Minutes of the November 18, 2015 Meeting of the National Industrial Security Program Policy Advisory Committee (NISPPAC)

The NISPPAC held its 52nd meeting on Wednesday, November 18, 2015, 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), served as Chair. The minutes of this meeting were certified on December 14, 2015.

I. Welcome and Administrative Matters:

Mr. Fitzpatrick welcomed the attendees, and after introductions, reminded everyone that NISPPAC meetings are recorded events. He then welcomed back new industry guests and friends of NISPPAC David Best, lately of ISOO, and Steve Lewis, lately of the Office of the Undersecretary of Defense for Intelligence (OUSD(I)) and pointed out that in this way we encourage strong ties between government and industry. He also recognized the two newest NISPPAC industry representatives Quinton Wilkes and Dennis Keith, who are beginning their terms today and again thanked former members Steve Kipp and Rick Graham for their loyal service which had concluded on September 30, 2015. He stated that there would be a public comment period at the end of the meeting, and reminded everyone that the minutes from the July 15th meeting are provided in the information packets, as well as the presentations for today's meeting, and noted that there were no action items from the last meeting. 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 attendees.)

II. Old Business:

Mr. Pannoni noted that the NISPPAC charter has now been renewed, and with that, the president has extended the existence of the committee to September 30, 2017. In addition, since we are recounting charter renewal, we pause for some Committee reminders that we are asked to provide in behalf of our responsibilities under the Federal Advisory Committee Act. First, with respect to non-government members, we remind all that you represent, from the smallest legal, one-person, one classified contract entity, to the largest, multi-classified contracts U.S. corporations. Also, that non-government members collectively possess considerable, valuable expertise in the primary focus areas of the NISP, including information security, personnel security, physical security, and information systems security. He then extended his welcome to Misters Wilkes and Keith, and thanked Tony Ingenito, the NISPPAC's Combined Industry Representative, for his helpful assistance in the nomination process. (See attachment 2 for the meeting's action item.)

III. Reports and Updates:

(A) Office of Personnel Management (OPM) Updates:

The Chair initiated the updates with a discussion of the recent OPM data breach, explaining that we have tried to use the NISPPAC partnership as a means of insuring the effective communication of information about the circumstances and responses to the various data breaches to make sure that our industry partners are aware of the government's efforts and the next steps that they should expect. He pointed out that we had covered the breach in depth at our July meeting, and while there is not a lot of new news, he asked that Lisa Loss, OPM, update the Committee with regard to breach notifications. Ms. Loss announced that notifications are being mailed to affected individuals, and that although she did not have up-to-date numbers, it was her understanding that as of last week more than seven million individual notifications have been mailed. In addition, in the coming weeks she posited that we will see a greater emphasis on mailings to industrial personnel, due to the progress we have made with the Department of Defense (DoD) in acquiring updated address information. Further, she suggested that if you have not yet received a notification, and you expect to, please bear with us, as within the next few weeks you should receive it, providing we have an accurate and current address. Also, understanding that that may not always be possible, DoD, which is partnering with OPM in the notifications process, is setting up a verification center that should be active by the beginning of December 2015. This center will exist so that people can call the number provided and find out if they were personally affected by the breach but have not yet received a notification. Finally, she noted that OPM will be reaching out to both industry and government partners to provide additional information about this new notification center, and she expects some forthcoming calls to industry, industry groups, and other partners within a few days of the Thanksgiving holiday. The Chair then called for the DoD updates.

(B) DoD Updates:

Laura Hickman, DoD, began the updates by noting that Conforming Change #2 to the National Industrial Security Program Operating Manual (NISPOM) has completed the initial review process and is currently in legal sufficiency review, and that as soon as it clears we will expedite all remaining actions for its approval and publication. She expects that process to be completed very soon. She explained that once it is published, industry will have six months to comply with its provisions. However, she encouraged all not to wait for final publication, but rather to start implementing the forthcoming changes by selecting a senior insider threat management official, and that beyond that, she reminded all that the Defense Security Service (DSS) website contains comprehensive information on other preparatory steps that industry should take. Also, she noted that for all contractors that are under DoD cognizance there will soon be an Industry Security Letter (ISL) issued that will provide additional guidance. She then updated the progress on the DoD Form 254, Contract Security Classification Specification automation process, stating that they expect the Federal Register notification's 60-day comment period to begin soon, and that at that time they will notify DSS, who will in turn notify NISPPAC. Finally, she noted that they are preparing to begin a new December 2015 program that will represent the second round in the Continuous Evaluation (CE) process. She reminded everyone that the initial phase had a population size of 100,000, but that in the second phase they will ramp up to approximately 225,000 cleared DoD individuals, approximately 25% of whom will be industry. Thus, we can anticipate about 50,000 personnel engaged in the CE program, and that as soon as this phase is initiated, we will begin receiving results from DSS's Personnel Security Management Office for Industry (PSMO-I).

(C) Defense Security Service (DSS) Updates:

Stan Sims, DSS, opened with an update from the government and industry stakeholders meetings which had occurred two days prior to this NISPPAC meeting. He noted that they too had additional discussions on the OPM breach, and thanked Ms. Loss for her thorough update. He explained that they had provided an update on the Tier 3 Implementation of the Federal Investigative Standards (FIS) as regards industry and pointed out that Chuck Tench and PSMO-I personnel have been working with industry to ensure as smooth and seamless a transition as is possible. Then, he updated the Periodic Reinvestigations (PR) process, explaining that given the recent Electronic Questionnaires for Investigations Processing delay there has been an increase in the backlog, but that they were doing everything possible to quickly return to normalcy, and that there had been an excellent dialogue through which everyone understood what the changes are going to be. He reminded all that if they have additional questions they can either consult the website or the PSMO-I team. He then explained the work that DSS and the Defense Manpower Data Center (DMDC) are doing to improve efficiency through creation of an electronic signing procedure that will soon reach completion. He noted that the process will ultimately save millions of pages as well as perhaps eighteen investigative man-years, thus ensuring a significant reduction in processing timeliness. He then discussed the update of the National Industrial Security System (NISS), for which a contract was recently awarded, stating that we are therefore in development of a new system which will ensure that industry partners are efficiently working on classified contracts through a single, unified system. He stated that they expect the system to come online within 15 to 18 months, and that they will require industry personnel to help test it prior to process automation and deployment. He described ongoing discussions regarding insider threat processes once Conforming Change #2 is complete, and especially with regard to the 180-day implementation process and future expectations for the protection of property, infrastructure, data, and national security. Finally, he spoke in greater detail of the forthcoming ISL previously introduced by Ms. Hickman. He explained that they had decided to employ some industrial partners in the development process prior to submission for OUSD(I) approval, and that this had proven to be the right business approach. The Chair then called for the combined industry presentation updates.

(D) Combined Industry Presentation Updates:

Mr. Ingenito, Industry, began (see attachment 3) by welcoming Misters Wilkes and Keith to the NISPPAC team and announcing the additions of Brian Mackey of the Contractor Special Security Working Group and Mark Ryan of the Industrial Security Working Group to the Memorandum of Understanding membership. He then responded briefly to the discussions regarding the OPM breach by reaffirming industry’s appreciation for the government’s continuous leadership, sharing, and ongoing dialogue with the industrial membership. He then reaffirmed industry’s expectation that there would be continued increases in the clearance backlog, as well as significant delays in Sensitive Compartmented Information (SCI) and Special Access Programs (SAP) processes that will ultimately cause a growing number of personnel to fall out of investigative scope. He also reiterated his desire that the government continue to help industry to better understand some of the changes involved in the new FIS effects on the backlog, the investigative process and resulting delays, as well as the Tier 3 investigation changes. In particular, how some of the new items that will be required to be performed and returned by industry might affect delays in the process. He thanked ISOO leadership for continuous updates on Controlled Unclassified Information (CUI) implementation and rollout, and again described how anxiously industry awaits promulgation of the complete National Institute of Standards and Technology (NIST) standards. In addition, as there are as yet no implementation guidelines available, he expressed concern that there is no apparent risk-based tailoring. He noted that industry is beginning to see areas where subcontractors, especially smaller subcontractors, may not be capable of meeting some of the requirements, once they are delineated, which in turn may jeopardize the ability of the larger defense contractors to utilize them to meet these needs. He explained that there are numerous initiatives currently in play that they are trying to work through, and that they know that the Aerospace Industries Association is very active in some of these areas. He then stated that the area in which they continue to be most interested is observation and review of the actual Federal Acquisition Regulation.

Mr. Ingenito then noted that industry had enjoyed the opportunity to read and study a draft of the forthcoming ISL, where they were able to discuss a number of items and to share some potential concerns that they have requested be considered in preparation for across-the-board implementation. They were especially keen on those items that affect the larger companies who are to implement from an enterprise level, as well as DSS' willingness to come on-site and actually review particular areas. He noted that many excellent tools are already in development that industry got to preview, and that they are enthusiastically awaiting receipt of copies of those so that they can study the tools in greater depth, and perhaps provide other comments that might promote improvements. In addition, they understand that there are a number of items in legal review regarding the SAP manual, and they appreciate the progress thus far made by the NISPOM Working Group, especially the frank and open dialog. He then pointed out that in behalf of Policy Integration, a working group was formed, but has not yet established formal meetings. However, as there are so many things going on in this arena, they look forward to the opportunity to pull the various policy initiatives into one coherent form. To that end, they wonder if it is perhaps time to consider forming a joint policy executive committee of industry and government agencies in an effort to bring interested parties together in an attempt to establish an aggressive and proactive initiative, as opposed to the traditional reactive approach. They have lately been experiencing little success progressing through the SAP Working Group; however, they did recently enjoy some substantive meetings with the Air Force's Security Assistance Policy Coordinating Office where they received positive clarification guidance and impacts. Nevertheless, they wish to stress the need for continuous, consistent efforts throughout all the SAP community as the different processes are examined. Regarding the NISP Contractor Classification System and the Automated DD Form 254, industry needs to understand the plan for deployment and account administration so that they can begin to develop and incorporate the required training initiatives. Concerning the NISS, industry appreciated participating in the system requirements phase, and is standing by for further development meetings. Valerie Heil then commented on the progress being made on the SAP Manual, Volume #2, stating that it has cleared legal sufficiency review, and is now in the DoD process, which upon completion will begin deployment planning.

(E) Working Group Updates:

C&AWG Updates:

Tracy Brown, DSS, provided the C&AWG updates (see attachment 4). She began by reminding the Committee that the group had three primary tasks for fiscal year (FY) 2015. The first was to complete integration of all Cognizant Security Authorities (CSA) into the C&AWG. She stated that this initiative continues, and that the initial request for a review of their processes and metrics has been accomplished. The second was to initiate the NISP's transition to the Risk Management Framework (RMF). To that end, they are in the process of reviewing supporting RMF artifacts. The third primary task involves the required RMF revisions in reporting criteria in reports to the NISPPAC. With regard to DSS Office of Designated Approving Authority timelines, we are holding steady in the issue of interim accreditations via either straight to Authority to Operate (within the 120-day goal) or Interim Authority to Operate (within the 30-day goal). She reported that they are continuing to improve the ODAA Business Management System, and have received many positive comments from both industry and other stakeholders. For example, in September 2015 the new release aloud industry to create unique identifiers, and we were able to finalize our reporting capability process.

PCLWG Updates:

Mr. Pannoni introduced the PCLWG's report by thanking Mr. Wilkes for standing in for him as Chair of the working group at its last meeting. He reminded the Committee that among quite a number of the membership at today's meeting, there is a concern with unfolding events over the last several months with regard to investigative timelines continuing on an upward, if not somewhat precipitous trend. Therefore, the various working group members will present some slides for discussion and illustration through which we can perhaps come up with a get-well plan. One of the things the PCLWG noted was that in 2006, Robert Andrews, Deputy Undersecretary of Defense for Counterintelligence and Security, issued a memo to all defense components and the military departments reminding them that personnel security clearances do not expire. Keeping that in mind, the thought arose that perhaps in today's environment, where we have a similar situation with the proliferation in the timelines and particularly at Top Secret (TS) level PRs, that the Director of National Intelligence (DNI), as the security executive agent, jointly with the DoD, where most of the SAPs reside, consider issuing a similar reminder to all Executive branch agencies. Next, Mr. Pannoni mentioned that the PCLWG industrial members expressed some concern with the lack of awareness as to the changes in the FIS. They had requested several months ago that they be provided with those new standards so that they might prepare for any operational changes, as they would have preferred to be proactive as opposed to reactive. Suffice it to say, we must remember that they are our partners, and that in the future we must try to share as much information as is possible. Another continued concern noted by the PCLWG, and as yet unresolved, is the lack of clarity on the backlog of cases that are in adjudication, and may be residing with the Defense Office of Hearings and Appeals (DOHA). Improved clarity in this issue might enable industry to manage expectations in terms of some of these cases that have been waiting for an inordinate amount of time. Thus the working group asks that the Committee inquire as to what can be done to share, not on a one-by-one basis of individuals, but in terms of the number of cases that have made their way to DOHA, and segmented in terms of a timeframe of perhaps one to 30 days, 31 to 90 days, and beyond 90 days. It should be made clear that the group is overall pleased, as we see the backlog has been significantly reduced. Nevertheless, there are some older cases in which it would be helpful to industry to have a better idea of where those cases reside in the process. Finally, he revisited the good news that signature click to sign should reduce cases that are either delayed in their opening or otherwise rejected, as well as the shrinking of the 180-day PR window to 90 days for the opening of cases.

Ned Fish, DoD CAF, provided the CAF updates (see attachment 5) and reminded the Committee that the trends for the backlogs continue to be reduced since the 2013 advent of the DoD CAF. He noted that the backlog is down about 75%, and that the overall workload is down about 50%. He reminded the Committee that some of the CAF's concerns remain the same as in previous reports, such as the continuing need to get the e-Adjudication business rules approved for Tier 3 implementation so that we don't lose that efficiency capability, at which point we will be able to increase capability. He expressed appreciation for the excellent success enjoyed by the OPM, Office of the Director of National Intelligence (ODNI,) and DoD partnership as they continue to work through the e-Adjudication process. He noted that the CAF is a full partner in the CE pilots. He explained that the CAF is still working exhaustively on deploying a single version of the Clearance Adjudication Tracking System (CATS), and now that DMDC owns both CATS and the Joint Personnel Adjudication System, we will be able to merge with the Joint Verification System into a single system which includes portals to the security officers. Without doubt, we are in a far better position today, but we look forward to that one system that will be deployed at the CAF early in the upcoming calendar year. It will inevitably cause a temporary negative impact as we take people offline to train them and ensure that they are ready to operate on the new system, but this will be a short- rather than mid- or long-term concern. He then reminded the Committee that approximately two years ago, when he first introduced them to the backlog, he described it as approximately 8% of the overall NISP yearly workload. He noted that they now have that down to about 1.6%, meaning that about 98% of the personnel are receiving quick adjudications. He suggested that should you look at the timelines you will note that the backlog has been dropping precipitously in the past six months, and you can now see why. As we close those old cases, those timelines, particularly for industry, have gone up. But, as we have brought them down even lower, closer to within where the timeline is now, the law of averages is going to bring that up. So the mantra remains the same: no matter the short-term cost we will keep going, and in the end we will have a very clean and efficient process. Finally, he stated that from the DoD CAF's perspective, the end-to-end process, even with those impacting outliers, will be completely gone by the end of FY 2016.

Ms. Loss, OPM, reported on industry investigations based on cases that have been adjudicated using the Performance Accountability Council (PAC) timeliness metrics (see attachment 6). She described a somewhat bleak account of the metric conditions with respect to average timeliness, and promised that Merton Miller, OPM, would provide a more in-depth understanding of where we are in the get-well plan for investigations timeliness. She began by stating that there is a correlation between the fastest 90% of adjudications and the total number that are completed. That is, the greater number of investigations there are to perform, the more time required to complete them all. For example, when we calculate metrics on an average, we are getting to a certain timeliness, but that does not account for the fact that some Secret (S) investigations sail right through the process, while some take longer because they are subject to varying factors, such as the need for local police checks in places where we don't have automated records, or the need to gather more information from the subjects themselves. At this point, the Chair expressed his appreciation for OPM's thoroughness in presenting the data in all iterations. He enlarged the concept by stating that an end-to-end metric is different from component part metrics, thus creating the ability to discriminate between what is occurring in adjudications versus investigations. Further, when combined, their interrelationship begins to emerge. Therefore, he applauded the efforts of all members of the PCLWG for the evolution of our metrics, yet warned that we must retain the ability to discriminate the metrics the Committee enjoys, and for the transparency that it gives us. However, he cautioned the Committee to be responsible metrics readers, so as to retain the ability to discriminate between what they do describe and what they do not, and that we must remain vigilant to select the right metric in order to discover the right answer. Ms. Loss then reminded everyone that these metrics have been approved by the PAC, but that they could certainly be supplemented if additional measurements are desired. The Chair then added that as we traverse the diverse concepts relating to the backlog, we must understand that reading metrics is contact sensitive, and therefore they must be carefully differentiated. Ms. Loss then explained that the primary concern of everyone is that we have an inventory that is much greater than our present capacity to complete investigations within the Intelligence Reform and Terrorism Prevention Act (IRTPA) timeliness metrics. In fact, the metrics illustrate that we actually require about twice as long, and that that directly equates to having approximately twice as much work in inventory as we have the capacity to perform. However, both we and our industry partners have been taking measures to increase capacity, and we will continue to investigate the conditions in order to uncover all the factors that influence inventory and capacity. At present, we have about 384,000 cases in inventory. She then noted that OPM typically considers maintaining approximately six weeks' worth of work in the inventory in order to meet timeliness objectives without exceeding timeframes. She then called upon Mr. Miller to discuss some of the circumstances that dramatically affect the present and future capacity in our achievement climate.

Mr. Miller noted that he would take a somewhat different approach to the questions surrounding IRTPA requirements versus workload capacity (see attachment 6a). He explained that from his perspective we are perhaps not attacking the conditions so much as the results, and that conditions were his primary function. First, he described some of the challenges that are occurring, and coupled that with a plea that the membership consider complaining to anyone who will listen about the impacts upon their work conditions from a business operations perspective and in light of the continuously growing backlog. He explained that most of the conditions occur as a direct result of numerous cost factors, and that most of us understand that any growth in capacity means additional dollars must be spent. He noted that when we had the original backlog we discussed the governmental efficiencies that were impacted, and indeed, billions and billions of dollars were impacted. So the question now becomes whether it is worth investing more dollars in growing capacity to avoid those lost efficiencies that we are now seeing across both industry and government. He reminded the Committee that Ms. Loss had mentioned some 384,000 cases in the current backlog, and that their normal operations run to approximately 160,000 cases and require about six weeks processing time. So when some decisions were made about who would actually perform the future workload, that immediately reduced our ability to grow and thus to meet the demands. Also, there would be delays in work completion because we had to transfer work away from the contractor work force and redistribute it to the federal work force. Therefore, there was an immediate backlog increase that we must recognize and face. Now our current contract partners are performing exemplary work, but we will not lose focus on the quality of the investigations or the need to deliver what is required to be able to properly adjudicate and vet the individuals who are going to work for you. We are constantly engaged in growing work capacity, and yet we have a commitment, even in light of reduced additional resources capable of conducting background investigations. In fact, we have reached maximized availability on both the contract and federal side to accomplish background investigations.

He recognizes that each case represents a certain number of man hours through which to actually deliver the product. Moreover, he noted that their contractors have made growth commitments over the next several quarters, meaning that work force efficiency will not come on the day of hire, but only after a thorough vetting procedure, a comprehensive training process, and a mentorship period that introduces them to the field and ensures delivery at a high standard. There will always be some hand-holding and some lost efficiency as we begin to grow, but we have a strong commitment in which we are investing in the hire of 400 new field investigators. But, due to that ever-present cost factor, we will be forced to move more slowly through 2016 in hiring new staff, causing us to fail to reach full capability as quickly as we would have desired. He asked that the membership carefully examine the slides, so that they will note that in some weeks we lose ground, and that there remains the other factor that we still have more incoming work than we typically see. In fact, in FY 2016, the field's work-intensive cases have already risen by 38%, and thus the capacity problem intensifies. We are trying to address these conditions, and our goal is to provide you more details about how we are proceeding in boarding staff, reducing growing capacity, and addressing the current backlog. He then promised a new report at the next meeting that would describe OPM's projections for a return to IRTPA's 40/80 investigative timeline standards. He admitted that the story he has to tell today is not good, and that they are potentially looking at 2020 before reaching a return to complete normalcy, and thus the reason for his pleas for the membership's help. Martin Strones, industry, asked if there was information available to share on why the volume of investigations was also increasing. Mr. Miller replied that OPM has actually reached out to all of its customers to find out why there are increases in projections, but that, as yet, there are no satisfactory answers. He noted that, most who have been in this business for a while understand that there is not a great deal of workload predictability. Further, he pointed out that even as the projections continue to vacillate, one of the conclusions in a recent DoD study was that we all really need to focus on how we can manage workload more efficiently, so we can perhaps reduce these fluctuations, and that we must continually strive to put new methods in place that would proactively address the issues. Mr. Pannoni commented that this might perhaps be identified as a capacity-capability issue even now in the beginning stages of a four-year run. Mr. Miller agreed that we were indeed in the grips of an extended capacity issue. Mr. Pannoni then made a general comment that although we always try to avoid considerations that amount to sacrificing security, perhaps we should be looking at doing a better job of risk management in terms of cases of people who are already on board but who have to be submitted for a PR? Mr. Miller went on to opine that at any time we are reinvestigating people out of scope, that is, not within the five-to-ten year period, there is already an increased national security issue. He went on to point out that government agencies are hard pressed in trying to move forward on CE, but that clearly we must do much in considering those populations that are either outside of scope or are in access but that may have some adjudicative anomalies or other vulnerabilities that might have been created based on performance, character, or conduct, and he declared that he would ask no one to advocate with Congress or anyone else about moving the standard in the wrong direction relative to vetting. Mr. Sims then commented that given the state of the investigative process, perhaps the only way we are going to improve is to employ automation in order to efficiently evolve the process itself. He pointed out that this is the CE process, and that our efforts should be always to advance this process in order to find more effective ways to better utilize it in support of the investigative process. Mr. Miller agreed, but cautioned that not everything relevant to adjudication resides somewhere in a database. Still, he noted that even if CE was ultimately to provide only a 50% solution, it would be beneficial. Even now DNI is spending a lot of time working with our commercial partners and others on how we might be able to query their systems on a more regular basis as a CE tool. Dorothy Rader, industry, pointed out that in view of the fact that government-industry partnerships already perform intensive investigations, might we join forces to share some of that data in order to accelerate potential leads and/or the government investigative process? Mr. Miller asked if there were industry vetting standards already in place? Ms. Rader responded that to her knowledge industry vetting procedures were not universal, and thus, not standard. He suggested that therefore there may be some challenges in attempting to determine what industry's contribution might be to such an initiative.

Mr. Miller posited about whether there might be stressors on the government-industry processes, and if there are already across-the-government records repositories in place. In addition, he cautioned everyone to understand that the systems used by law enforcement and similar agencies are not without stressors. As an example, and without prejudice, he described the FBI's rather significant backlog on name checks, stating that without this particular problem OPM could deliver up to 20,000 cases immediately. The Chair thanked Mr. Miller for this additional data included in the OPM presentation, and advised that his initiative reflected yet another example of the overall posture that OPM has towards the industrial community, which is as helpful as anyone could want it to be. He also suggested that the Committee would invite him to return as the story evolves, and asked if he might have a follow-up conversation about how the NISPPAC could help him with an articulation of the impacts of the current situation, as he believes that is a perfect role for the Committee as a supplier of that kind of feedback. He explained that his objective would be to calibrate it for both components of the industry-government partnership, illustrating the differing impact perspectives, but all rooted in the same experience. Mr. Miller welcomed the opportunity to meet with the Chair in a certain sharing and learning experience for both.

Gary Novotny, ODNI, then presented the Intelligence Community's (IC) timeliness metrics (see attachment 7). He prefaced his remarks with a reminder to the Committee that, in support of earlier discussions regarding PRs and the backlog, there had been an October 2012 DNI memorandum to agency heads discussing the use of a risk-based approach when prioritizing investigations. He pointed out that many of the areas of concern surfaced in today's discussions were mentioned in that memorandum, and that he could request that it be re-issued, and perhaps updated, especially for the sections emphasizing the risk-based approach to active PR investigations. The Chair thanked him for reminding the Committee of the memorandum, and added that he also had attended many meetings where there had been discussions about reminding agencies that there is already latitude existing in any number of policies, whether related to SCI or SAP access, regarding which cases to put into the queue and in what order, or numerous other investigations issues. He corroborated that both OPM and the IC had confirmed the memorandum about which Mr. Novotny spoke, and suggested that the Committee would welcome its re-issue so that we could refresh ourselves with its content. Also, prior to beginning his IC metrics presentation, Mr. Novotny introduced David Morrison, the Special Security Directorate's new Deputy Systems Director, and encouraged the membership to take the opportunity to greet him at the conclusion of today's meeting.

Mr. Novotny then began his presentation by explaining that the IC metrics follow, much as in the case of OPM, the PAC timeliness methodology. He explained that with regard to PRs, the last quarter of FY 2015 had shown a slight decrease in TS, S, and Confidential adjudications timeliness cases. However, he noted that background investigations still continued to increase for the year. He then elaborated on his metrics with regard to quality assessment standards for background investigations, and especially the initiatives on which OPM, ODNI, and DoD are presently working. He reminded the Committee that in January 2015 they had distributed to the receiving agencies the ability to rate the quality of investigations, and that, in so doing were able to establish a consistent and community-wide quality assessment lexicon. He noted that in the coming months they would issue an agency implementation plan explaining how to put these quality standards into action. In addition, he detailed their progress towards development of the design of a new quality assessment reporting tool, which will be a repository of agency background investigations' assessments. In addition, there will be another tool with which they will be able to analyze metrics in order to illustrate and troubleshoot total Executive branch background investigations' quality. He then touched briefly on the group's new e-Adjudication initiatives, explaining that there is an upcoming conference call for the purpose of solidifying the basic business rules, so that they can eventually increase the number of cases that are likely to clear the process. He then informed the Committee they were already working with the agencies to troubleshoot any issues with the Tier 3 implementation plan, and that he would be amenable to answering implementation-related questions.

Ms. Loss added that there was some information that might enhance concerns with the FIS's Tier 3 implementation. She pointed out that they have to date been unable to release the new FIS, as access to the standards and associated expansion model could be a means for people to game the system. However, there are new information categories that are collected in the investigation that we are able to share. For example when employers are receiving requests for employment information it is clear that that is part of the new Tier 3 standards, and we can certainly take this to the PCLWG. The other piece we can take to the group concerns the S-level OPM INV 41, which is a supervisory form through which FIS may send a written inquiry to the employer in an attempt to verify the subject's employment history and gather relevant character and conduct information. She noted that the OPM INV 41 is not a new form, as it has been used for some government employees for over 20 years, but as it can now be used in industry it should soon improve investigations through across-the-board reciprocity. Moreover, we never intended that the use of the form should break timeliness or cost barriers, and the things that were accomplished when we had investigators speak to the limited references were determined to be cost prohibitive. Whereas we do get a good return on the completed form which therefore makes it more cost effective. She pointed out that OPM is however asking for assistance from the community, as this is a perfect opportunity to exercise the "if you see something, say something" challenge. Kim Baugher, Department of State, asked under what circumstances a company who has previously vetted an employee might simply put that information on a copy of the form so someone could look at it? Ms. Loss replied that perhaps there are some possibilities for this iteration in the use of the form, and that they may in the future ask the PCLWG to consider the concept. Ms. Hickman then asked Ms. Loss to share a little more in-depth information about manipulation of the form, such as with whom the form is shared. Ms. Loss responded that the form is sent to the employing entity and the listed supervisor. Mr. Wilkes responded that the forms are indeed being sent to individuals rather than the entity's Human Resources (HR) office where the companies might consolidate the information and subsequently have HR attest to it. In addition, due to the fact that the information goes only to an individual, we can only hope that it ultimately gets shared with the company, which is often not the case, and thus we can never track it to determine its true value. Ms. Loss responded that she would take the concept under advisement, but that she did not want to create a condition that would undermine the original objective, which was to substitute the form for the on-site investigator and thus reduce prohibitive costs.

The Chair then summed up the discussion by reminding the Committee that this issue involves an element of reform relative to the FIS and Tier 3 implementation, and that although we have now acquired some degree of measurability since we first began to align investigative processes, we have by no means conquered all our objectives. Therefore, we will continue this conversation in the PCLWG, and we'll begin by trying to figure out how does bringing this community into the established practice of sending out these forms, which we have known for over 20 years, alter or offer different opportunities to optimize it going forward. The Chair then concluded the discussion by explaining that this whole dialogue pertaining to things that happen in the working groups is about sharing information such as perspectives and impacts, and there is an element of trust established there. Therefore, the dynamic has a natural "we-don't-know-it-until-the-government-shares-it-with-us perspective," and even though both industry and government participants are interested, there is a trailing effect that posits that until the government asks us they don't know what we think, even though we already have thoughts. Thus, this idea of releasing the FIS is an example of where there's a little grit in those gears, and for all the right reasons. Now some government individuals know this, but in the larger government reaction to the breaches there are a number of things going on across government with regard to repositories of private information that don't have anything to do with the background investigations process, but rather are symptomatic of what happened with OPM. The government is aggressively trying to figure out what are the new requirement levels and rules and what are the ways to handle and protect this kind of information. In addition, in this conversation, as well as in the post-OPM breach conversation there are questions related to the establishment of clearer controls guidance that are being impressed on background investigation information. So the difficulty that Ms. Loss expressed regarding how much you can be told initially seems in stark contrast with the usual we-give-it-to-you-and-you're-informed methodology, and is all a part constrained by that dynamic. Hence, there are now recommendations being made about placing more formal controls on background investigations information, as well as and other categories of sensitive, personally identifiable, information, in new ways and for all of government. But we must understand that until all this sorts itself out, we are going to keep having conversations that are impaired in their ability to share everything. He asked that our industry partners keep this in mind, and explained that he knows that our government partners are already thinking of these things, but that at the working group level we should be able to do everything we can in that room and during that meeting time to make available as much information as possible and to share as many ideas as are fruitful. He asked for everyone's patience, as it is a difficult and complex problem that goes far beyond background investigations information, though it simultaneously encapsulates everything about background investigations information.

(F) Controlled Unclassified Information (CUI) Updates:

The Chair reminded the membership that in the July 2015 NISPPAC meeting we had just closed the public review and comment stage of the CUI regulation, and that in the time since, we received approximately 250 comments from industry and academic groups, members of the public, and public interest advocacy groups. He noted that all of the comments were helpful, and that they resulted in a revision of the rule that is currently out with agencies for what may be a last or a second-to-the-last policy review in the Office of Management and Budget's (OMB) regulatory review and comment process. This then is where we are down to "last chance to say" agency comments, and the remaining burden upon we who are charged with writing the regulation is to find fixes for the lingering issues. He noted that the issues that remain in the CUI rule largely have to do with writing the rule in a way that avoids unintentionally infringing upon agencies' authority to perform their mission. He informed that we are talking about the control of information essential to agencies' ability and freedom of motion to meet their mission requirements, and that has differing impacts in law enforcement, homeland security, privacy, and acquisition communities. Therefore, we have the tough task, and we're sitting down with agencies individually and going through and working some of these things out. He expressed understanding for and appreciation of Mr. Ingenito's comments, as well as the comments that we get regularly through informal sharing sessions, about the DFARS that is currently in effect, and the way that it employs some aspects of the future CUI regulatory regime. We want to make sure that we learn and fix all of the issues that are present there and give the best possible advice to the agencies about how to use their authority when it comes to CUI.

In his capacity as the CUI Executive Agent, he advised that agencies need to be more discriminate in the use of their authority, and more attentive to the impact of their requirements to put control on information, because that directly impacts operations in industry and other non-federal partners. So, if you ask for everything to go out under some form of control because you have that authority do so, you need to understand the tremendous impact that that has on day-to-day operations and potentially costs in negative impacts on information sharing. Thus, there are still issues that remain for agencies to work through, and it will continue for some time yet to be a bumpy ride. He described how in other parts of government emphasis on cyber security incident reporting and increased consistency in the protection levels that are on contractor systems that handle government information is even now a strong area of emphasis in the Federal Chief Information Officer (CIO) space. He continued by informing how OMB and the Office of Federal Procurement Policy (OFPP) have put out draft guidance for comment on improving cyber security in federal acquisition, all of which sounds exactly like the areas included in Mr. Ingenito's comments with regards to where the DFARS has gone. He noted that we are working together with the OFPP and the Federal CIO's office to align the CUI regulation in its near-final draft status. The plans to have a federal acquisition rule standardized for all of these topics that would supplant the elements of the DFARS' clause, bring the NIST standard into application, and tell you clearly the rules for identifying and handling CUI. Doing so in a cyber-secure 2016 context is a complicated policy integration, but one in which we are starting to see some success. He noted also that we have commitments from OMB and OFPP that will allow us to write one FAR clause that will handle all of these things, and that the guidance that comes out from OMB instructing agencies on how to seek the security levels they need in protecting their systems is synchronized and consistent with the CUI regulation as promulgated. He ensured the Committee that this was as much time as we have spent with you, your companies, and your trade associations explaining CUI and its intentions, and that he has done the same thing within the Executive Office of the President. He promised to inform everyone when the next round of public comment is sought on any OMB guidance relative to improving cyber security in the federal acquisition process, and then noted that they would hear from us first when we have the ability to formally propose a FAR clause or set of FAR clauses that will address these things and get that whole public review and comment started. Finally, he described this all as a lot of process, a lot of writing, and a lot of waiting until it can be shown. However, he stressed that is the way the process works, and that he is hopeful that we are going to see a CUI rule in the early part of calendar 2016. This will allow for discussion about the FAR rule and timelines for implementation and when you can see requirements coming your way through contracts in a way that the government agencies together plan. He then called for Mr. Pannoni to present the NISP implementing directive updates.

(G) The 32 C. F. R., Part 2004, "NATIONAL INDUSTRIAL SECURITY PROGRAM DIRECTIVE NO 1" Updates:

Mr. Pannoni then presented the NISP implementing directive updates, describing its function as that of assisting agencies with performing their industrial security requirements under the NISP. He noted that the directive has not been updated in several years, and over the last two months the five CSAs, plus DSS, Central Intelligence Agency, and ISOO, have been meeting to define and describe the requirements. The ultimate plan is to assemble the NISPPAC for comment and discussion relative to the recommended changes prior to its submission for public comment. He explained that one of the most important and required changes will be the inclusion of insider threat guidance, as defined in Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," coupled with the minimum standards that agencies must achieve in order to implement their responsibilities vis-a-vis insider threat requirements under the NISP. In addition, the group will examine some of the long-standing, overarching goals of the NISP, namely the endorsement of a single, integrated, cohesive program, through which they will develop guidance related to essential mechanisms such as facility security clearance and foreign ownership, control or influence standards, and a responsible CSA determination. He noted that they plan to present an updated implementing directive draft to the NISPPAC in early 2016.

IV. New Business:

There was no new business proposed.

V. General Open Forum/Discussion:

The Chair then opened the meeting to comments from the attendees, and asked for inputs on any issues of interest or concern. There were none.

VI. Closing Remarks and Adjournment:

The Chair confirmed that the next NISPPAC meeting is scheduled for March 16, 2016, at NARA. He then reminded the Committee that subsequent to the November 2015 meeting we asked for feedback regarding the notion of holding our spring/summer meeting concurrent with the National Classification Management Society's annual conference, to be held June 7-9, 2016 in Nashville, TN. He noted that while the feedback we have received from both government agencies and our industry partners was all favorable towards holding the meeting at that venue, we have nevertheless not yet heard from all government or industry membership. Therefore, we've asked Mr. Pannoni and the ISOO team to follow up so that by the next NISPPAC meeting we can announce the final determination. Finally, he reminded the membership that the budget forecast for FY 2016 maintains the status quo, and that as such there will be no travel funds available for our industry representatives, and he again expressed his appreciation to all who attend these meetings at their own expense, thanked their company leadership for sponsoring their travel, and reminded all meeting participants that a dial-in capability will again be available for any who cannot travel to the meetings. The Chair adjourned the meeting at 11:44 a.m.

Attachment #1

Attachment 1

NISPPAC MEETING ATTENDEES

The following individuals attended the November 18, 2015, NISPPAC meeting:

John Fitzpatrick,	Information Security Oversight Office	Chairman
Greg Pannoni	Information Security Oversight Office	Designated Federal Official
Stan Sims	Defense Security Service	Member/Presenter
Laura Hickman	Department of Defense	Alternate/Presenter
Kim Baugher	Department of State	Member
Christopher Corbin	Department of the Air Force	Member
Jeffrey Bearor	Department of the Navy	Member
Charles White	National Security Agency	Attendee
Scott Ackiss	Department of Homeland Security	Member
Eric Dorsey	Department of Commerce	Member
Merton Miller	Office of Personnel Management	Member/Presenter
Gary Novotny	Office of the Director of National Intelligence	Attendee/Presenter
Anthony Ingenito	Industry	Member/Presenter
J. C. Dotson	Industry	Member
Martin Strones	Industry	Member
Michelle Sutphin	Industry	Member
Keith Minard	Defense Security Service	Attendee
Anthony Smith	Department of Homeland Security	Alternate
Mark Nolan	Department of the Army	Alternate
Valerie Kerben	Nuclear Regulatory Commission	Alternate
Kathleen Branch	Defense Security Service	Attendee
George Ladner	Central Intelligence Agency	Alternate
Cheryle Winder	Office of the Director of National Intelligence	Attendee
Lisa Loss	Office of Personnel Management	Alternate/Presenter
Tracy Brown	Defense Security Service	Presenter
Valerie Heil	Department of Defense	Attendee
Jay Buffington	Defense Security Service	Attendee
Dan McGarvey	MOU Representative	Attendee
Bryan Mackey	MOU Representative	Attendee
Kirk Poulsen	MOU Representative	Attendee
Lisa Desmond	Department of the Army	Attendee
Dennis Keith	Industry	Member
Ken Kirby	Industry	Attendee
Leonard Moss, Jr.	Industry	Attendee*
Carl Piechowski	Department of Energy	Attendee*
Vince Jarvie	Industry	Attendee*
Steve Lewis	Industry	Attendee
David Best	Industry	Attendee
Bill Davidson	Industry	Member
Stephanie Clearwater	Industry	Attendee

Christopher Heilig	Industry	Attendee
Mitch Lawrence	Industry	Attendee
Joseph Costanza	National Aeronautics and Space Administration	Attendee
Glen Clay	Department of Navy	Attendee
Mark Pekrul	Department of Energy	Alternate
Charles Tench	Defense Security Service	Attendee
Dennis Arriaga	MOU Representative	Attendee
Anna Thomas	Industry	Attendee
Noel Matchett	Industry	Attendee
Aprile Abott	Industry	Attendee
David Morrison	Office of the Director of National Intelligence	Attendee
Mark Rush	Industry	Attendee
Dorothy Rader	Industry	Attendee
Dorianna Rice	Industry	Attendee
Sandra Sohenmann	Industry	Attendee
Alegra Woodard	Information Security Oversight Office	Staff
Robert Tringali	Information Security Oversight Office	Staff
Carolina Klink	Information Security Oversight Office	Staff
Michael Manning	Information Security Oversight Office	Staff
Joseph Taylor	Information Security Oversight Office	Staff

*Attended via Teleconferencing

Attachment #2

Action Item

From 11/18/2015

NISPPAC meeting

The PCLWG will propose a metric or other means to assess the value of the data garnered from the use of the OPM INV 41 Form, “Investigative Request for Employment Data and Supervisor Information.”

Attachment #3

NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

Industry

18 Nov 2015

Outline

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

National Industrial Security Program

Policy Advisory Committee Industry Members

Members	Company	Term Expires
J.C. Dodson	BAE Systems	2016
Tony Ingenito	Northrop Grumman Corp.	2016
Bill Davidson	KeyPoint Government Solutions	2017
Phil Robinson	Squadron Defense Group	2017
Michelle Sutphin	BAE Systems Platforms & Services	2018
Martin Strones	Strones Enterprises	2018
Dennis Keith	Harris Corp	2019
Quinton Wilkes	L3 Communication	2019

National Industrial Security Program

Industry MOU Members

AIA	J.C. Dodson
ASIS	Dan McGarvey
CSSWG*	Brian Mackey
ISWG *	Marc Ryan
NCMS	Dennis Arriaga
NDIA	Mike Witt
Tech America/PSC	Kirk Poulsen

National Industrial Security Program

Policy Advisory Committee

- Charter
  - Membership provides advice to the Director of the Information Security Oversight Office who serves as the NISPPAC chairman on all matters concerning policies of the National Industrial Security Program
  - Recommend policy changes
  - Serve as forum to discuss National Security Policy
  - Industry Members are nominated by their Industry peers and must receive written approval to serve from the company’s Chief Executive Officer
- Authority
  - Executive Order No. 12829, National Industrial Security Program
  - Subject to Federal Advisory Committee Act (FACA), the Freedom of Information Act (FOIA) and Government Sunshine Act

OPM Data Breach

- Actions Taken
  - DIA & NRO discontinued use of e-Qip.
  - OPM suspends e-Qip for processing of new BI cases.
  - OPM and the ODNI work alternative process for BI processing.
  - OPM actions taken to harden and protect the systems and data
  - Notifications made or in process of being made to affected individuals on breach and government provided services.
  - DSS,USD(I), and OPM did a good job of promulgating information to industry with their telecom's as they worked through the issues. (KUDOS)
- IMPACT
  - Lack of initial coordinated leadership to oversee agency actions.
  - Timely guidance not promulgated to industry.
  - Significant delays in BI process directly impacting contract performance (SCI/SAP efforts)
  - Increase to existing clearance backlog due to the shutdown.
- Next Step
  - Working thru the backlog. What is the "Get Well Plan"?
  - NISPPAC involvement to ensure consistent agency actions.
  - Interim policy guidance to address:
    - Interim Clearances and Out of Scope BIs. ODNI Memo to Components (similar to 2006 letter)
    - CAC Suitability (NACI) .

Security Policy Update

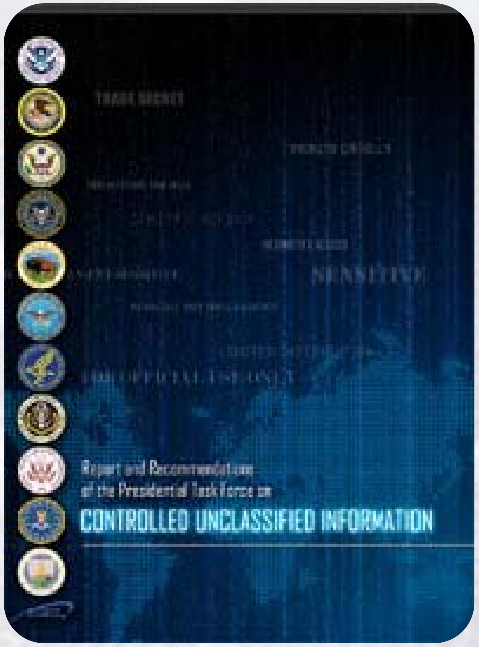
Executive Order #13556

EO # 13556

Controlled Unclassified Information (CUI)

4 NOV 2010

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



Report and Recommendations of the Presidential Task Force on CONTROLLED UNCLASSIFIED INFORMATION

- Next Steps
  - (NIST Special Publication 800-171) Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations published June 2015.
    - Provides no implementation timelines nor guidance
    - Does not allow for risk based tailoring
    - Fails to address non applicability of requirements due to the use of compensating controls
    - No mechanism to address inefficiencies due to conflicting guidance.
    - Challenges for small contractors to implement (cost and lack of staff).
  - ISSO working with FAR Council on specific CUI clause.
    - Awaiting opportunity to review draft clause.

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 InfoSec, Personnel Security and System Security
- 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.
  - Fractured implementation guidance being received via agency/command levels.
  - Awaiting release of NISPOM Conforming Change # 2 and DSS ISL.
  - Many customers already asking industry to describe their Insider Threat programs

Security Policy Update

Executive Order #13691

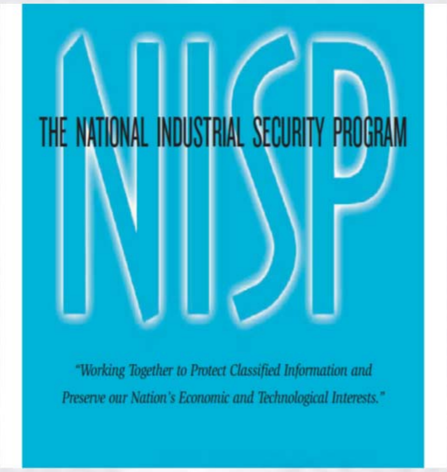
EO # 13691

Promoting Private Sector Cybersecurity Information Sharing

13 February 2015

Department of Homeland Security

- Builds on EO 13636 (Improving Critical Infrastructure Cybersecurity) and PPD-21 (Critical Infrastructure Security Resilience) to address the area of Private Sector information sharing.

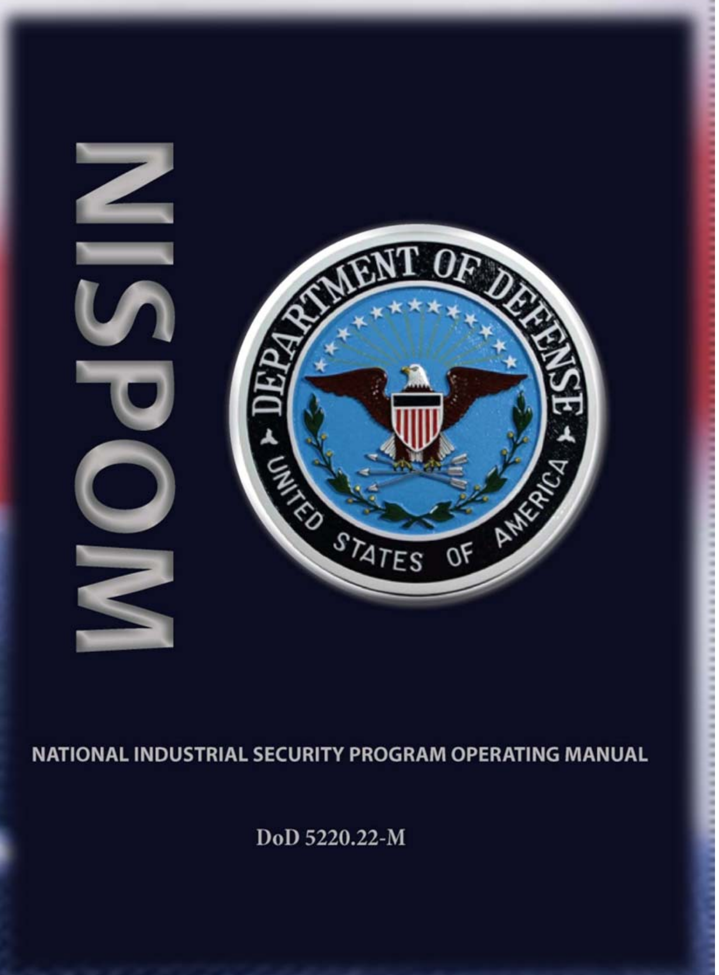

NISP
THE NATIONAL INDUSTRIAL SECURITY PROGRAM
"Working Together to Protect Classified Information and Preserve our Nation's Economic and Technological Interests."

- Amends the National Industrial Security Program (EO 12829)
  - Inserts the Intelligence Reform and Terrorism Prevention Act of 2004.
  - Adds the Secretary of Homeland Security as a cognizant security agency.
    - Drafting NISPOM enclosure addressing Critical Infrastructure Program
- Meeting with ISOO, DOD Policy and DHS
  - Afforded the opportunity for Industry to better understand the change to the NISP and have questions addressed.
- Next Step: DHS development of corresponding NISPOM section
  - Awaiting opportunity to review draft. No ETA on draft.

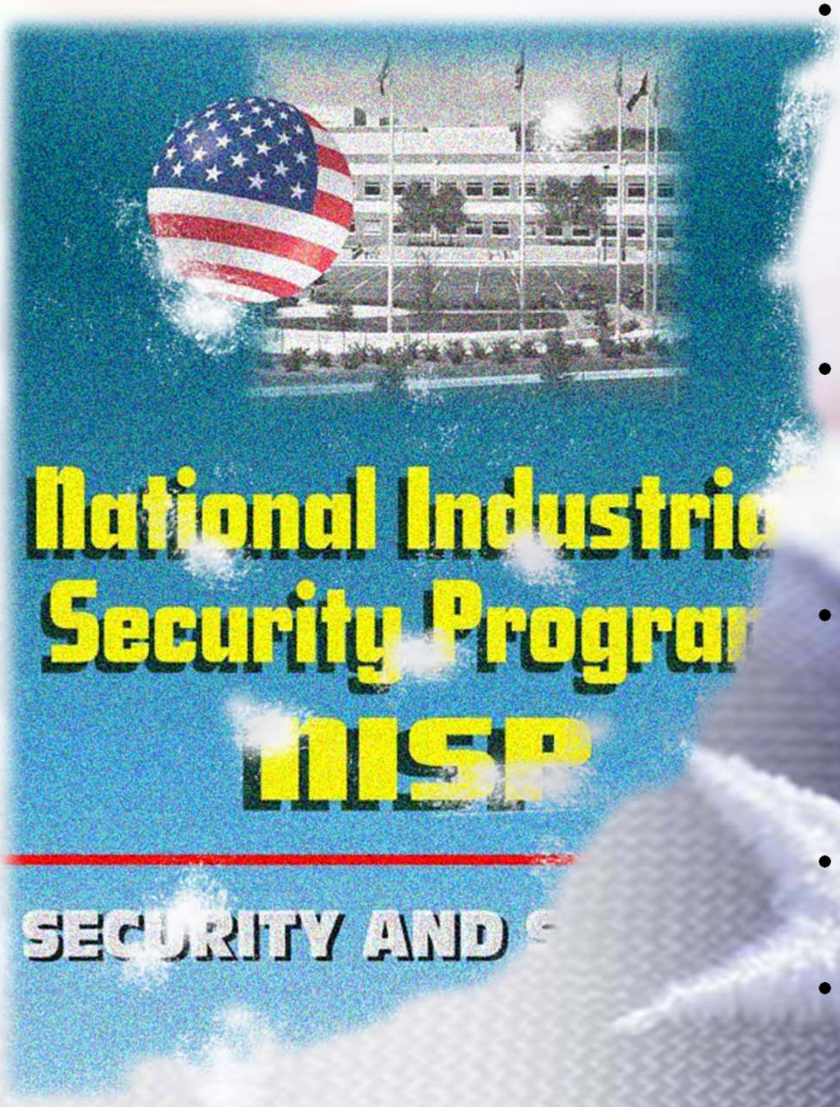
Security Policy Update

Industrial Security Policy Modernization

- National Industrial Security Program Operating Manual revision and update
  - Industry provided comments on draft Jun/July 2010
  - NISPOM Re-Write WG established. Gov/Industry team held numerous successful joint meetings working Bucket 1 thru 4. Bucket 5 meeting not scheduled yet.
  - Awaiting conforming change #2 release and DSS ISL.
  - Reviewed JPAS ISL and provided comments.
- Department of Defense Special Access Program Manual development
  - Vol 1 (General procedures) Just published in June
  - Vol 2 (Personnel Security) in Legal review
  - Vol 3 (Physical Sec) Published
  - Vol 4 (Classified Info Marking) Published
  - Eliminates JFAN and NISPPOM SAP Supplement upon publication of all the above.
- 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



Policy Integration Issues



- National & world events have stimulated reactions for policy changes and enhanced directives to counter potential vulnerabilities
  - Key areas include Cyber Security, Insider Threat and PERSEC.
  - Recent OPM Data Breach
- Process for directive/policy development and promulgation has become cumbersome and complicated.
  - Multiple years in most cases.
- Complications and delays have resulted in fractured lower level organization implementing a singular focused plan.
  - Inconsistency among guidance received.
- Driving increased cost for implementation and not flowing changes thru contract channels
- Policy Integration Working Group
  - Consider forming a joint policy executive committee.
  - Tracking in excess of 80+ initiatives on the policy tracking matrix.

National Industrial Security Program

Policy Advisory Committee Working Groups

- Personnel Security
  - Working group moving out to address areas of concern.
    - E-adjudication business rules will be aligned with new Federal Investigative Standards. New FIS expected to produce an decreased in e-adjudication across the board.
    - DOHA SOR Process. Definitively ID true caseload and aging of those cases.
    - Focused on the e-signature (click-to-sign) release expected 12 Dec 2015.
    - Expecting backlog to continue growing based on OPM Breach, new FIS and DSS change to 90 day PR clearance initiation process.
- Automated Information System Certification and Accreditation
  - Working group focus is on incorporating the Risk Management Framework (RMF) into future process manual updates. Early collaboration on this initiative will be key to successful transition. Positive interactions in the multiple meetings.

National Industrial Security Program

Policy Advisory Committee Working Groups (cont.)

- SAP Working Group
  - Numerous situations with inconsistent guidance and implementation of changes relating to JSIG (RMF), TPI and PerSec.
  - Formalized working group established and multiple meetings occurred.
  - Held separate meeting with USAF SAPCO office and OSI. Good dialogue and progress visible.
- Ad-hoc
  - NISP Contractor Classification System (NCCS) – Automated DD254 system
    - What is plan for deployment and account administration?
    - Industry need to plan for training of security, contracts and PM's.
  - Development of National Industrial Security System (NISS)
    - Participated on the system requirements phase and standing by for further development meetings.

Attachment #4

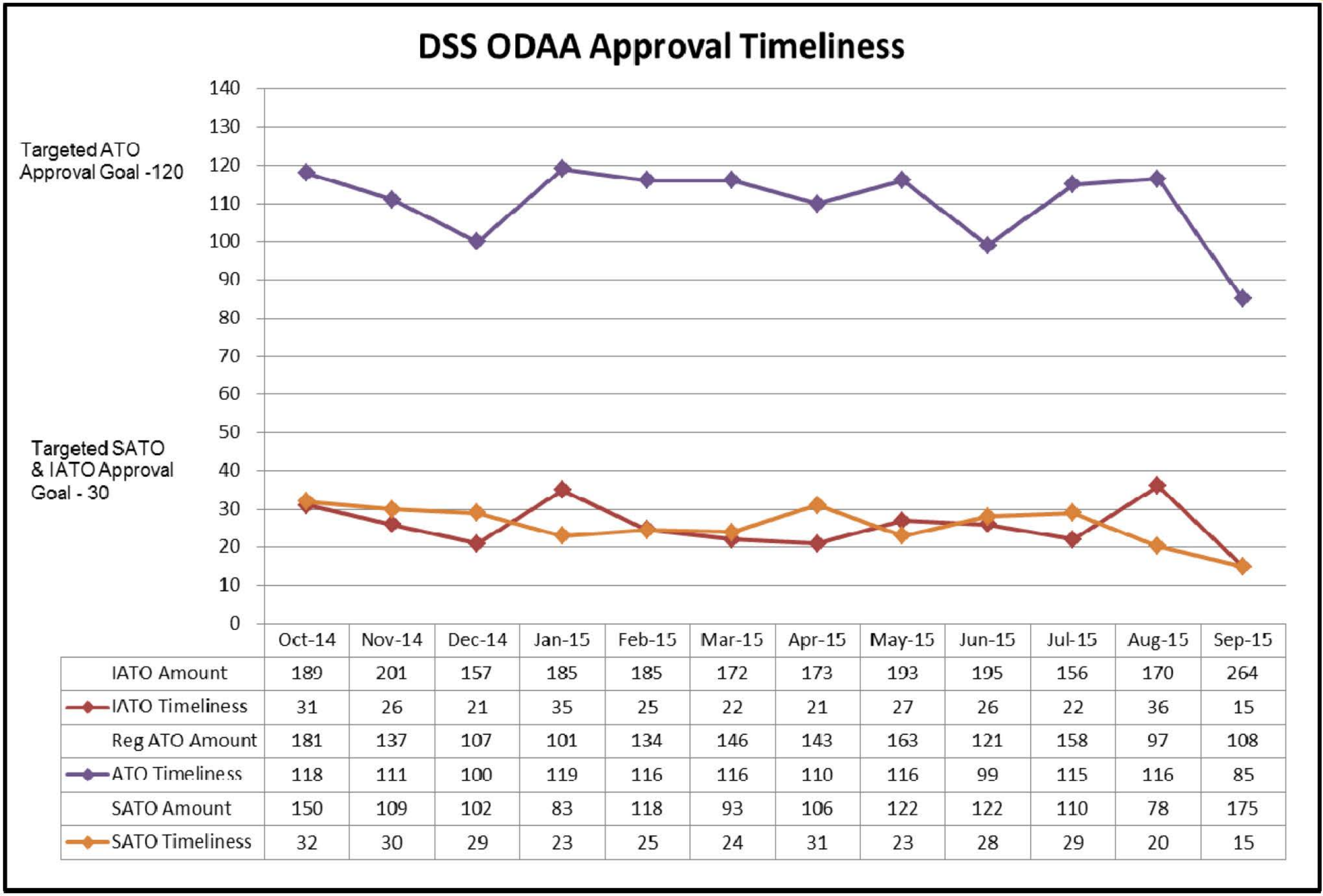
NISPPAC C&A Working Group Update for the Committee

September 2015

Working Group Initiatives

- Integrating other CSAs into the WG to establish an overall NISP C&A picture and ensure reciprocal processes are in place. Initial request for a review of their processes and metrics has been sent.
- Reviewing supporting artifacts for Risk Management Framework (RMF) transition within the NISP.
- We will be revisiting reporting criteria during RMF transition.

ISFO – ODAA



DSS ODAA Approval Timeliness

Targeted ATO Approval Goal -120

Targeted SATO & IATO Approval Goal - 30

	Oct-14	Nov-14	Dec-14	Jan-15	Feb-15	Mar-15	Apr-15	May-15	Jun-15	Jul-15	Aug-15	Sep-15
IATO Amount	189	201	157	185	185	172	173	193	195	156	170	264
IATO Timeliness	31	26	21	35	25	22	21	27	26	22	36	15
Reg ATO Amount	181	137	107	101	134	146	143	163	121	158	97	108
ATO Timeliness	118	111	100	119	116	116	110	116	99	115	116	85
SATO Amount	150	109	102	83	118	93	106	122	122	110	78	175
SATO Timeliness	32	30	29	23	25	24	31	23	28	29	20	15

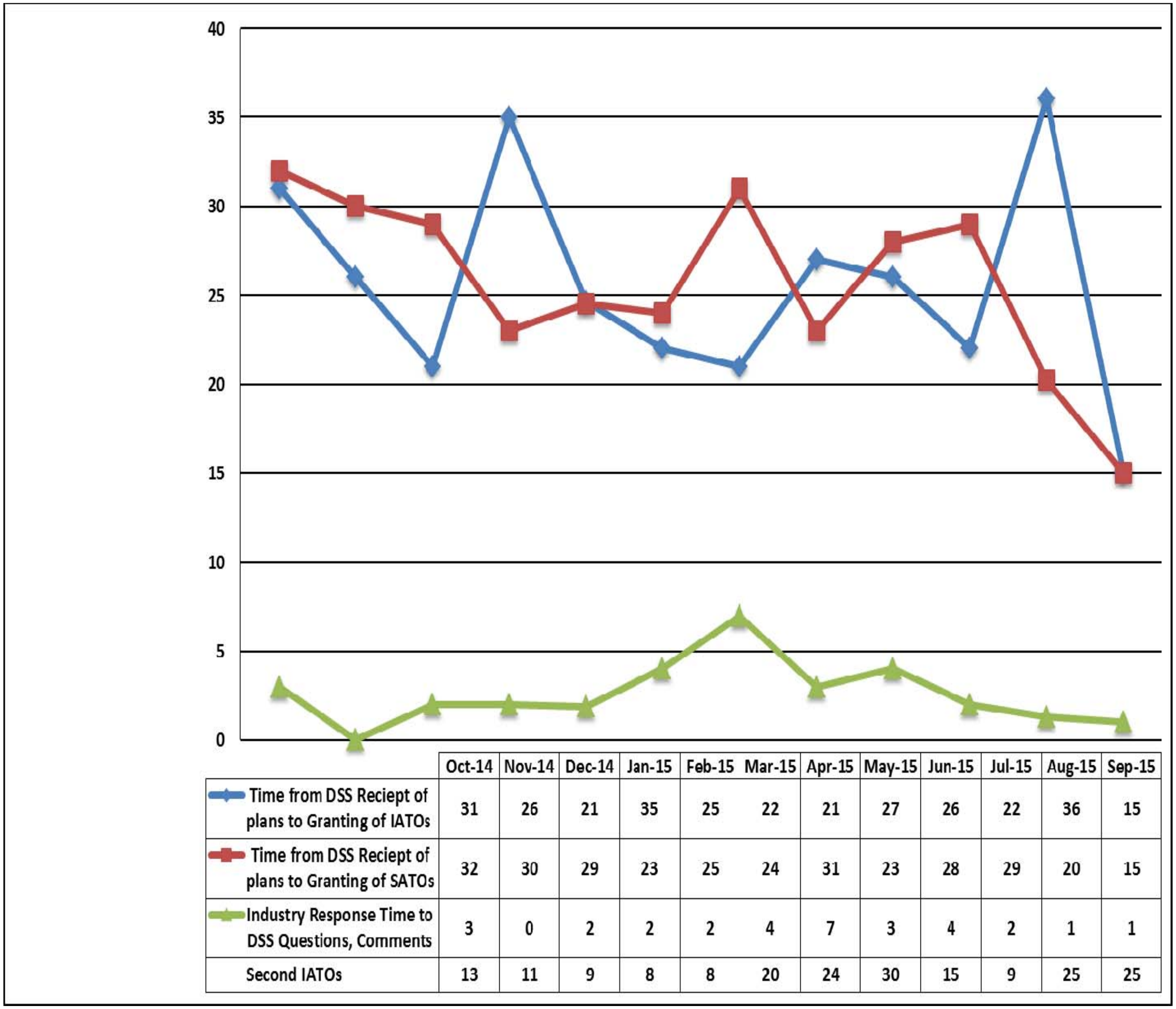
DSS ODAA Business Management System (OBMS) Version 2.3 was deployed in early September 2015.

New functionality enhancements include:

- Contractor Submitter has the option to create UIDs or have the UID auto-generated by OBMS for Initial Accreditations.
- Ability to add Program Name to IS Profile
- Auto-generated Expiration Notifications (30, 60, 90 days)
- Canned Reports
  - Facility Report
  - Self-Certified Report
  - Pending Report

Back-Up Slides

Security Plan Review Results from Oct 2014- Sept 2015



	Oct-14	Nov-14	Dec-14	Jan-15	Feb-15	Mar-15	Apr-15	May-15	Jun-15	Jul-15	Aug-15	Sep-15
◆ Time from DSS Reciept of plans to Granting of IATOs	31	26	21	35	25	22	21	27	26	22	36	15
■ Time from DSS Reciept of plans to Granting of SATOs	32	30	29	23	25	24	31	23	28	29	20	15
▲ Industry Response Time to DSS Questions, Comments	3	0	2	2	2	4	7	3	4	2	1	1
Second IATOs	13	11	9	8	8	20	24	30	15	9	25	25

3596 System security plans (SSPs) were accepted and reviewed during the preceding 12 months.

2240 Interim approvals to operate (IATOs) were issued during the preceding 12 month period, it took an average of 25 days to issue an IATO after a plan was submitted.

1368 “Straight to ATO (SATO)” were processed during the preceding 12 months, it took an average of 26 days to issue the ATO.

852 of the SSPs (24%) required some level of correction prior to conducting the onsite validation.

628 of the SSPs (17%) were granted IATO with corrections required.

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

Denials: 162 of the SSPs (5%) were received and reviewed, but denied IATO until corrections were made to the plan.

Rejections: 17 of the SSPs (1%) 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: September 2015

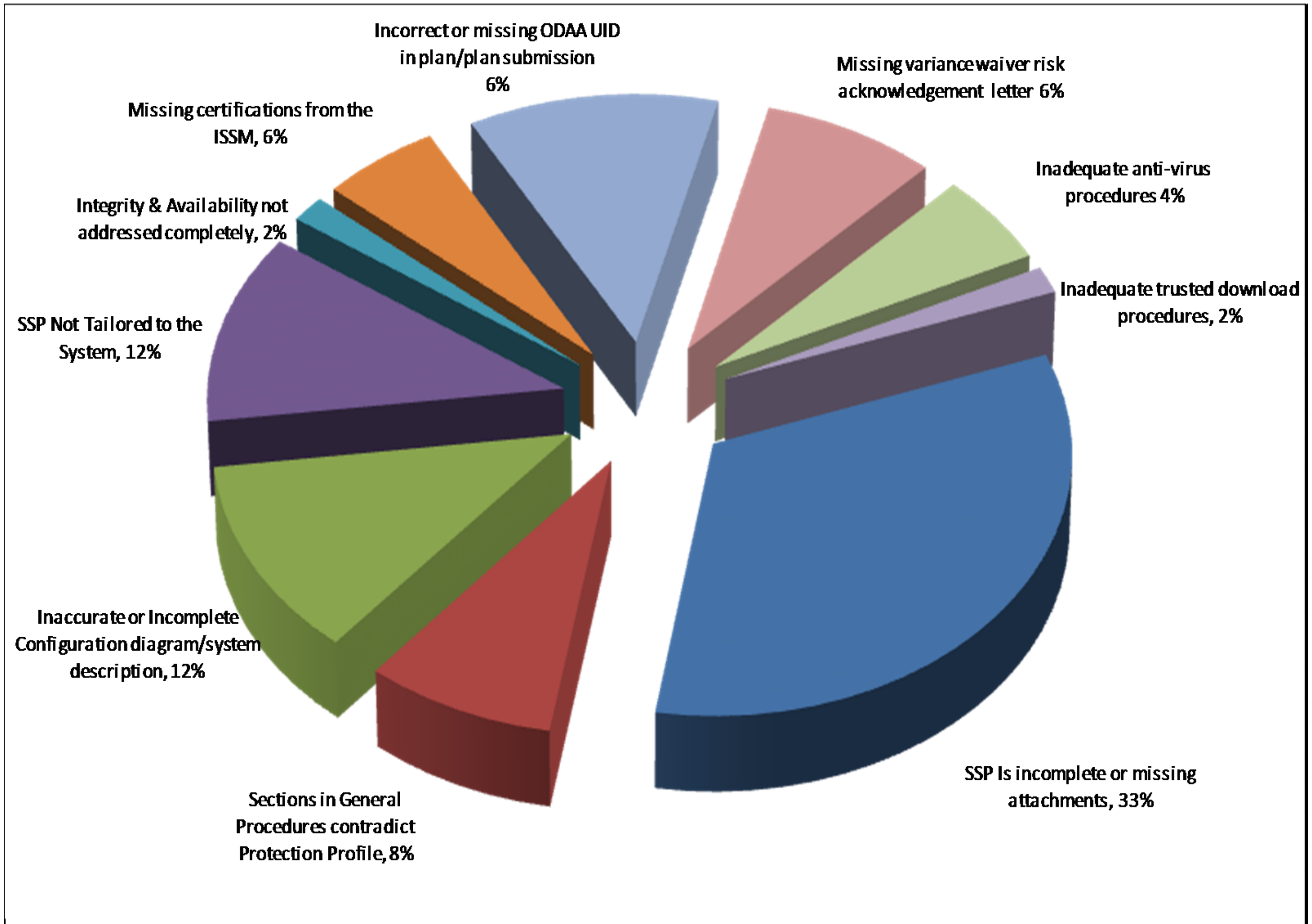
264 IATOs were granted with an average turnaround time of 15 days

175 SATOs were granted with an average turnaround time of 15 days

NISPPAC C&A Working Group

Sept 2015

Common Deficiencies in Security Plans from Oct 2014- Sept 2015



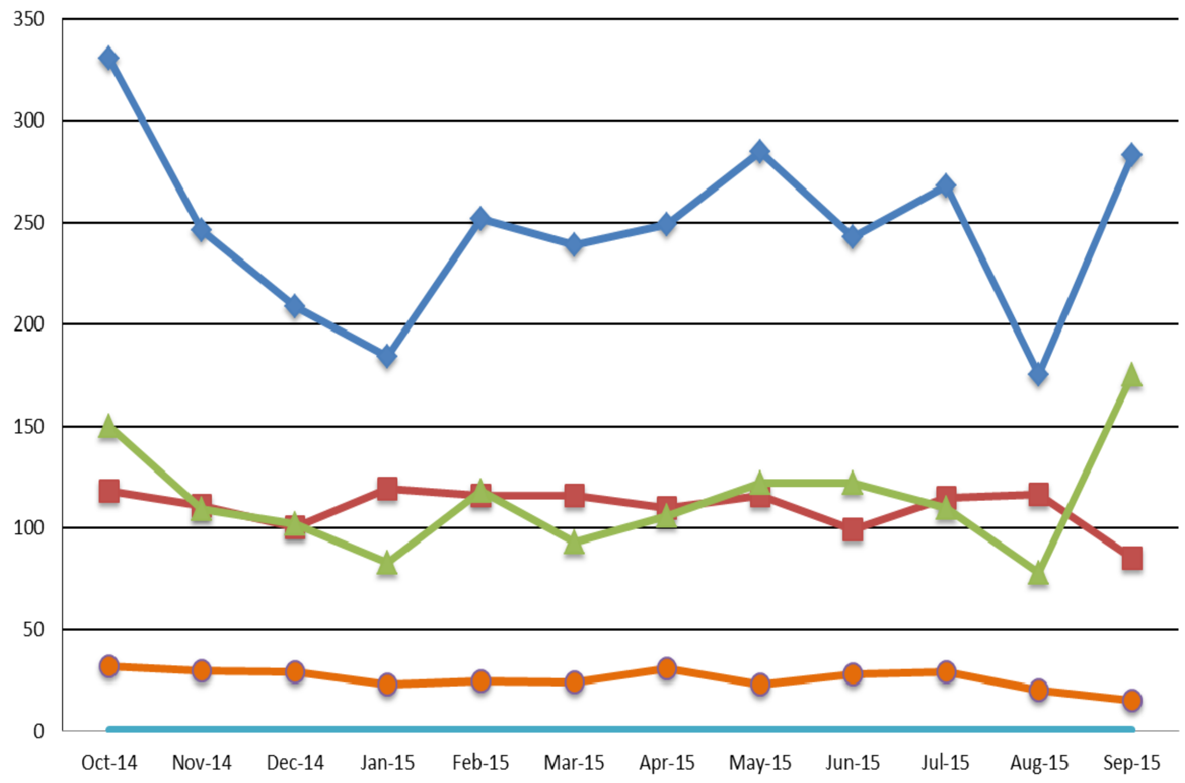
	Oct-14	Nov-14	Dec-14	Jan-15	Feb-15	Mar-15	Apr-15	May-15	Jun-15	Jul-15	Aug-15	Sep-15
# Deficiencies	137	128	101	162	122	106	94	108	88	86	73	73
# Plans w/ Deficiencies	95	109	64	81	75	63	50	76	65	53	69	69
# Plans Reviewed	357	322	279	286	309	281	298	331	329	280	262	262
Avg Deficiency per Plan	0.38	0.40	0.36	0.57	0.39	0.38	0.32	0.33	0.27	0.31	0.28	0.28
Denials	18	12	17	14	5	14	17	15	10	12	14	14
Rejections	0	0	3	4	1	2	2	1	2	2	0	0

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 Oct 2014- Sept 2015

Performance: Metrics reflect excellent performance across the C&A program nationwide. Improvements have been made in the number of systems processed straight ATO and reducing the number of days systems operate on an IATO when compared to six months ago. We are averaging over 45% of all ATOs being straight to ATO.



	Oct-14	Nov-14	Dec-14	Jan-15	Feb-15	Mar-15	Apr-15	May-15	Jun-15	Jul-15	Aug-15	Sep-15
Total ATOs	331	246	209	184	252	239	249	285	243	268	175	283
Avg Days to Reg ATO	118	111	100	119	116	116	110	116	99	115	116	85
Total SATOs	150	109	102	83	118	93	106	122	122	110	78	175
Avg Days to SATO	32	30	29	23	25	24	31	23	28	29	20	15
% SATO's	45%	44%	49%	45%	47%	39%	43%	43%	50%	41%	45%	62%

2756 completed validation visits we completed during the preceding 12 months

1596 systems were processed from IATO to ATO status during the preceding 12 months, it took 111 days on average to process a system from IATO to ATO

1368 systems were processed Straight to ATO status during the preceding 12 months, it took 26 days on average to process a system Straight to ATO

Across the 12 months, (46%) of ATOs were for systems processed Straight to ATO

2147 systems (78%) had no vulnerabilities identified.

574 systems (21%) had minor vulnerabilities identified that were corrected while onsite.

35 systems (1%) had significant vulnerabilities identified, resulting in a second validation visit to the site after corrections were made.

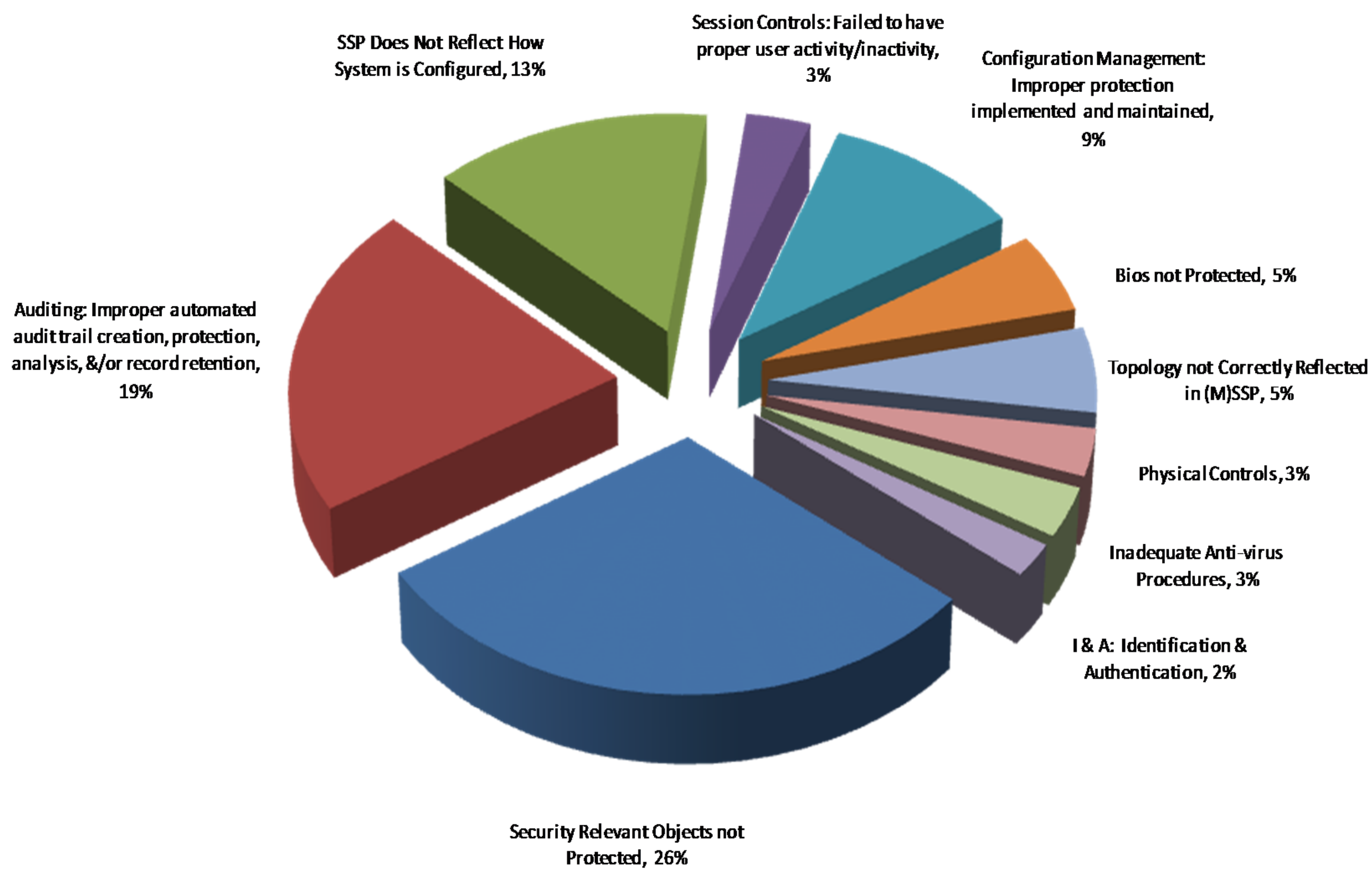
Last Months Snapshot: Sept 2015
108 ATOs were granted with an average turnaround time of 85 days

175 SATOs were granted with an average turnaround time of 15 days

NISPPAC C&A Working Group

Sept 2015

Common Vulnerabilities found during System Validations from Oct 2014- Sept 2015

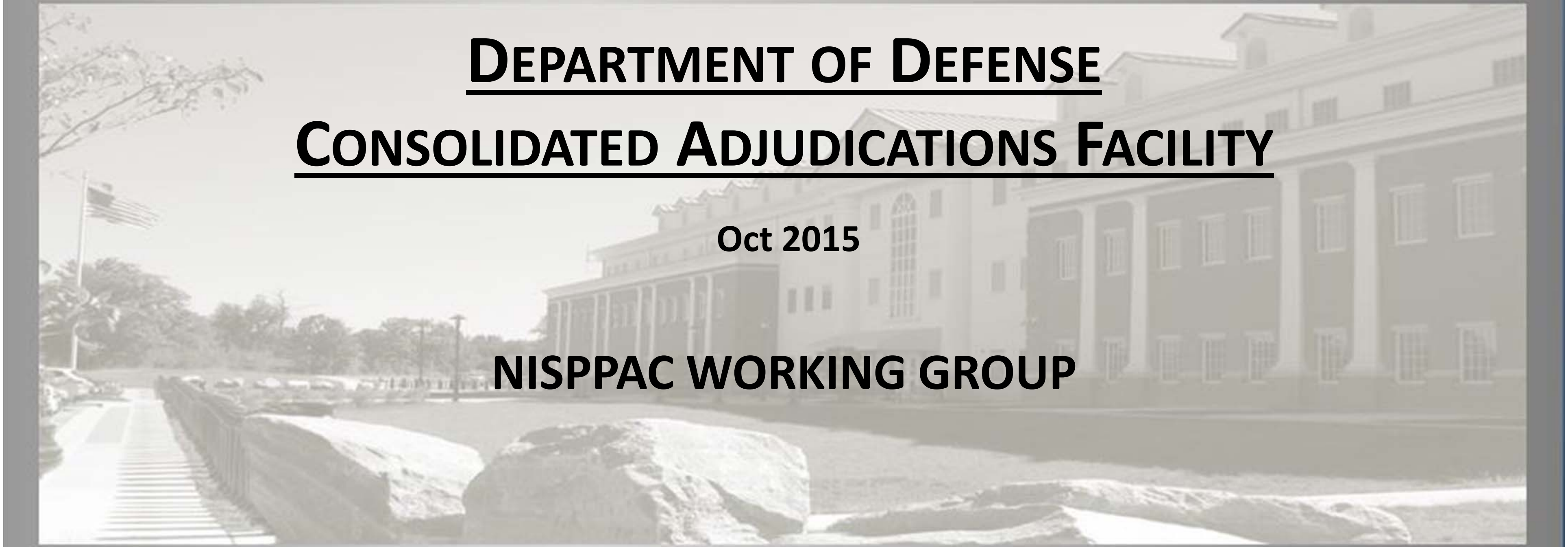


	Oct-14	Nov-14	Dec-14	Jan-15	Feb-15	Mar-15	Apr-15	May-15	Jun-15	Jul-15	Aug-15	Sep-15
# Vulnerabilities	121	60	48	65	71	51	64	61	52	51	30	30
# Onsites w/ vulnerabilities	108	66	44	44	49	37	53	54	56	46	26	26
# Onsites	327	226	192	171	253	229	238	276	235	271	169	169
Avg Vulnerability per Onsite	0.37	0.27	0.25	0.38	0.28	0.22	0.27	0.22	0.22	0.19	0.18	0.18

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. Inadequate configuration management
5. Improper session controls: Failure to have proper user activity/inactivity, logon, system attempts enabled.
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 #5



DEPARTMENT OF DEFENSE

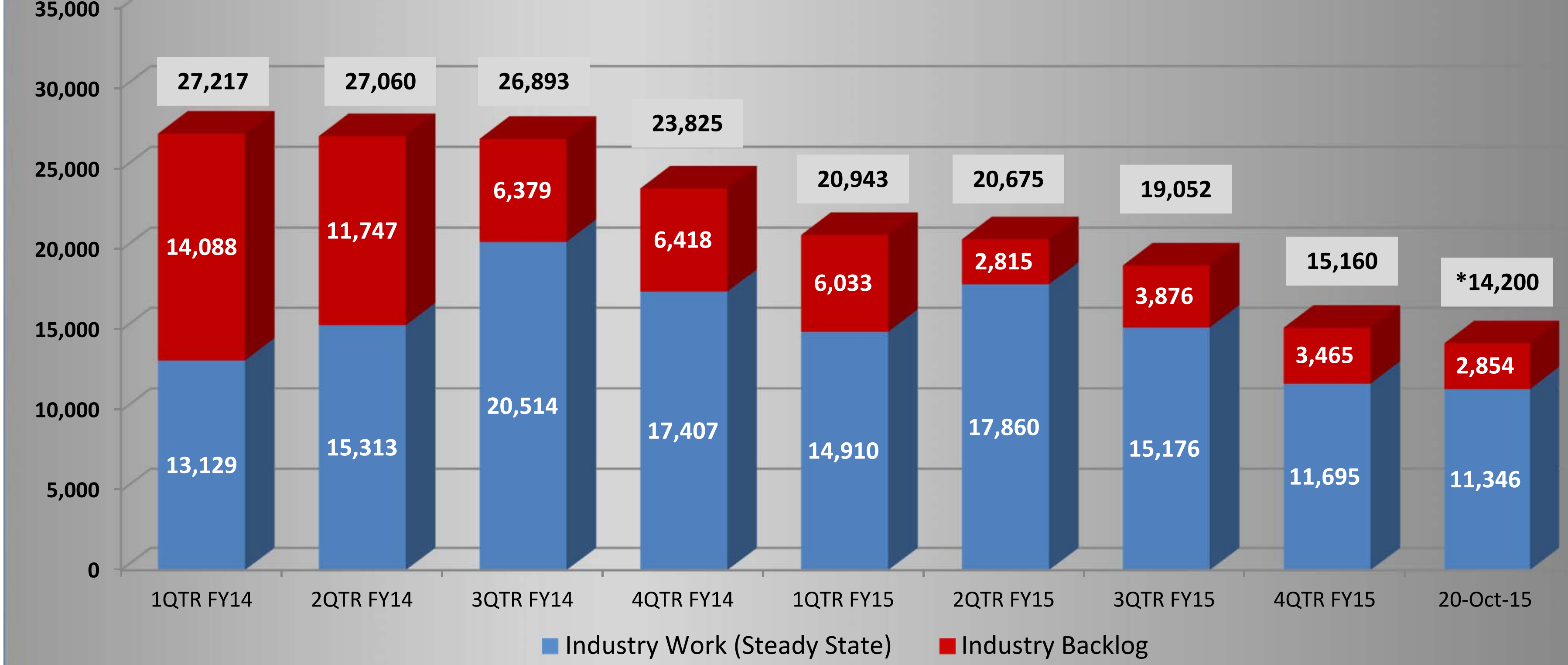
CONSOLIDATED ADJUDICATIONS FACILITY

Oct 2015

NISPPAC WORKING GROUP

Pending Industrial Workload

Backlog reduced by ~75% since CAF consolidation in early-2013



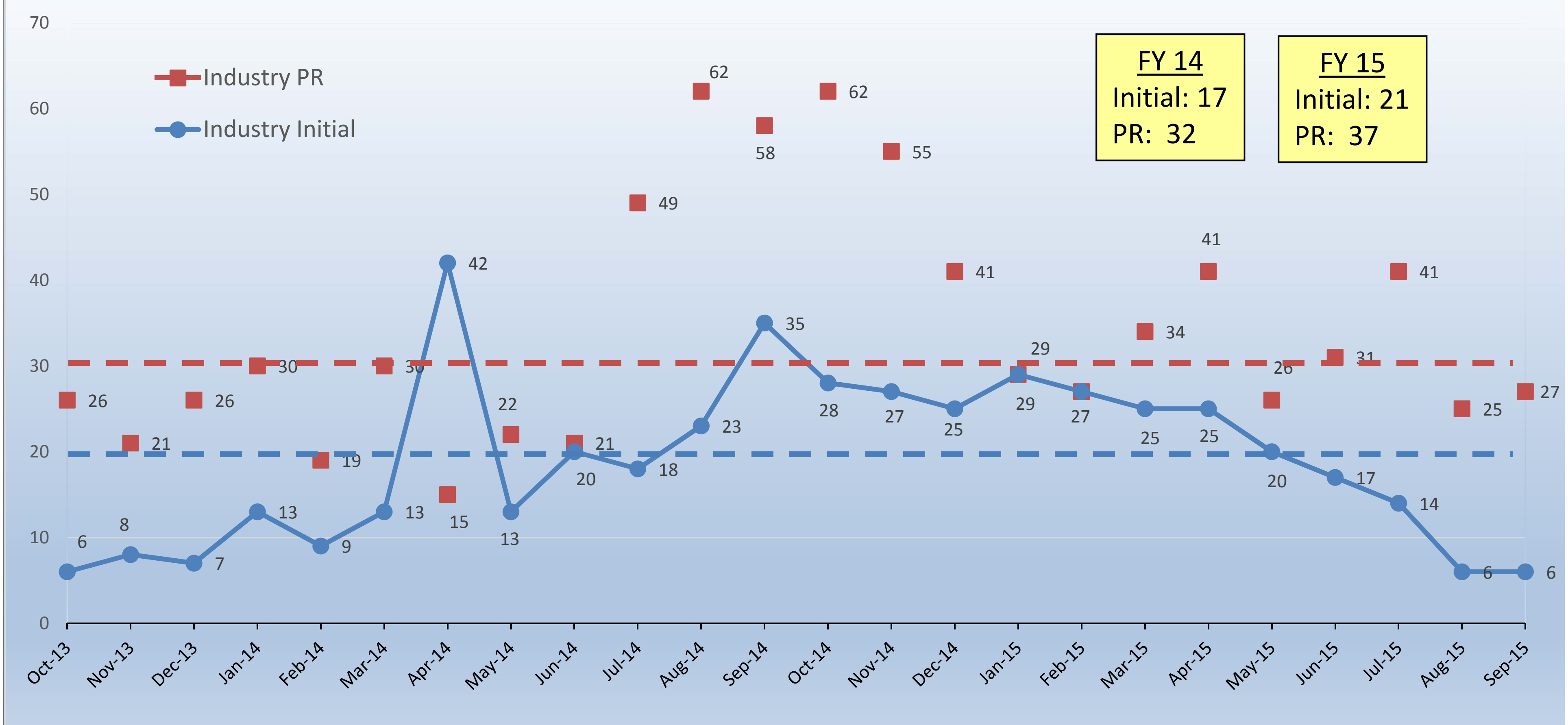
***- Includes Cases Undergoing Legal sufficiency Review**

- **Backlog to be eliminated not earlier than late-FY16**
- **Potential Complications Remain:**
  - **+ CATs v4 Deployment to reduce production by ~20% over 2 mos.**
  - **+ Full impact of CE pilots and implementation not yet realized**
  - **+ FY16-18 – New FIS to both increase workload and possibly reduce e-Adjudication**

Month	NISP Backlog	Annual NISP Receipt	Backlog % of Total NISP
October 13	13,515		8.1%
October 15	2,854		1.6%
	-10,700	~ 180,000	

UNCLASSIFIED

Industry
Intelligence Reform and Terrorism Prevention Act Performance FY14-FY15 to Date



FY 14
Initial: 17
PR: 32

FY 15
Initial: 21
PR: 37

- **FY 15 - Both NISP and non-NISP timeliness metrics fluctuated as backlogs addressed**
- **FY 16 - Timelines to remain more stable, and within IRTPA mandates, as last vestiges of "old"/backlog cases are closed**

DoD CAF
Bldg. 600, 10th Street, FGGM

???

Attachment #6

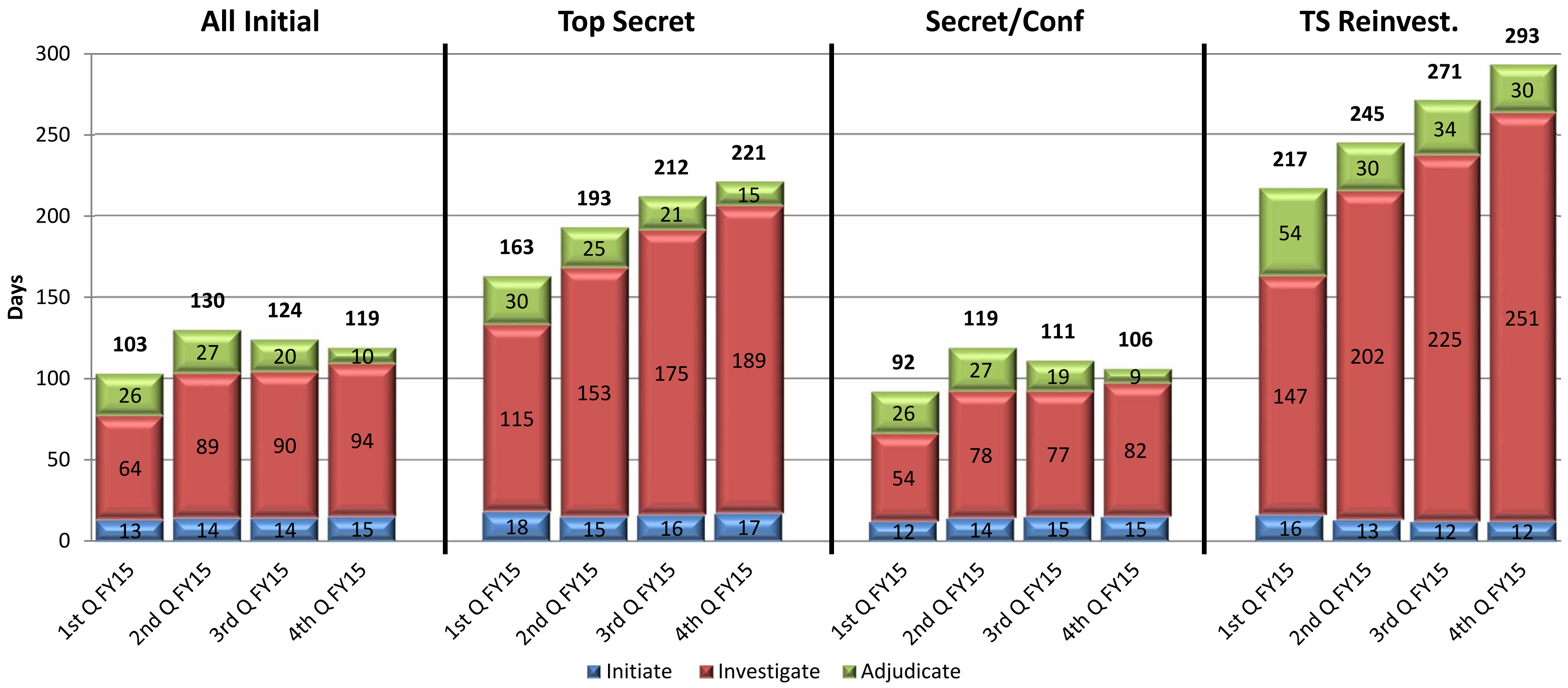
Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

DoD-Industry

November 2015

Quarterly Timeliness Performance Metrics for Submission, Investigation & Adjudication* Time

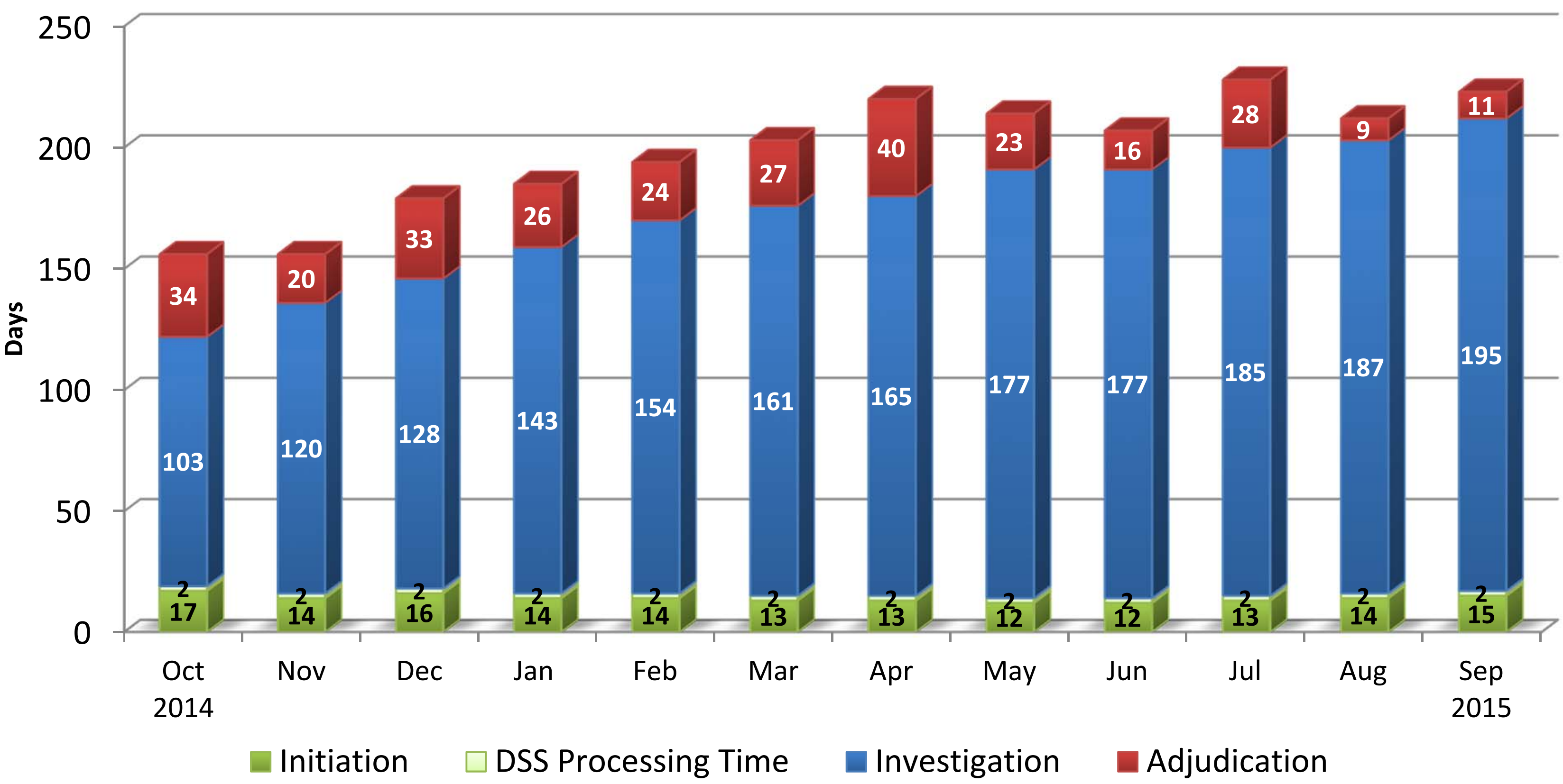
Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 1st Q FY15	18,958	3,118	15,840	8,339
Adjudication actions taken – 2nd Q FY15	18,870	2,984	15,886	7,518
Adjudication actions taken – 3rd Q FY15	20,791	2,906	17,885	7,299
Adjudication actions taken – 4th Q FY15	21,047	2,597	18,450	7,357

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

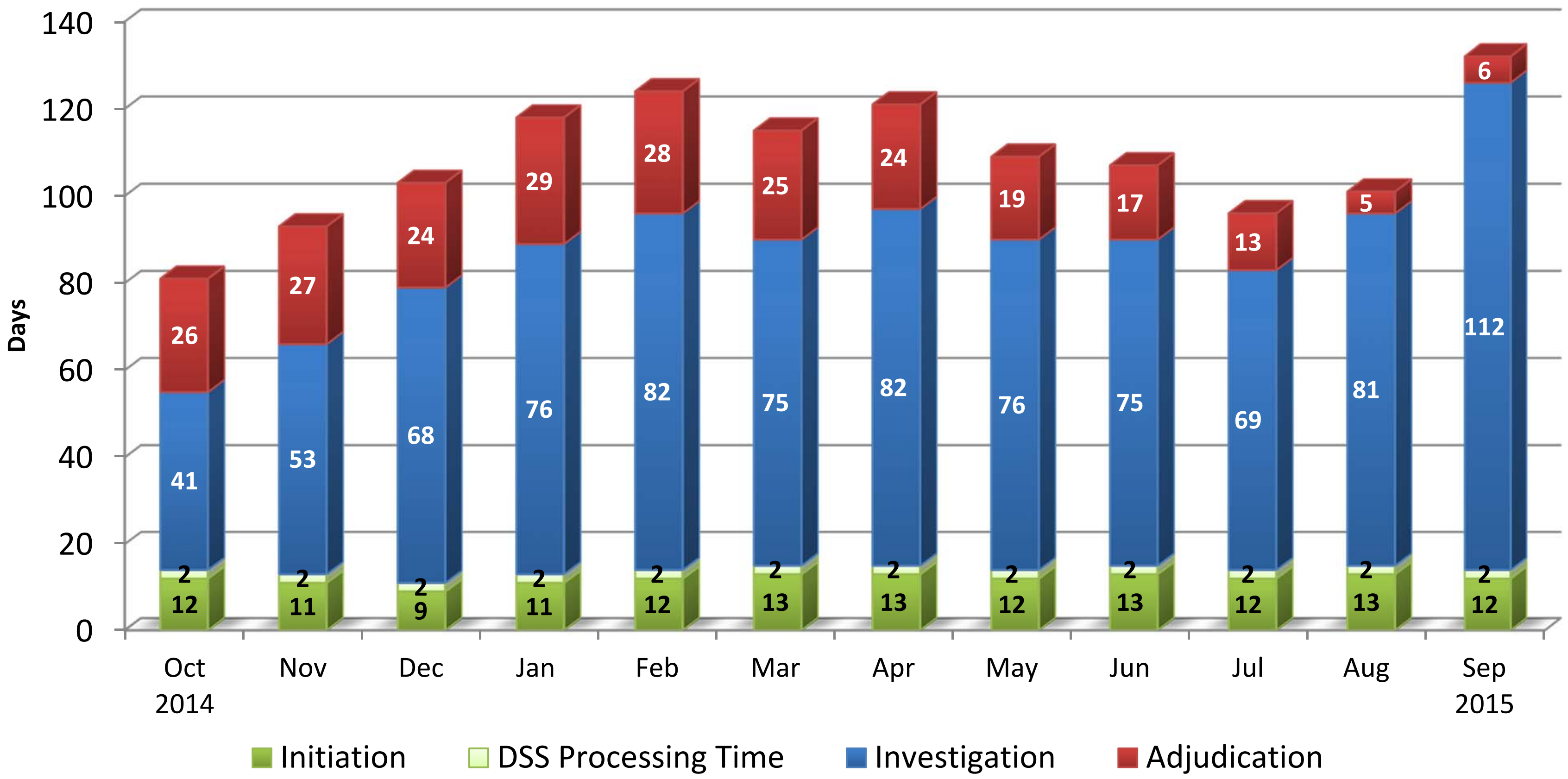
Industry's Average Timeliness Trends for 90%
Initial Top Secret Security Clearance Decisions



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

	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015
100% of Reported Adjudications	1,206	933	983	1,045	988	954	817	966	1,128	838	911	868
Average Days for fastest 90%	156 days	156 days	179 days	185 days	194 days	203 days	220 days	214 days	207 days	228 days	212 days	223 days

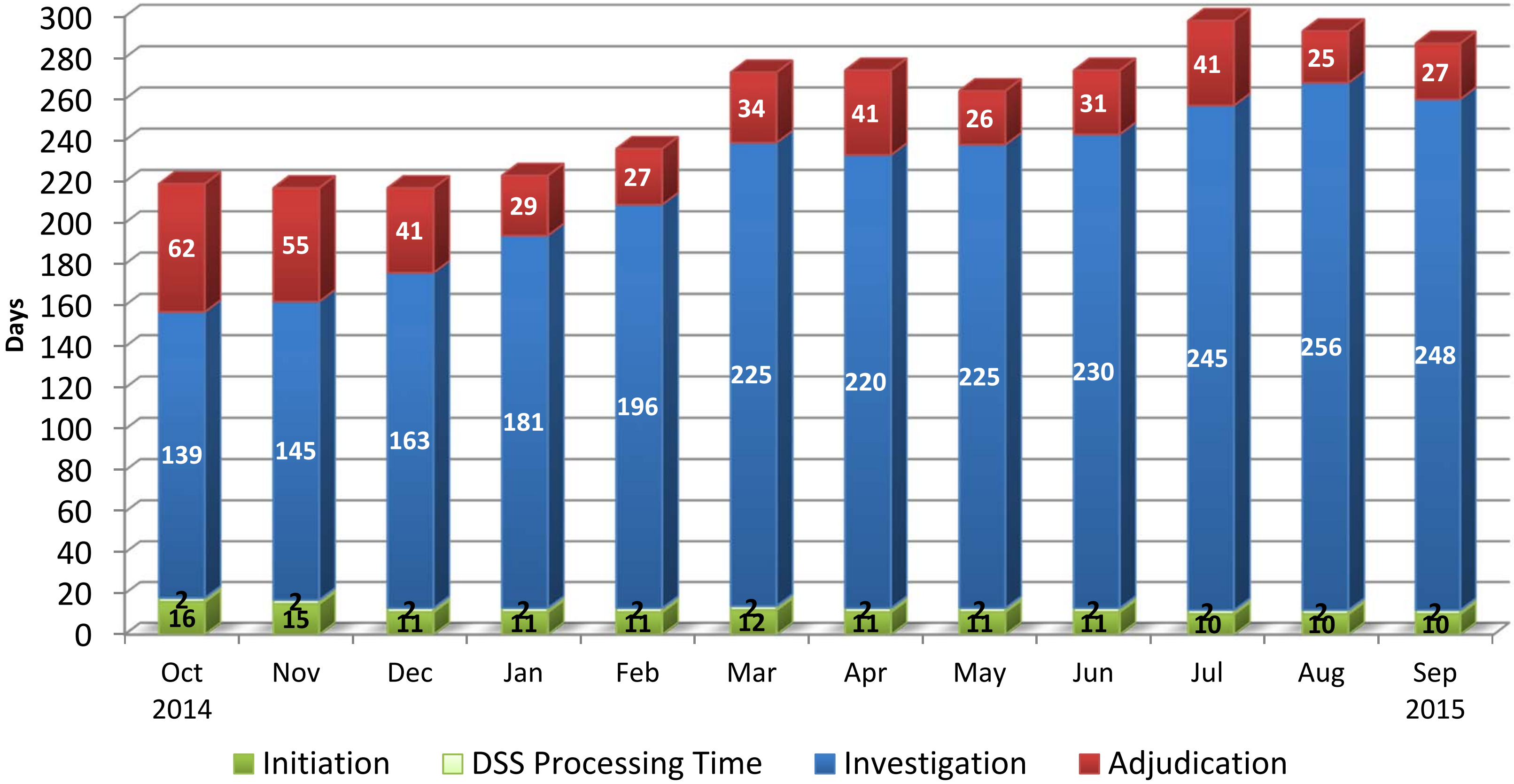
Industry's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



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

	Oct 2014	**Nov 2014**	**Dec 2014**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Apr 2015**	**May 2015**	**Jun 2015**	**Jul 2015**	**Aug 2015**	**Sep 2015**
100% of Reported Adjudications	5,293	4,978	5,579	5,358	4,916	5,620	5,002	5,287	7,602	9,052	5,131	4,272
Average Days for fastest 90%	81 days	93 days	103 days	118 days	124 days	115 days	121 days	109 days	107 days	96 days	101 days	132 days

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

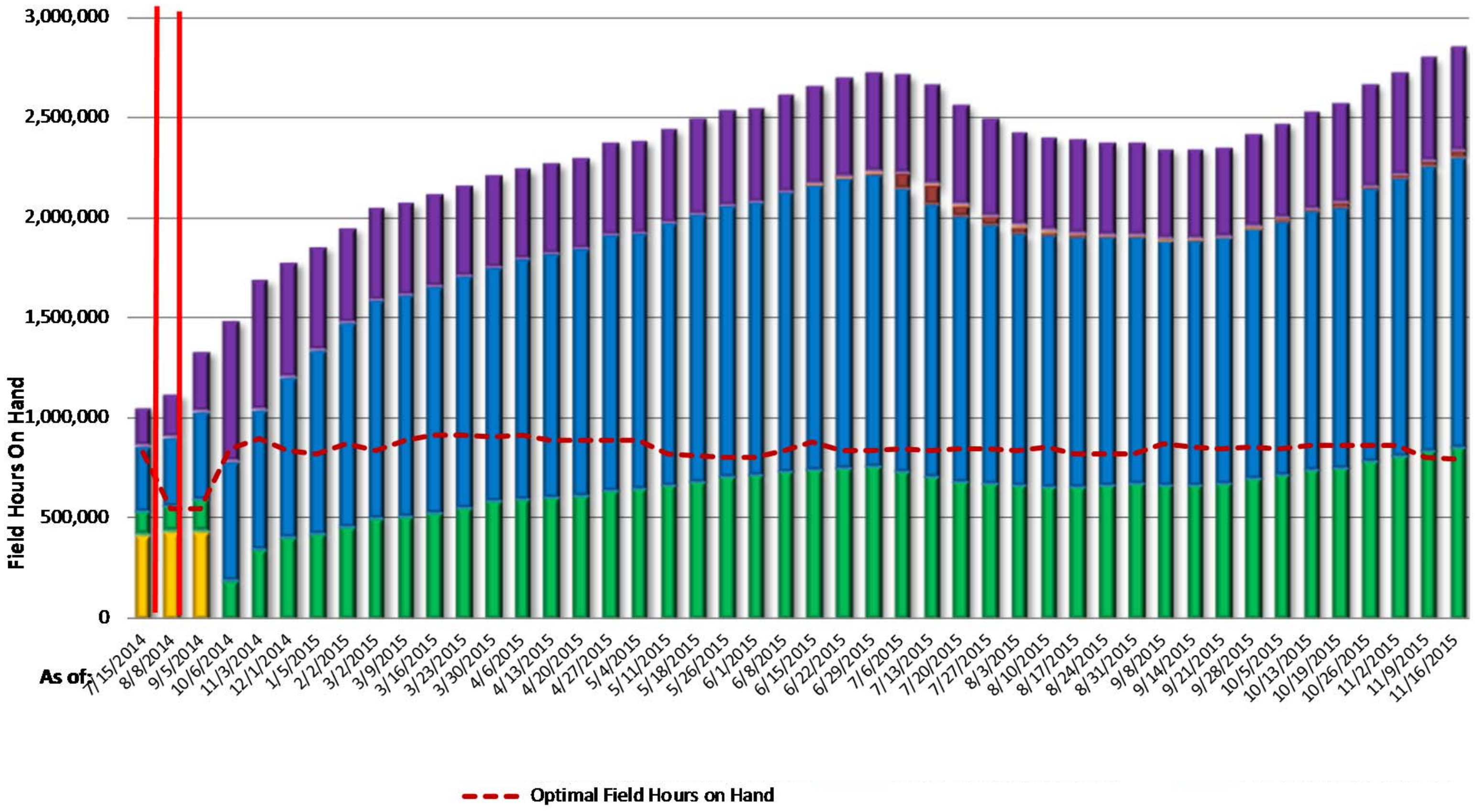


GOAL: Initiation – 14 days ***Investigation – 150 days*** ***Adjudication – 30 days***

	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015
100% of Reported Adjudications	3,079	3,084	2,168	2,321	2,442	2,745	2,597	1,985	2,688	2,233	2,596	2,548
Average Days for fastest 90%	219 days	217 days	217 days	223 days	236 days	273 days	274 days	264 days	274 days	298 days	293 days	287 days

Attachment #6a

Pending Field Hours vs. Optimal



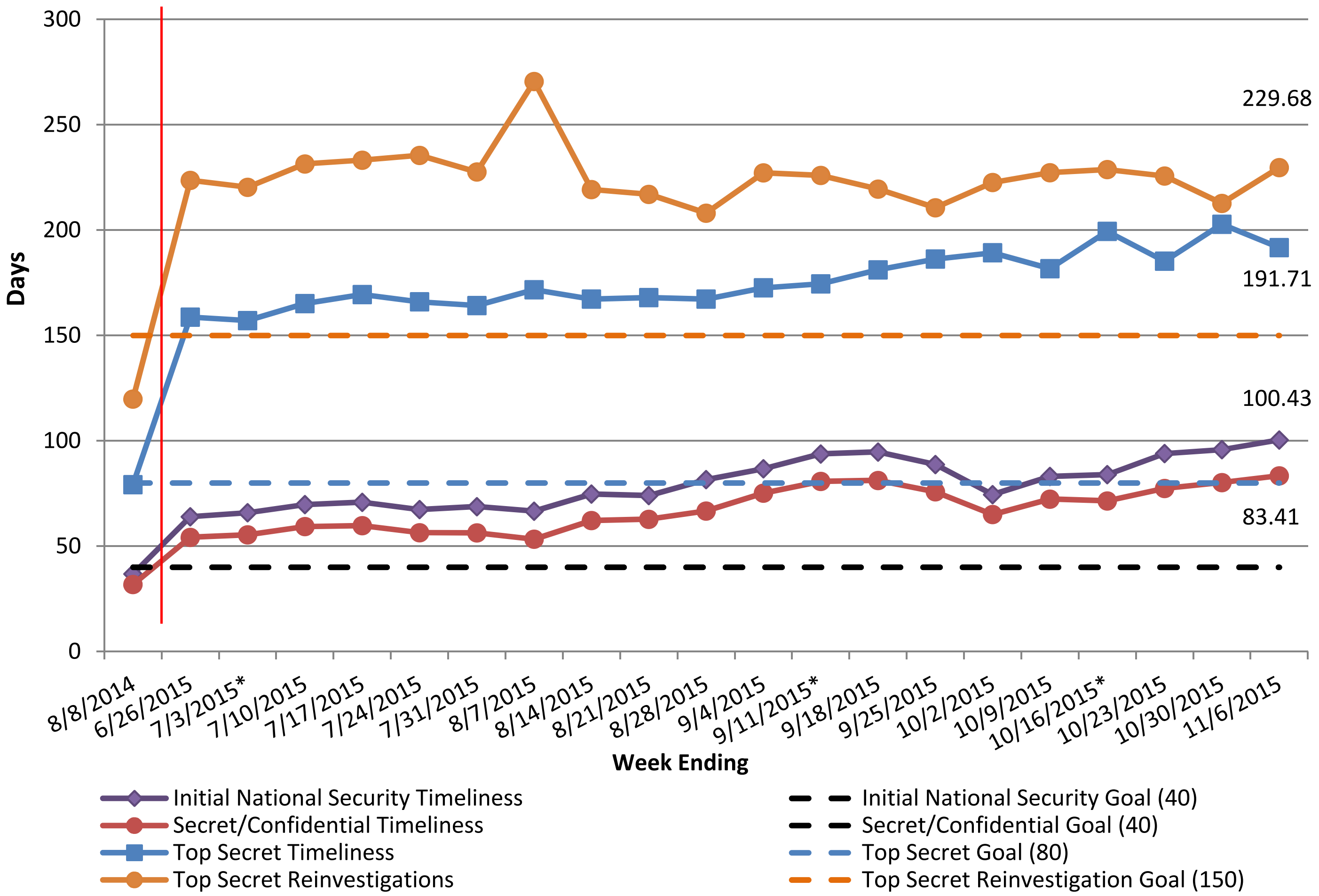
Take-away: After decreasing for seven weeks as a result of the eQIP shutdown, total field hours on hand has continued to increase again. During the past week, total field hours on hand increased from 2,802.3K last week to the current level of 2,854.8K. This represents an increase of 52.5K hours (1.9%). Since the beginning of FY16, total field hours on hand has increased by 382.7K.

Fieldwork Hours On Hand: Sum of the estimated time to complete all pending fieldwork, based on how long on average it takes to complete each item type, submit reports, etc.

Optimal Fieldwork Hours On Hand: Optimal or healthy workload based on current staffing levels. This line shows amount of work that could be completed by all available field resources within 6 weeks. The goal is to have the red line as close as possible to the top of the bar. *The contractors' estimated man hours are provided by the field contractors on a regular basis.*

Timeliness Performance & Standards

Weekly Timeliness (Fastest 90% of Cases)



Top Secret Reinvestigations

FY16

221.88

Top Secret

FY16

189.09

All Initial

FY16

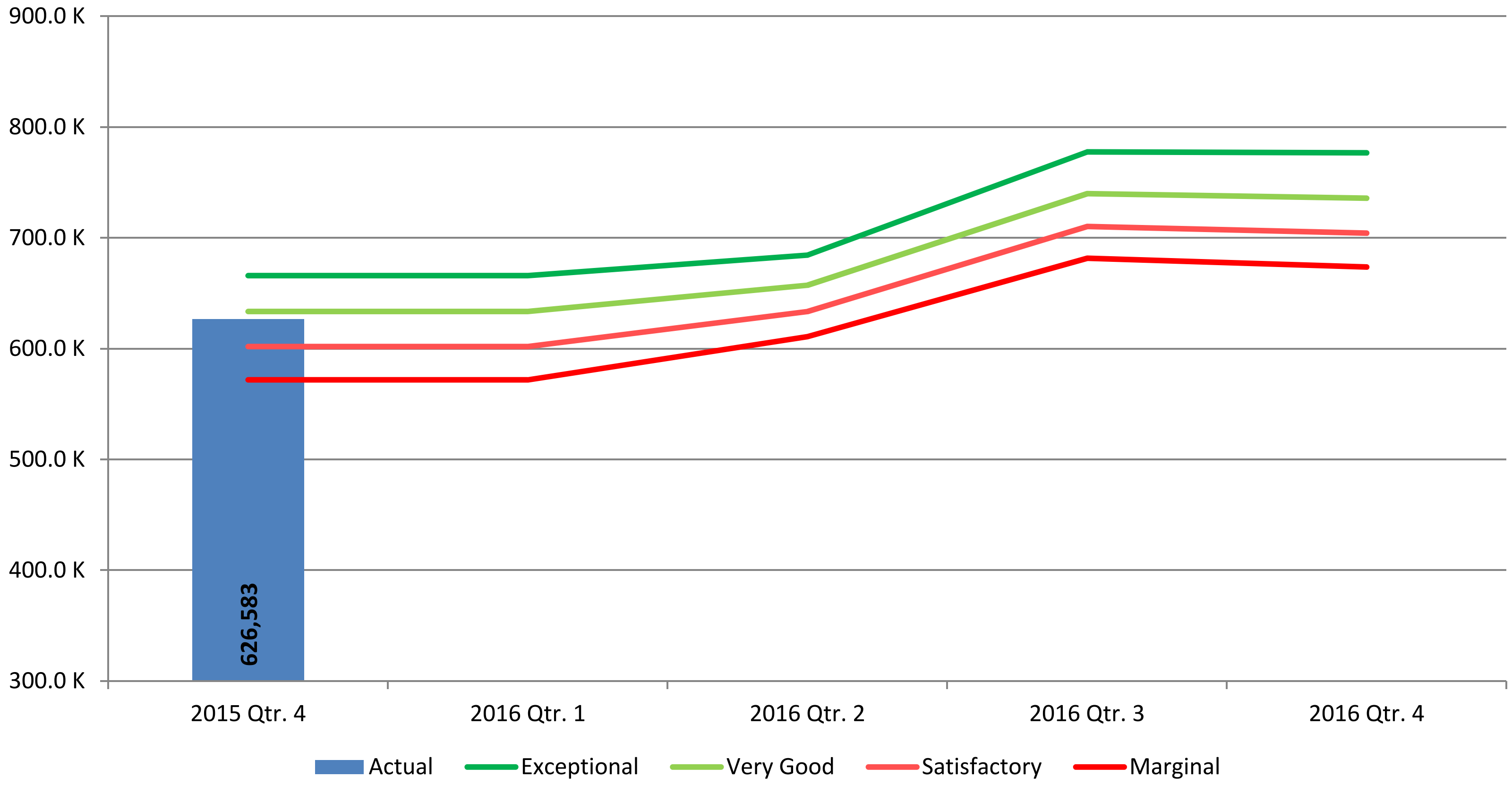
90.07

Sec/Conf

FY16

76.28

Quarterly Contractor Productivity Targets



Attachment #7

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Industry Performance Metrics & Quality Initiative

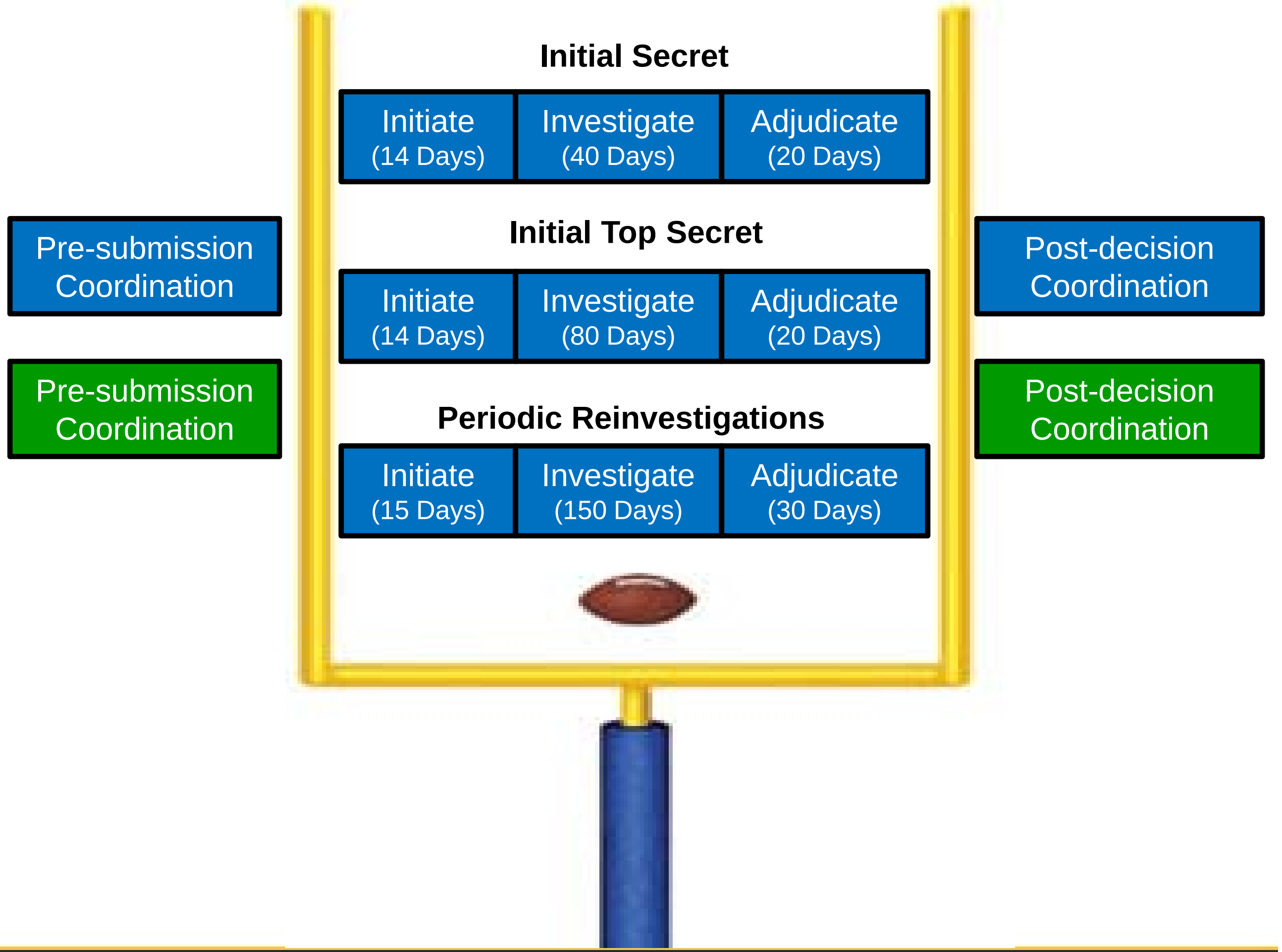
NCSC/Special Security Directorate

LEADING INTELLIGENCE INTEGRATION

18 November 2015

Performance Accountability Council (PAC) Security Clearance Methodology

- Data on the following slides reflects security clearance timeliness performance on Contractor cases. DoD Industry data is provided by OPM and IC Contractor data is provided by the following IC agencies: CIA, DIA, FBI, NGA, NRO, NSA and Dept. of State.
- 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



Pre-submission Coordination

Pre-submission Coordination

Initial Secret

Initiate (14 Days)	Investigate (40 Days)	Adjudicate (20 Days)

Initial Top Secret

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

Periodic Reinvestigations

Initiate (15 Days)	Investigate (150 Days)	Adjudicate (30 Days)

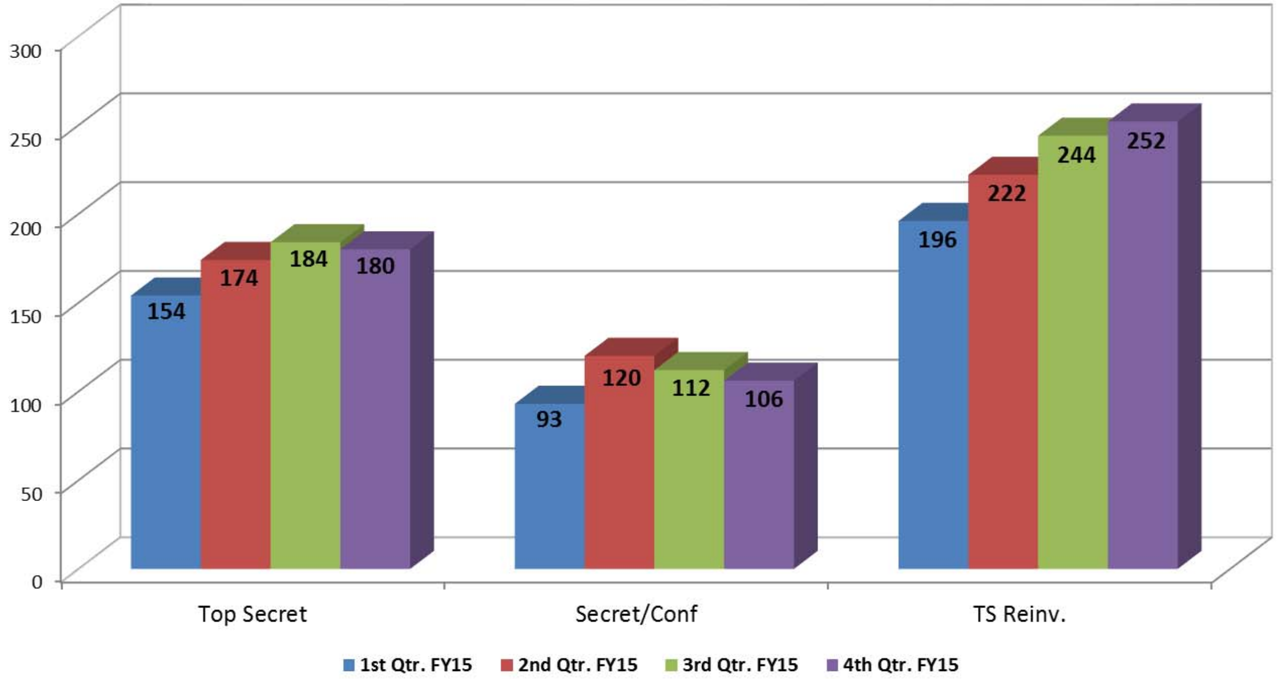
Post-decision Coordination

Post-decision Coordination

Timeliness Performance Metrics for IC/DSS

Industry Personnel Submission, Investigation & Adjudication* Time

Average Days of Fastest 90% of Reported Clearance Decisions Made

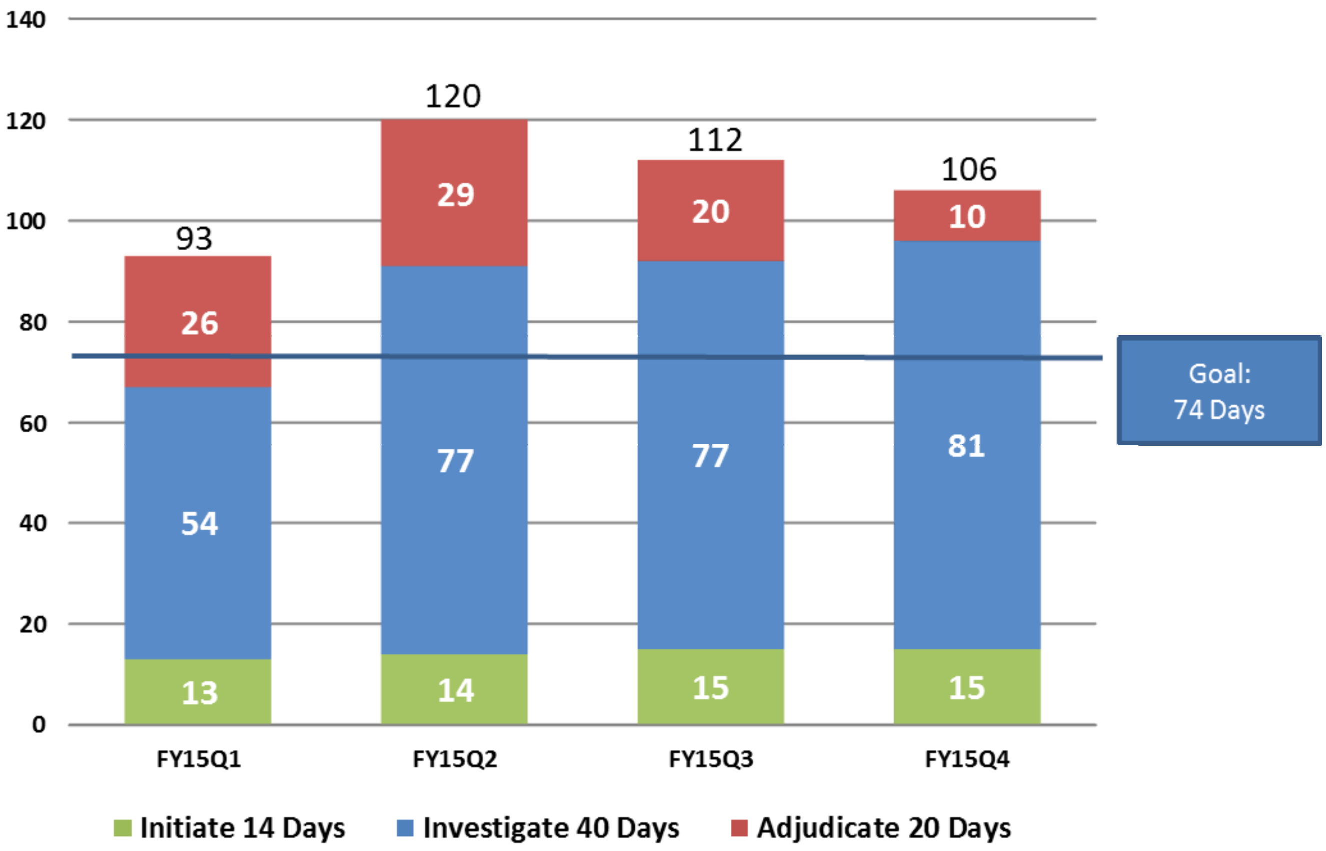


	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken –1st Q FY15	4,253	15,650	9,699
Adjudication actions taken – 2nd Q FY15	4,628	17,938	9,652
Adjudication actions taken – 3rd Q FY15	4,473	20,165	8.827
Adjudication actions taken – 4th Q FY15	4,436	19,007	10,519

*The adjudication timeliness includes collateral adjudication and SCI, if conducted concurrently

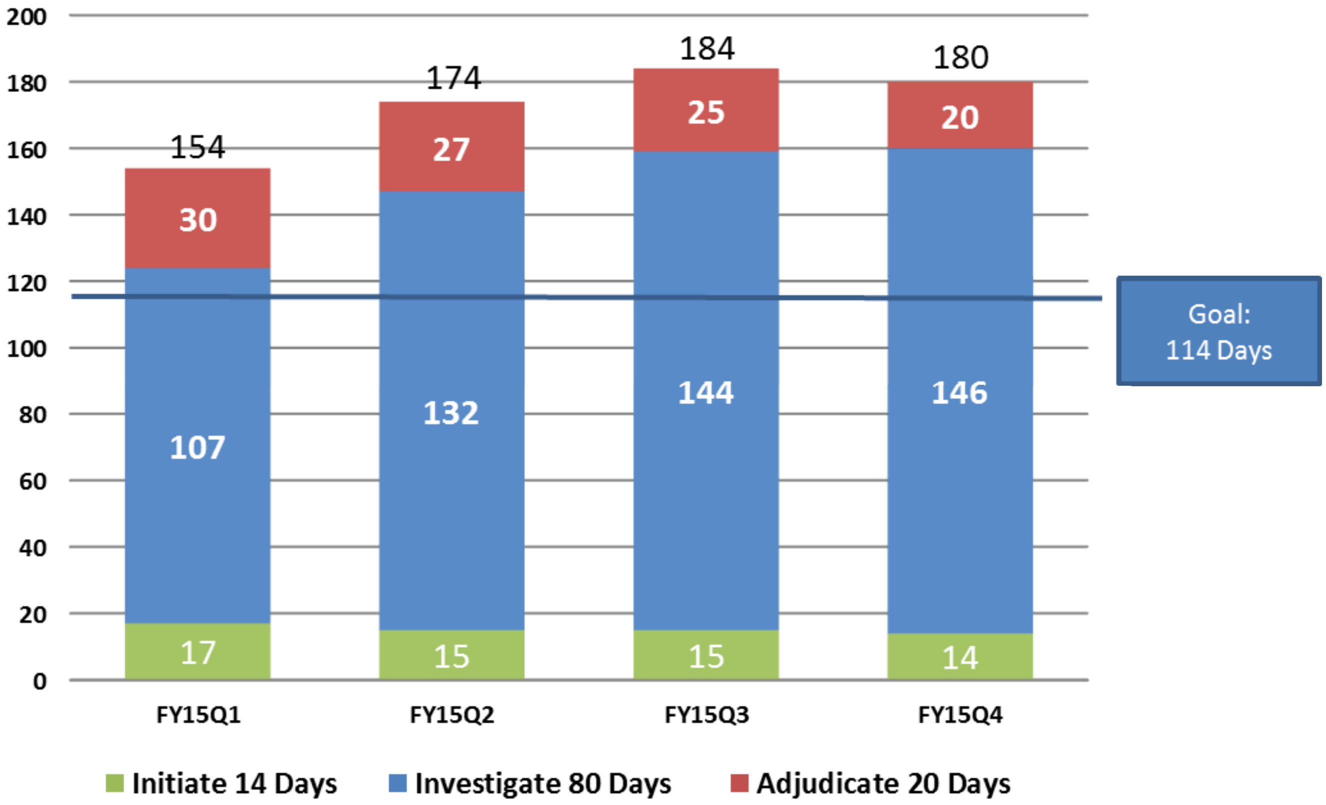
IC and DoD Industry – Secret Clearances

Average Days of Fastest 90% of Reported Clearance Decisions Made



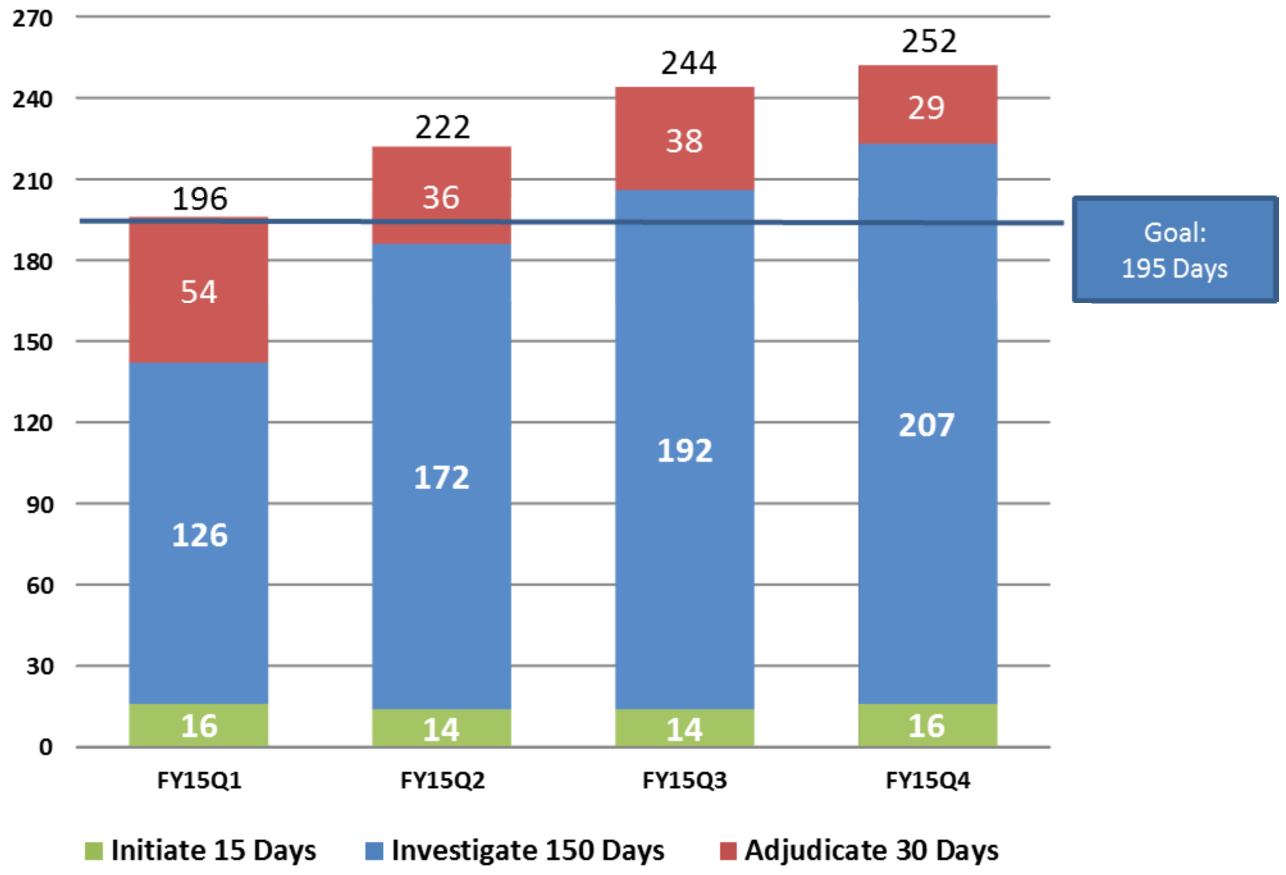
IC and DoD Industry - Top Secret Clearances

Average Days of Fastest 90% of Reported Clearance Decisions Made



IC and DoD Industry - Periodic Reinvestigations

Average Days of Fastest 90% of Reported Clearance Decisions Made



Quality Assessment Standards of Background Investigations

- On 22 January 2015, Quality Assessment Standards (QAS) were distributed to agencies
- QAS codify how to assess investigative quality and establishes consistent quality assessment lexicon
- QAS Implementation Plan to be distributed in the coming months
- Quality Assessment Reporting Tool

For questions, please contact:

Gary Novotny
NCSC/SSD/PSG
Assessments Program Manager
Phone: 301-227-8767
Email: GARYMN@dni.gov

Nilda Figueroa
NCSC/SSD/PSG
Metrics Team Lead
Phone: 301-227-8794
Email: Nilda.Figueroa@dni.gov

Diane Rinaldo
Metrics Team
Phone: 301-227-8778
Email: SecEAmetrics@dni.gov

Attachment #8

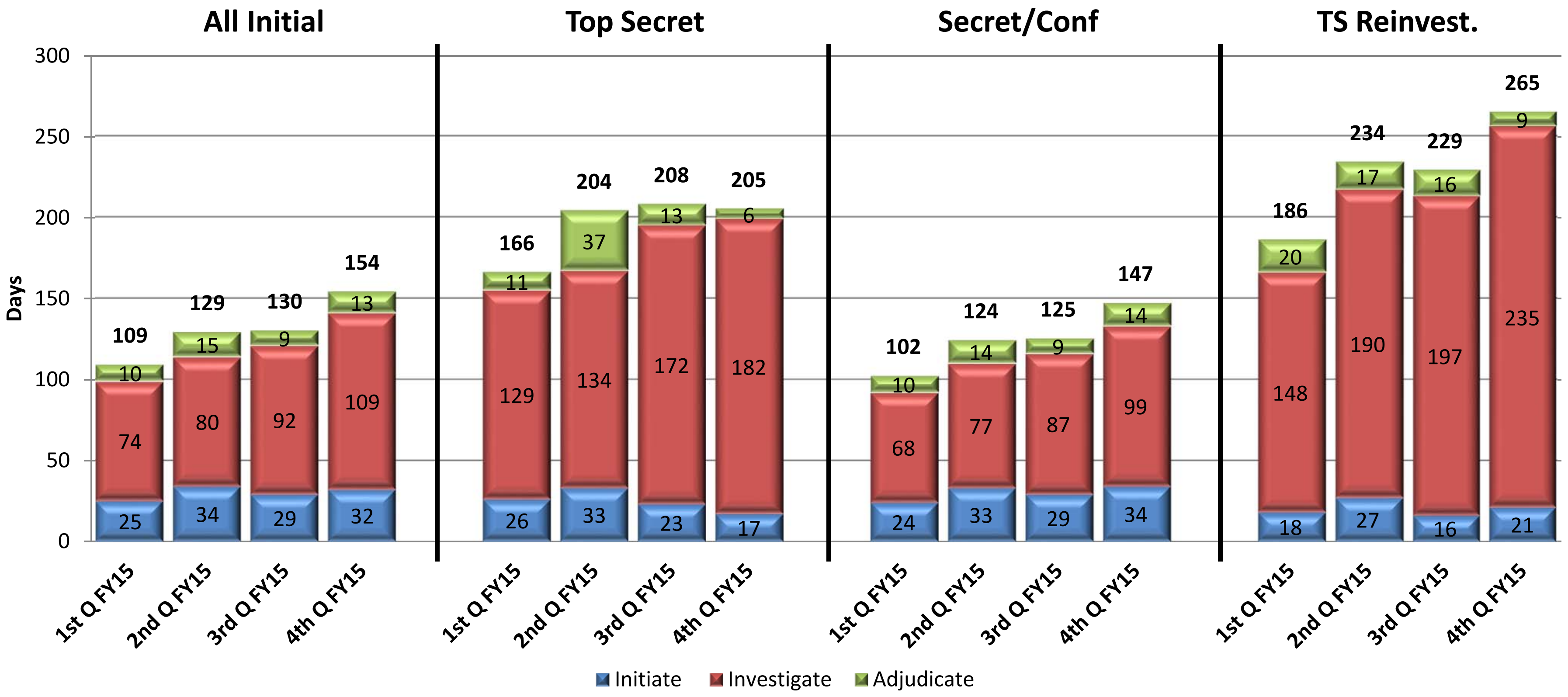
Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

NRC

November 2015

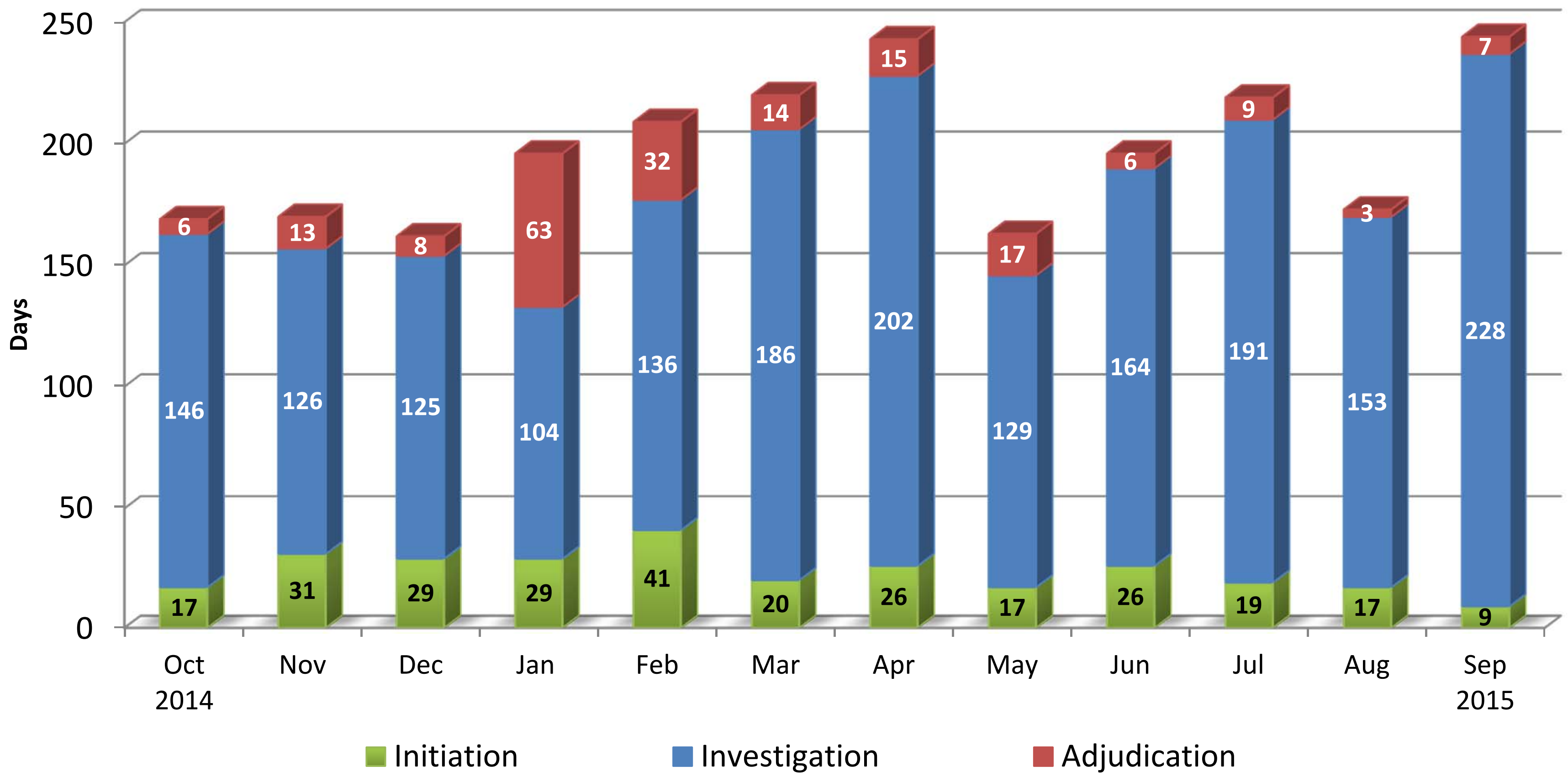
Quaretrly Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 1st Q FY15	1,431	552	879	1,338
Adjudication actions taken – 2nd Q FY15	1,474	527	947	1,488
Adjudication actions taken – 3rd Q FY15	1,706	662	1,044	1,994
Adjudication actions taken – 4th Q FY15	1,768	698	1,070	2,153

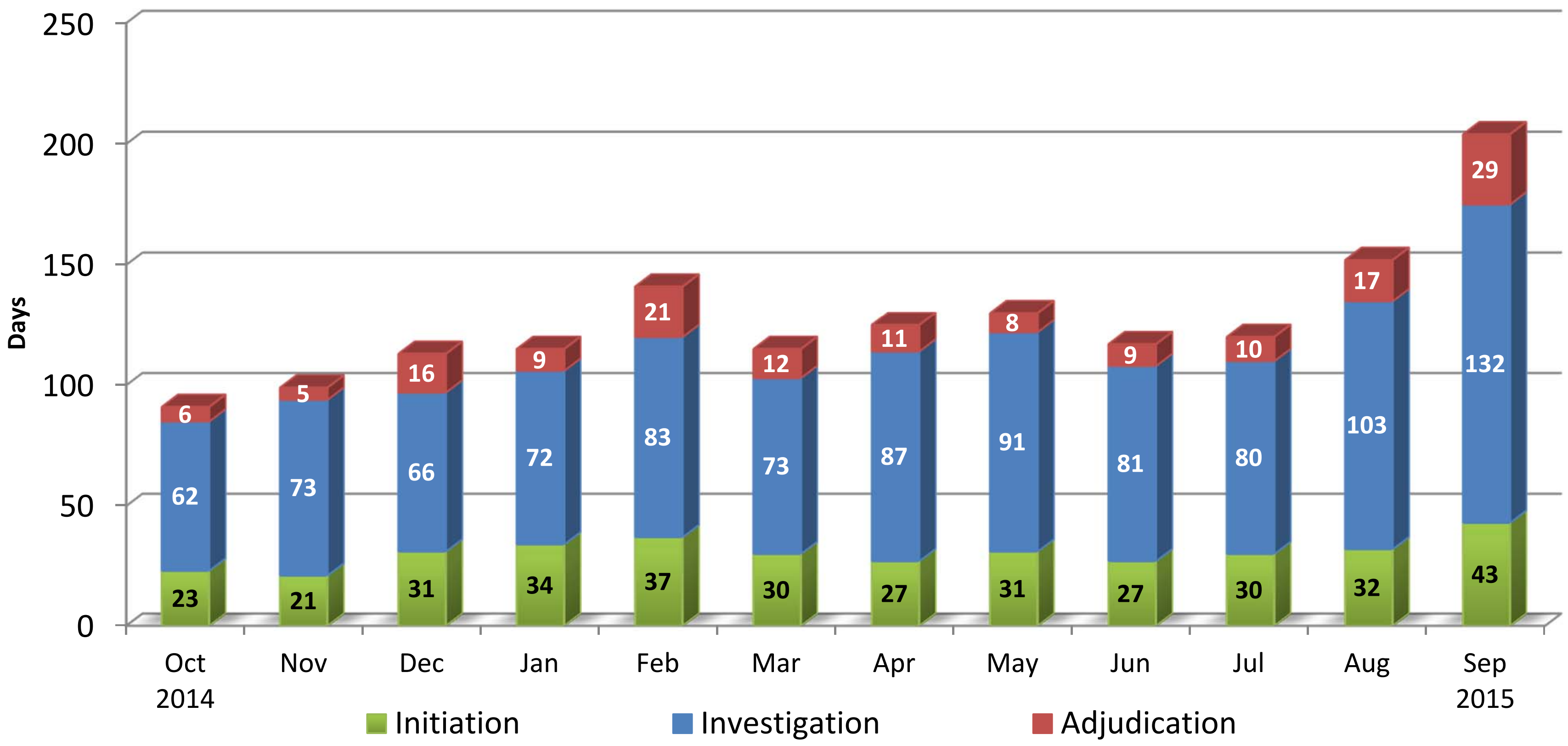
NRC's Average Timeliness Trends for 90%
Initial Top Secret Security Clearance Decisions



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

	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015
100% of Reported Adjudications	6	4	6	2	4	3	6	3	3	7	7	4
Average Days for fastest 90%	169 days	170 days	162 days	196 days	209 days	220 days	242 days	163 days	196 days	219 days	173 days	244 days

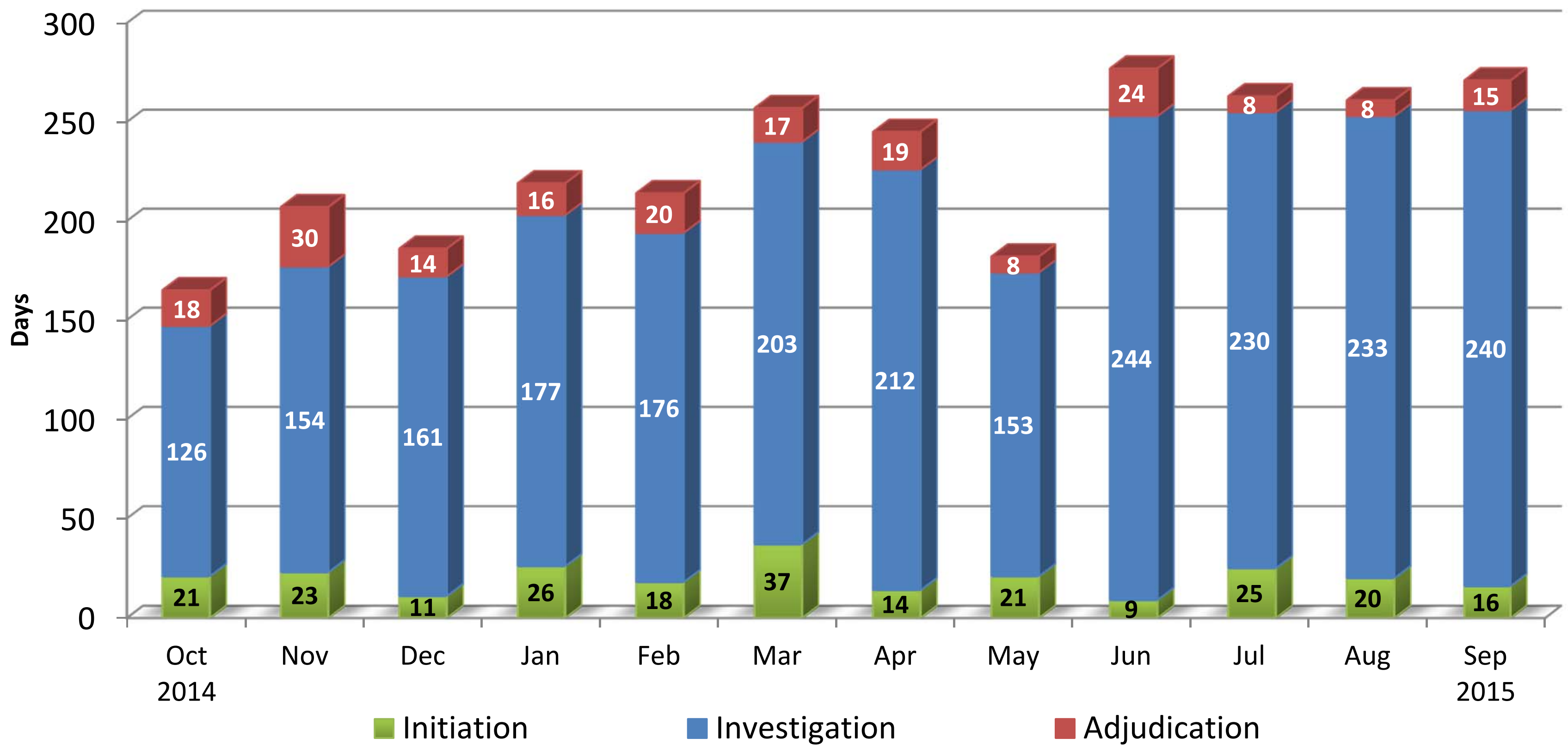
NRC's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



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

	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015
100% of Reported Adjudications	30	40	52	29	39	41	31	60	55	57	39	34
Average Days for fastest 90%	91 days	99 days	113 days	115 days	141 days	115 days	124 days	130 days	117 days	120 days	152 days	204 days

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



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

	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015
100% of Reported Adjudications	6	5	7	8	7	8	12	9	4	10	18	10
Average Days for fastest 90%	165 days	207 days	186 days	219 days	214 days	257 days	245 days	182 days	277 days	263 days	261 days	271 days

Attachment #9

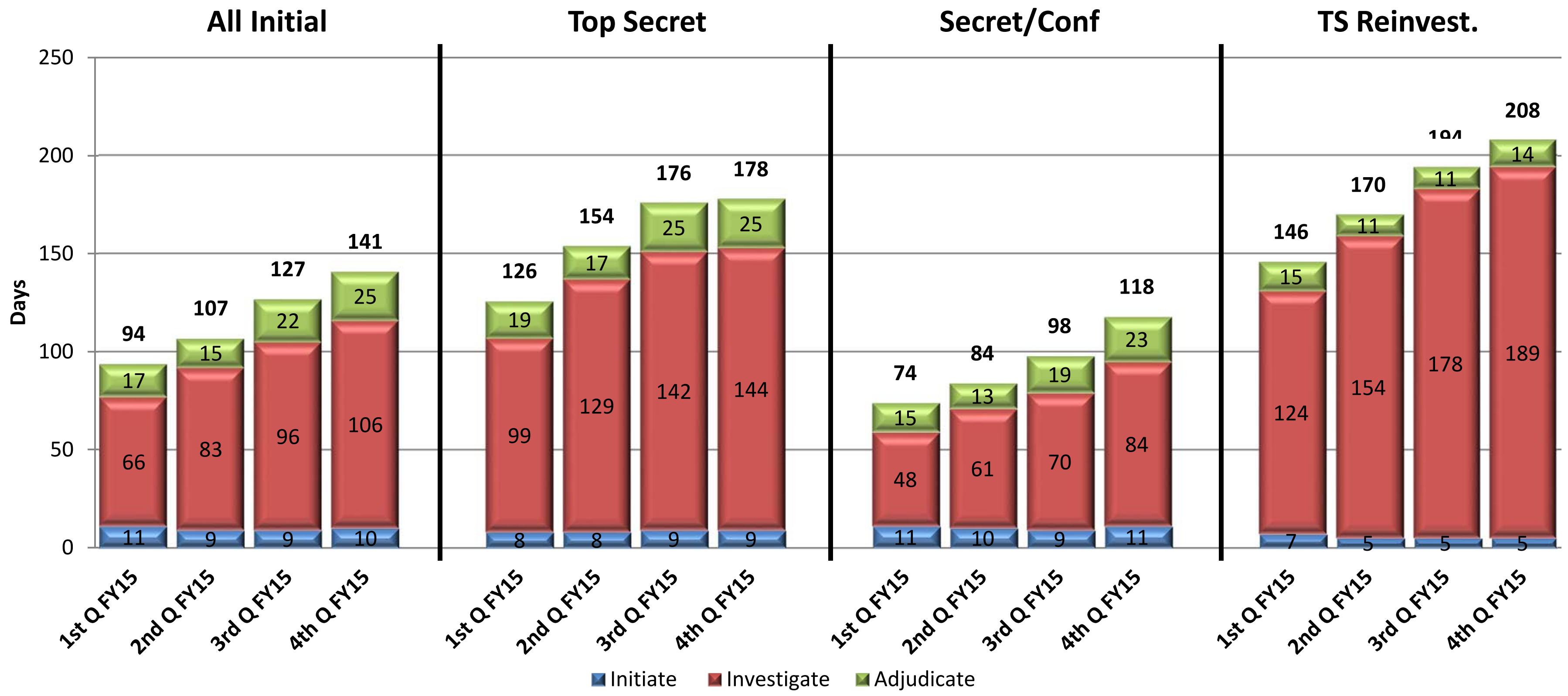
Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

DOE

November 2015

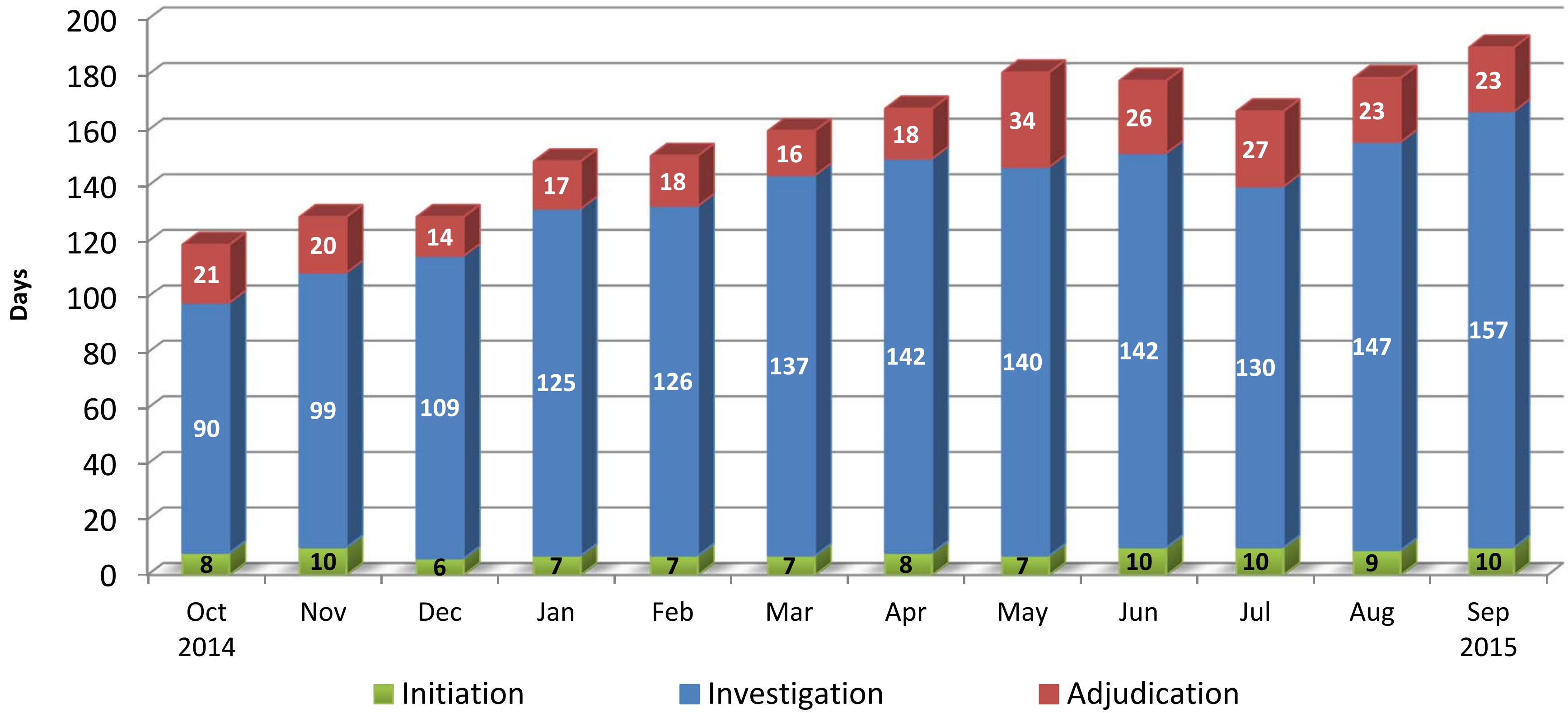
Quarterly Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 1st Q FY15	1,431	552	879	1,338
Adjudication actions taken – 2nd Q FY15	1,474	527	947	1,488
Adjudication actions taken – 3rd Q FY15	1,706	662	1,044	1,994
Adjudication actions taken – 4th Q FY15	1,768	698	1,070	2,153

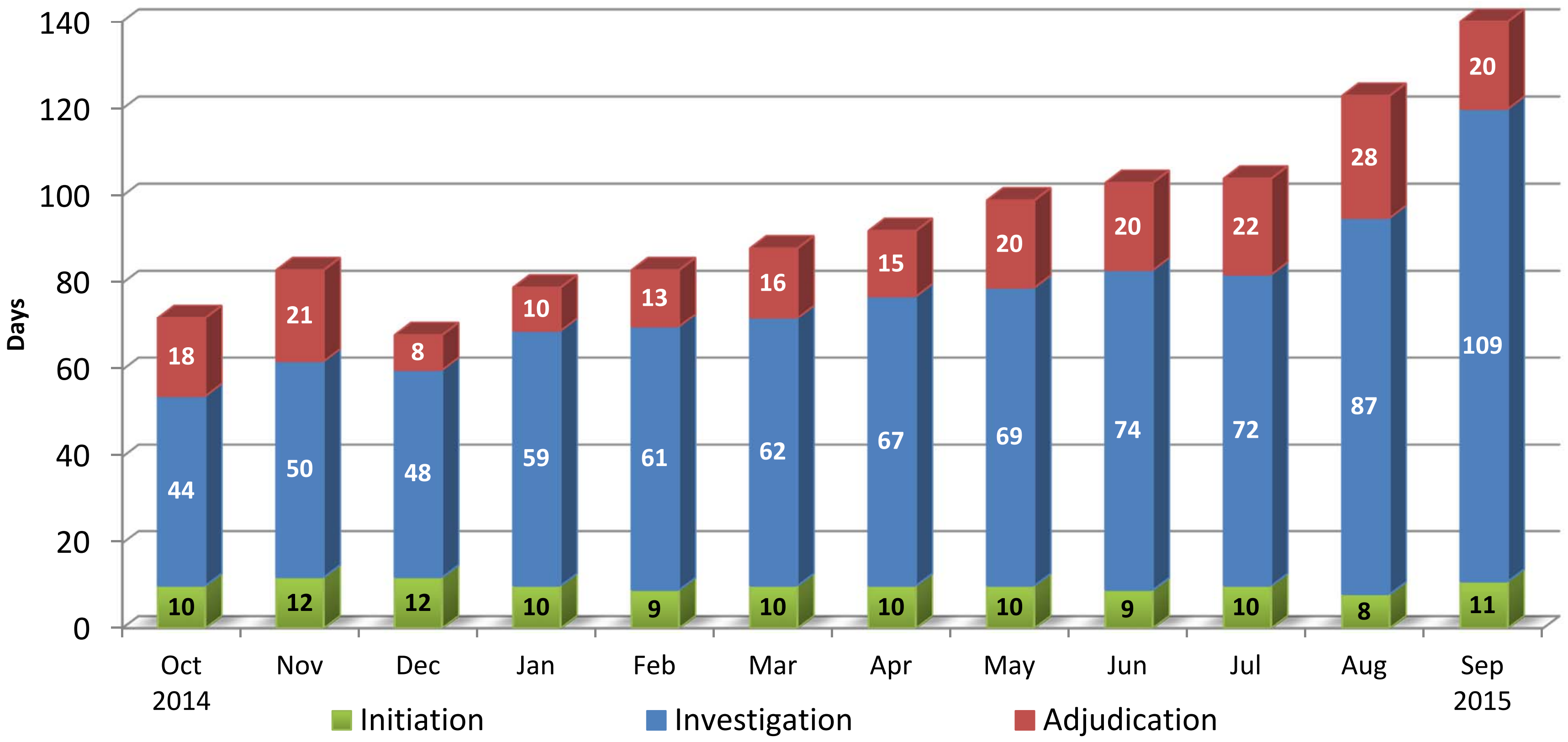
DOE's Average Timeliness Trends for 90%
Initial Top Secret Security Clearance Decisions



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

	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015
100% of Reported Adjudications	171	191	184	152	163	205	206	238	203	211	263	212
Average Days for fastest 90%	119 days	129 days	129 days	149 days	151 days	160 days	168 days	181 days	178 days	167 days	179 days	190 days

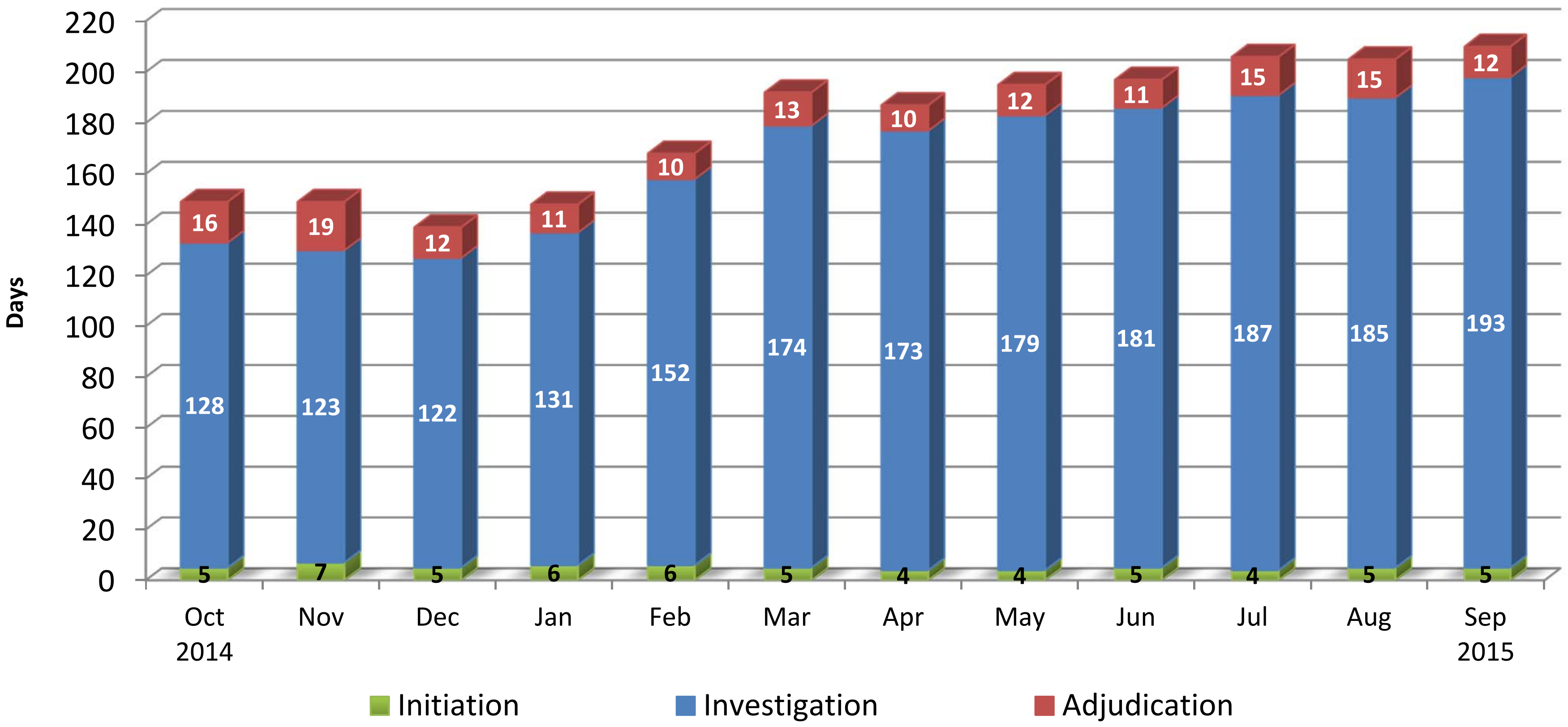
DOE’s Average Timeliness Trends for 90%
Secret/Confidential Security Clearance Decisions



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

	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015
100% of Reported Adjudications	238	305	326	263	248	391	254	397	356	523	301	219
Average Days for fastest 90%	72 days	83 days	68 days	79 days	83 days	88 days	92 days	99 days	103 days	104 days	123 days	140 days

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



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

	Oct 2014	**Nov 2014**	**Dec 2014**	**Jan 2015**	**Feb 2015**	**Mar 2015**	**Apr 2015**	**May 2015**	**Jun 2015**	**Jul 2015**	**Aug 2015**	**Sep 2015**
100% of Reported Adjudications	510	382	440	475	464	538	588	669	724	642	676	805
Average Days for fastest 90%	149 days	149 days	139 days	148 days	168 days	192 days	188 days	195 days	197 days	206 days	205 days	210 days