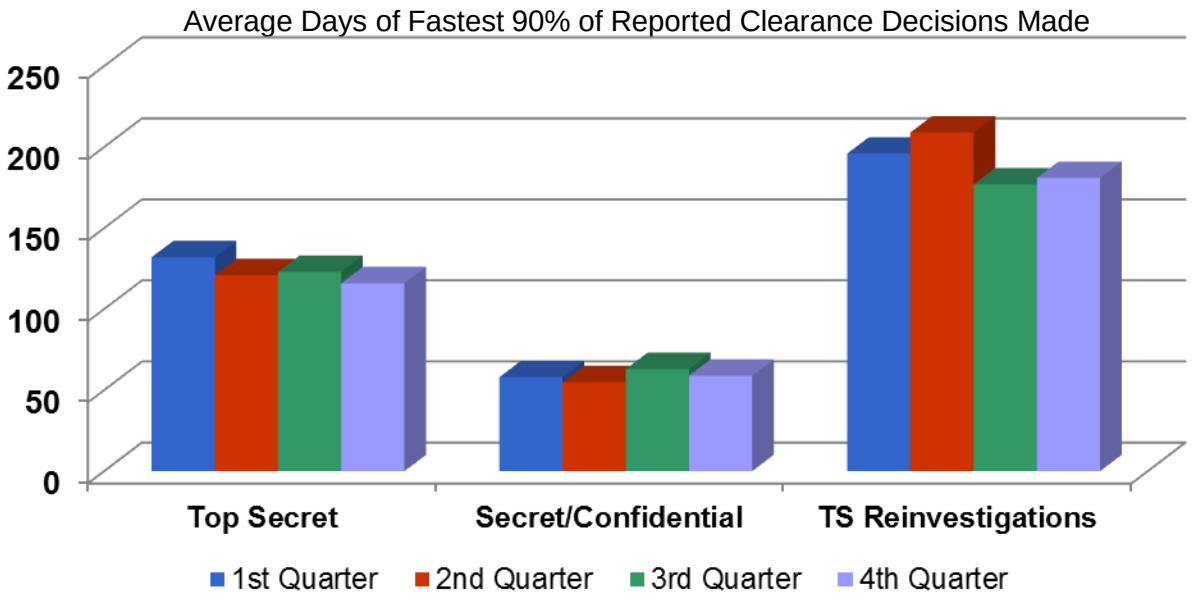
Industry Performance Metrics

ONCIX/Special Security Directorate

LEADING INTELLIGENCE INTEGRATION

NISPPAC Working Group
March 19, 2014

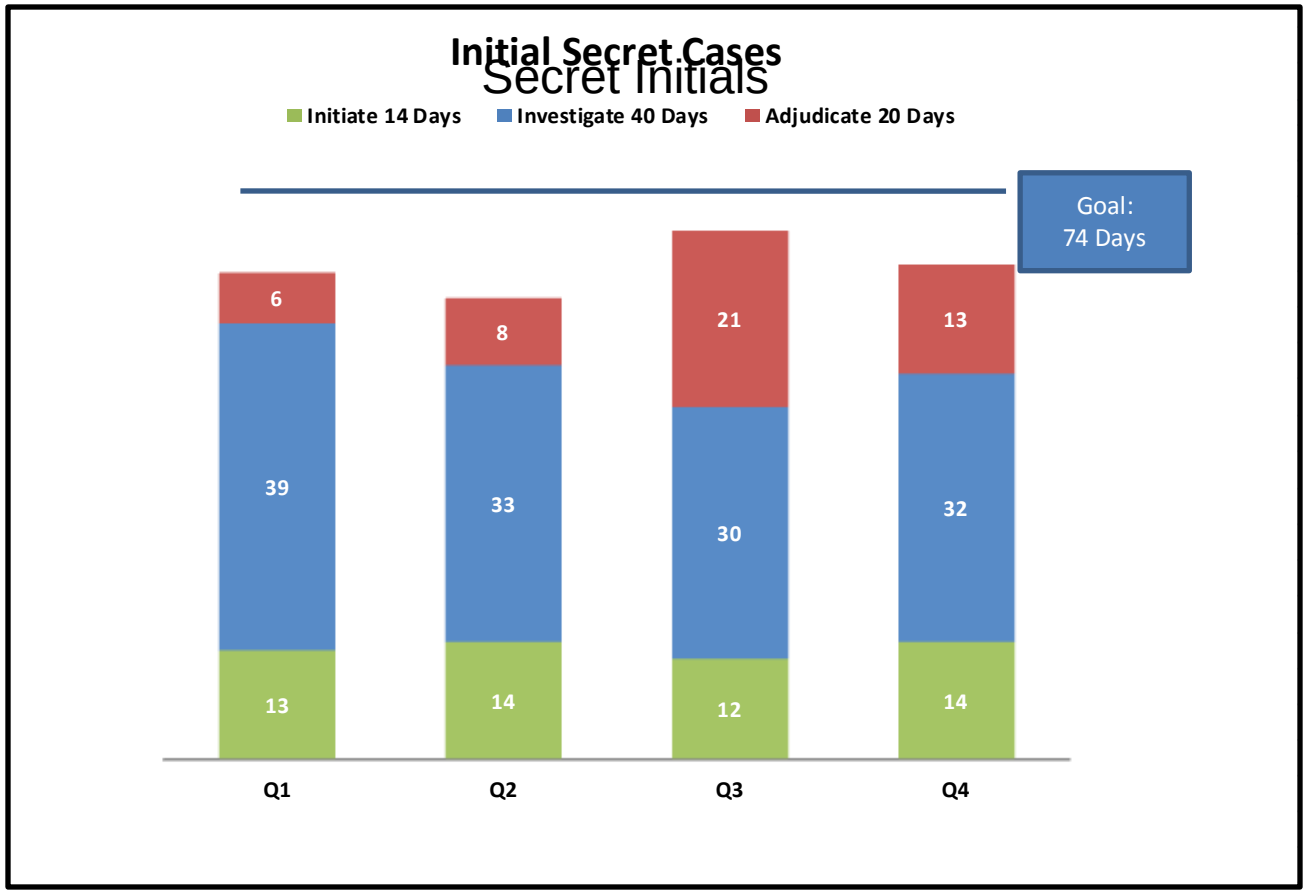
FY 2013 Timeliness Performance Metrics for IC / DSS Industry Personnel Submission, Investigation, and Adjudication* Time



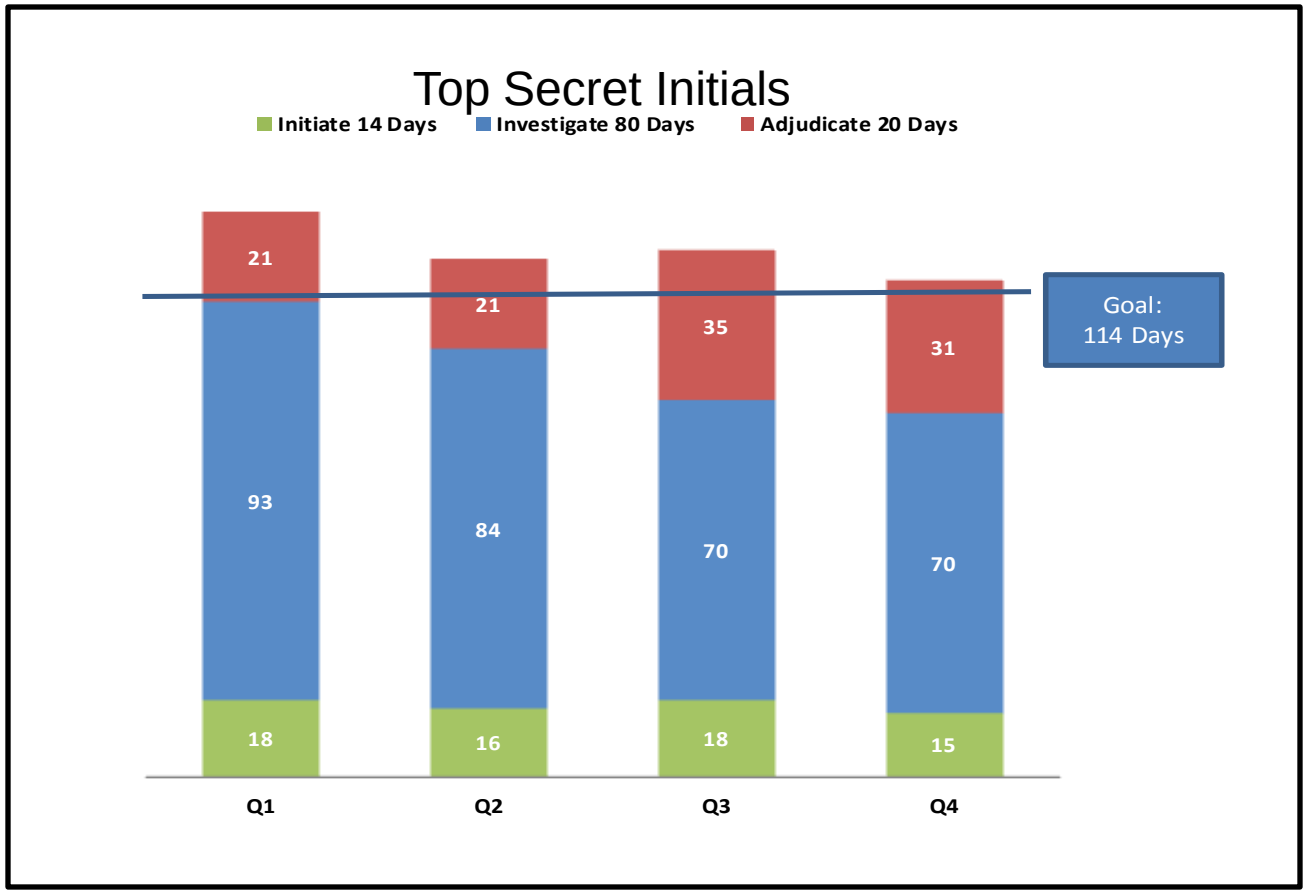
Adjudication Actions	Top Secret	Secret/Confidential	Top Secret Reinvestigations
Adjudication actions taken – 2nd Q FY13	10,330	21,029	13,080
Adjudication actions taken – 3rd Q FY13	8,883	20,981	12,385
Adjudication actions taken – 4th Q FY13	9,268	20,165	18,807

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

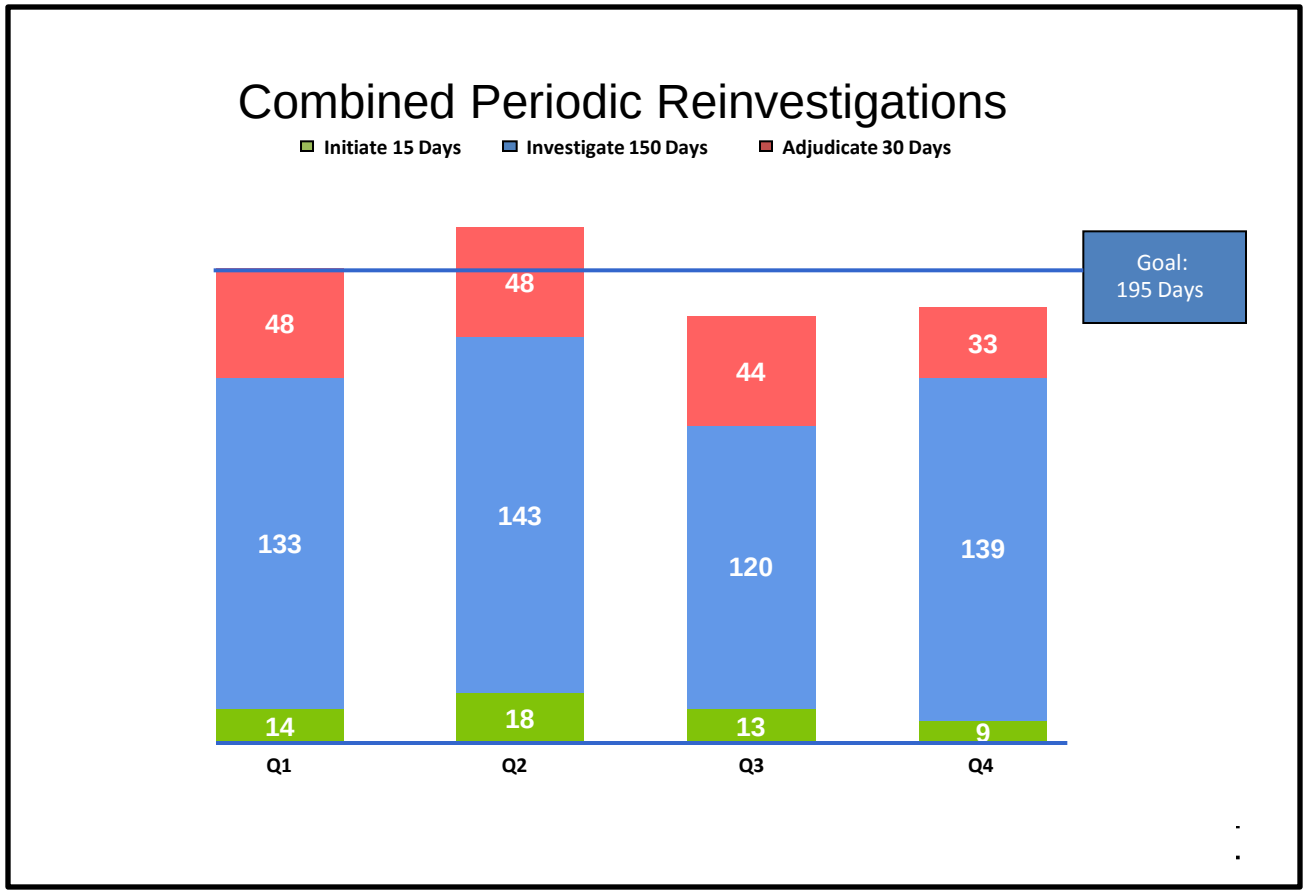
Roll-up IC and DoD Industry



Roll-up IC and DoD Industry

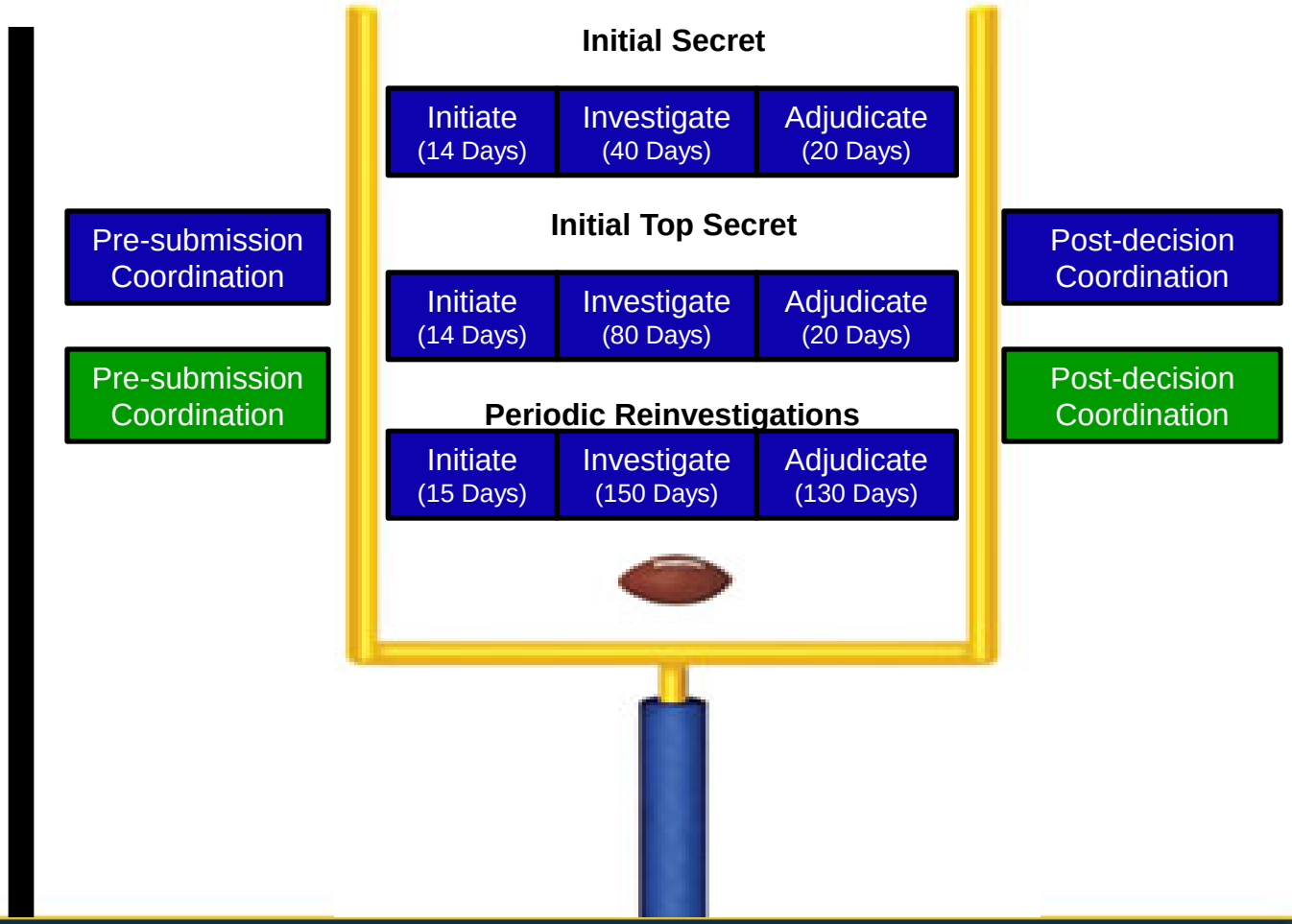


Roll-up IC and DoD Industry



PAC Security Clearance Methodology

- Timeliness data on the slides reflects USG performance on Contractor cases
- Timeliness data is 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



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

Attachment #9

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Continuous Evaluation
Informational Briefing

LEADING INTELLIGENCE INTEGRATION

Continuous Evaluation (CE) Authorities

Executive Order 13467: CE is defined as "reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility."

Executive Order 12968 (as amended by EO 13467): States that any individual who has been determined to be eligible for or who currently has access to classified information shall be subject to continuous evaluation under standards (including, but not limited to, the frequency of such evaluation) as determined by the DNI.

Federal Investigative Standards (Signed by the DNI December 2012): Requires that a continuous evaluation program be in place for all individuals cleared to Tier 5 (individuals eligible for access to TS or TS/SCI information, or eligible to hold a sensitive position). Tier 5 implementation is scheduled for September 2016.

Bridging the Security Gap

INITIAL

CE

- Enhanced Security
- Managed Risks
- Workforce Mobility
- Shortened PR Timeframes
- Promotes Reciprocity

PR

INITIAL INVESTIGATION	CONTINUOUS EVALUATION	PERIODIC REINVESTIGATION
Year 0	**Years 0-5**	**Year 5**
Information from Initial used for CE	Individual is evaluated for continued eligibility	Information from CE used for PR
INITIAL 	CE 	PR 

CE Implementation Strategy

- Develop a government-wide solution – includes military and civilian, government employee and contractor
- Implementation phased in over the next three years
- Start small with the highest risk population
- Expand the program to include more data and more agencies
- CE data follows individual as they move from job to job
- Goal to provide a more secure workforce and enhance reciprocity

Questions?

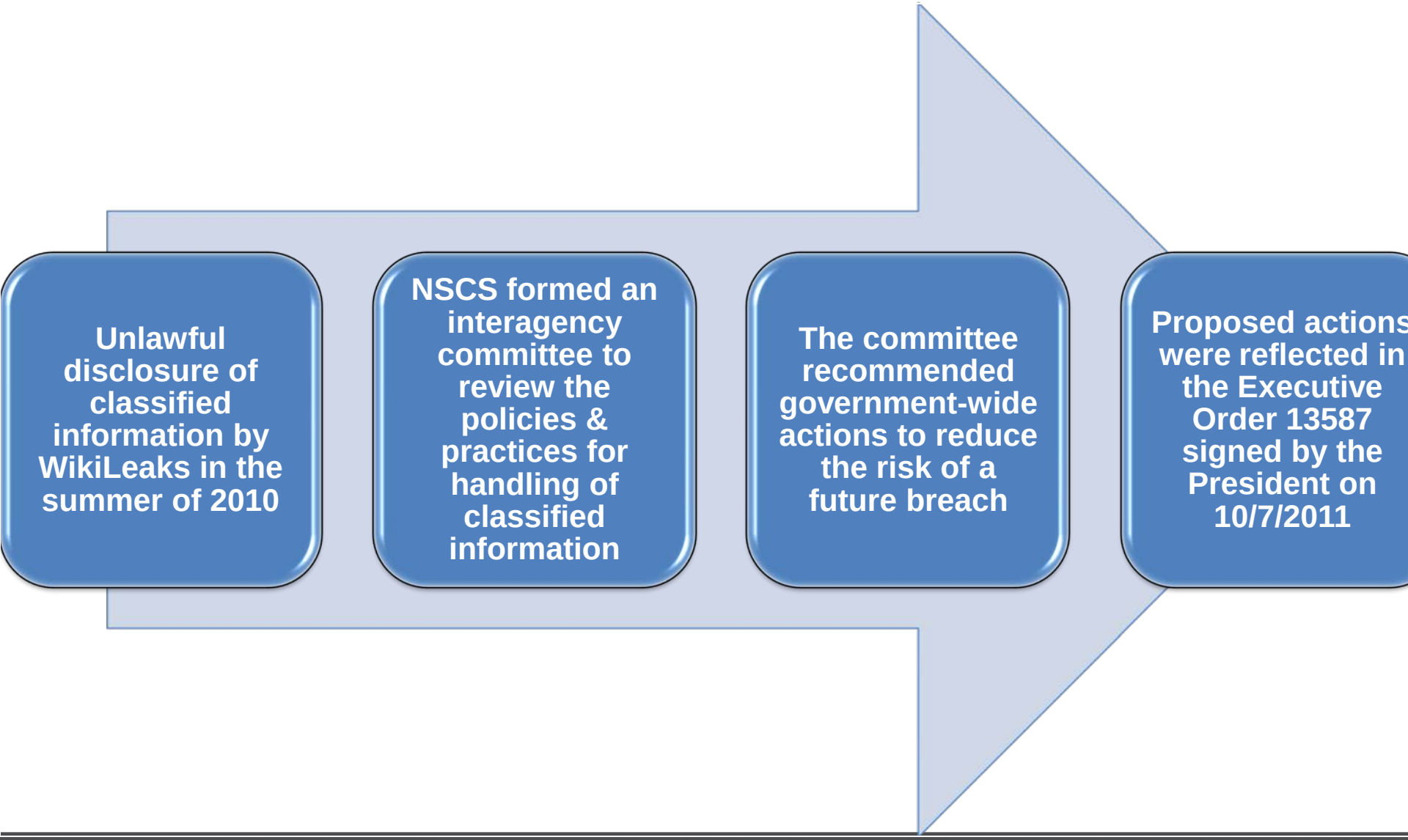
Attachment #10

EO 13587 Update

Ray Sexton

Classified Information Sharing and Safeguarding Office

Background


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

Areas of Focus & Ongoing Improvement

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

Changes for FY 14

Control of removable media – **move to maintenance mode**

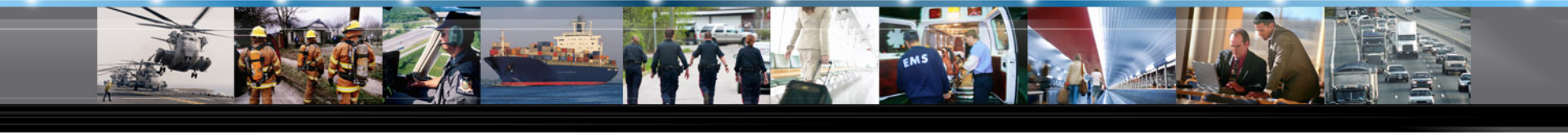
Identity Management – **"front runner" to be named top Steering Committee priority**

Continuous Monitoring and Diagnostics (CDM) added as sixth priority

Since Last Summer

- **45 Day Report to POTUS.**
- **J15 CAP objectives**
- **Tab A White House Tasking**
- **120 Day Review of Security Clearances and Suitability**
- **Safeguarding Reporting Streamlining**

Questions?



Attachment #11

Controlled Unclassified Information

Executive Order 13556

Shared • Standardized • Transparent

CONTROLLED
UNCLASSIFIED
INFORMATION

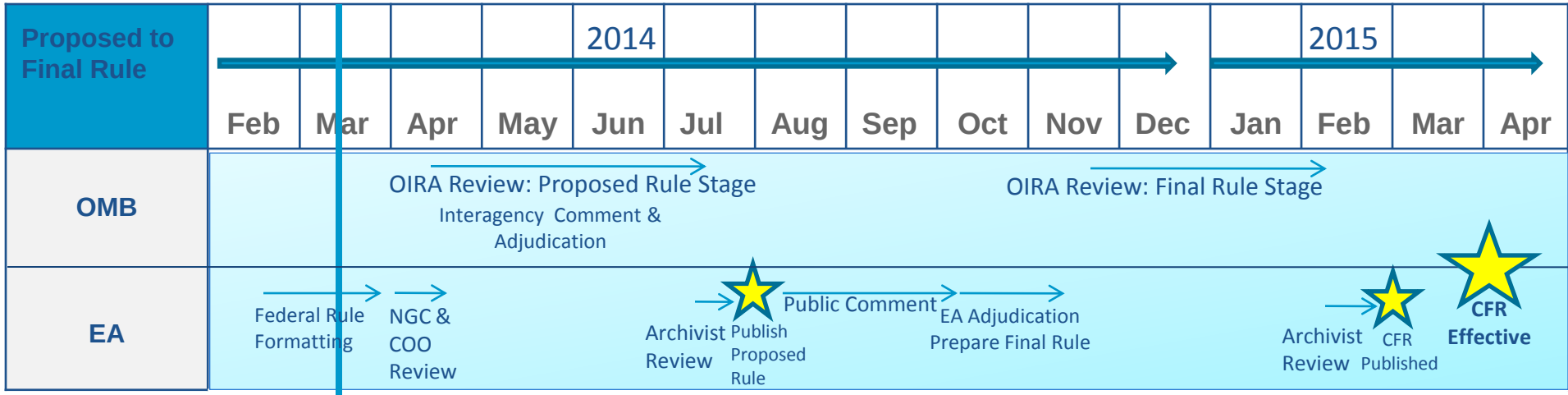
Information Security Oversight Office (ISOO)

Agenda

- Policy Status
- Supplemental Guidance Status
- Phased Implementation

Projected CUI Policy Timeline

as of 12 March 2014



Supplemental Guidance Status

Guidance:	Format:	Council Action:	Status:
Marking	Marking Handbook	-**Comment by Council:** January 2014 -**Final Version to Council: 31** March 2014 -**Published:** Day 0	
Coversheets	Coversheets	-**Comment by Council:** January 2014 -**Final Version to Council: 31** March 2014 -**Published:** Day 0	
Safeguarding: Storage, Discussion/Telephonic, Reproduction, Destruction, Transportation, Transmission, Remote Access, Internet/Intranet	Additional ISOO Issuance	**-Comment by Council:** February 2014 **-Final Version to Council: 31** March 2014 **-Published:** Day 0	
Misuse	Additional ISOO Issuance	**-Comment by Council:** February 2014 **-Final Version to Council: 31** March 2014 **-Published:** Day 0	
Dissemination	Additional ISOO Issuance	**-Comment by Council:** February 2014 **-Final Version to Council: 31** March 2014 **-Published:** Day 0	
Decontrol	Additional ISOO Issuance	**-Comment by Council:** February 2014 **-Final Version to Council: 31** March 2014 **-Published:** Day 0	

Note: OMB/OIRA informed the EA that the draft versions of supplemental guidance (marking, safeguarding, dissemination, misuse, and decontrol) must accompany the proposed CUI rule when submitted. The EA is planning on submitting the CUI rule and all supplemental guidance to OMB/OIRA by 31 March 2014.

Revised Phased Implementation: Notional Timeline

	Planning	Readiness	Initiation	Final
Phases	Identify and initiate planning activities for CUI implementation	Prepare environment and workforce for the CUI transition	Begin implementation of CUI practices Begin Phase Out of obsolete practices	Full Implementation of the CUI program
Key D/A Activities	• **Develop & Publish Policy*** • Develop Training • Consider Agency's CUI Investment Process • Develop IT Transition Plan • Develop Self-Inspection Plan • Develop process for internal non-compliance	• **Assert Physical Safeguarding*** • **Conduct Training*** • Initiate Awareness • Prepare IT Transition • Prepare Agency's Investment Process	• Initiate CUI Implementation **IOC** • Handle • Recognize • Receive • Initiate IT Transition • Permit Creation of CUI • Initiate Self-Inspection Program	• Eliminate Old Markings • Assure use of only New Markings • Complete IT Transition • Monitor & Report Implementation **FOC**

***Required for IOC**

Attachment #12

Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

Program Overview

17 March 2014

Mission Statement

Provide the DoD with a security center of excellence for the professionalization of the security community and be the premier provider of security education and training for the DoD and industry under the National Industrial Security Program (NISP). The CDSE provides development, delivery, and exchange of security knowledge to ensure a high-performing workforce capable of addressing our Nation's security challenges.

Center for Development of Security Excellence

A nationally recognized, accredited, and award winning organization supporting security workforce professionalization

CDSE
Center for Development of Security Excellence
Learn. Perform. Protect.

Professionalization of Security Enterprise

- Education – developing future security leaders
- Training – supporting today's security practitioners
- Certification – validating security professional achievement of skills and competencies

Supports

- DoD Functional Community Manager for Security Education, Training, and Certification
- Responsibilities Outlined in:
  - DoDD 5105.42
  - DoDI 3305.13
  - DoDM 3305.13-M
- Defense Intelligence Enterprise Human Capital Strategic Plan
- ICD 610
- DoD Security Skill Standards (DS3)

Audience

- DoD civilian and military personnel
- Industry
- Other U.S. Government personnel
- Employees of Foreign Governments

Products and Services

- eLearning Courses
- Instructor-led Courses
- Asynchronous Collaborative Learning
- Webinars
- Toolkits
- Shorts (Security Short Format Learning)
- Job Aids
- SPēD Certification Program

IACET The Standard for Lifelong Learning

COE Council on Occupational Education

ACE CREDIT American Council on Education College Credit Recommendation Service

NCCA

ICE Institute for Credentialing Excellence

Education

- **Security Education Program**
  - Collegiate-level security courses
    - Designed specifically to develop leaders for the DoD security community
    - Highly qualified SME Instructors
    - Delivered online using a collaborative learning environment
    - ACE credit recommendations allow students to transfer credit
  - Seventeen Courses in Curriculum

Training

- **Training Areas**
  - 4 Core Security Disciplines
    - Information
    - Physical
    - Industrial
    - Personnel
  - Specialty Areas
  - General Security
  - Facilitated Programs

- **Training Products & Services**
  - Instructor-led
  - eLearning
  - “Short” Format Learning
  - Webinars
  - Virtual Simulations
  - Instructor Facilitated Online Training
  - Performance Support Tools
  - Toolkits

Professionalization

- **SPēD Certification Program**
  - Skill standards-job competencies
  - Certification Programs
    - Security Fundamentals Professional Certification (SFPC) **
    - Security Asset Protection Professional Certification (SAPPC) **
    - Security Program Integration Professional Certification (SPIPC)
    - Specialty Certifications and Credential
      - Adjudicator Professional Certification (APC)
      - Due Process Adjudicator Professional Credential (DPAPC)
      - Physical Security Certification (PSC)
      - Industrial Security Oversight Certification (ISOC)
      - Special Programs Security Certification (SPSC)

** Nationally Accredited by NCCA

Recent Successes

- Achieved first two national accreditations of federal government-developed certification
- Attained status as a continuing education and training provider, with ability to transfer credits for some courses to participating colleges and universities
- Received over 30 awards for security training courses and products since 2009

Questions?