Minutes of the July 15, 2015 Meeting of the
National Industrial Security Program Policy Advisory Committee (NISPPAC)

The NISPPAC held its 51st meeting on Thursday, July 15, 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 November 6, 2015.

I. Welcome and Administrative Matters:

Mr. Fitzpatrick welcomed the attendees, and after introductions, reminded everyone that NISPPAC meetings are recorded events. He stated that there would be a public comment period at the end of the meeting, and reminded everyone that the minutes from the March 18th meeting are provided in the information packets, as well as the presentations for today's meeting. He noted that there were no action items from the last meeting. He acknowledged departing industry members Steve Kipp and Rick Graham, and presented each with a gift of appreciation from the ISOO staff and the Committee membership at large. 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 with the end of the term of the two departing members we would need to fill their positions. He stated that industry had been requested to nominate two new candidates by September 1, 2015, and that these nominees would subsequently require NISPPAC Chair concurrence. He then reminded the Committee that it was time to renew the NISPPAC charter, a biennial Federal Advisory Committee Act requirement, and that a copy of the revised charter was included in their packets. Soliciting any proposed changes to the charter and receiving none, he requested a motion for its approval. The Chair offered the motion to approve the revised charter, and it was unanimously affirmed.

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. He explained that two distinct sets of data had been breached: a repository of federal personnel record information, and a repository of background investigations information. He noted that the first incident had affected approximately 4.2 million individuals, and that the second had impacted approximately 21.5 million individuals, which included current and former federal employees, current and former cleared contractors, and in fact all who had completed and submitted a Standard Form (SF) 86, 85, or 85P within the last 10 years. Further, he pointed out that, due to their discovery and announcement at different points in time, the timelines for dealing with the consequences of the two breaches were distinct, and that the requirements for remediation for the

two populations thus required separate attention. He explained that the government is making an effort to fortify cyber protections, as well as other information related to these attacks, to an unprecedented degree, and described the specific activities related to this initiative as the "cyber sprint": a coordinated effort of federal Chief Information Officer and Chief Information Security Officer entities across executive branch offices whose challenge it is to find solutions and take swift action towards fortification and protections of federal systems, with enhanced interest in particular repositories of personally identifiable information (PII), which have been heavily involved in both breaches. He offered that the best portal for dissemination of information related to this activity was OPM.gov/cybersecurity, and pledged that both the Federal Investigative Services (FIS) and ISOO would be providing information to stakeholders in an effort to create a sphere for focused communications. He noted that the currency of the information provided in the forms (accurate addresses and telephone numbers, etc.) would heavily impact the ability to get the notifications to the proper individuals, and explained that OPM was in the process of constructing partnership notification solutions that would allow people to identify themselves as being potentially impacted. He described concerns that have been noted regarding shutting down the Electronic Questionnaire for Investigations Processing (e-QIP) system and the delay that has resulted in providing access and initiating investigations. He noted that much attention is aimed at getting e-QIP back up as quickly as possible. He then called for Mr. Merton Miller, FIS, to continue the discussion.

Mr. Miller reaffirmed the scope of the breach impact to which the Chair had alluded, and added that there was a great deal of emphases being placed on juveniles that, due to their special vulnerability, have suffered major impacts. He also reiterated the Chair's point regarding the difficulties in contacting individuals who had moved or otherwise changed their contact information since their form's completion. In addition, he stated that fiscal short falls have resulted in a reduced workload capability, and that OPM has experienced a reduction in revenue which, when coupled with the price increase associated with investigations for fiscal year 2015, has resulted in operating at a loss. He also explained that due to the loss of some primary contractors the capabilities of investigative services have diminished while contractor roles have increased. He described the normal workload as approximately 160,000 – 180,000, and the current caseload at approximately 358,000, and pointed out that these conditions caused increases in the delivery of investigations timelines. Finally, he stated that he hoped to soon bring good news related to e-QIP, especially with regard to restarting the system while assuring users of the safety of the information they have provided, and he noted that there were new partnerships with the Department of Defense (DoD) and the National Security Agency designed to exceed previous information security standards.

(B) DoD Update:

Steve Lewis, Office of the Undersecretary of Defense for Intelligence (OUSD(I)), began the update 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. He described this as the final substantive step before it is signed. He explained that the focus of Conforming Change #2 was the application of insider threat requirements to industry, to include reporting, establishing a program, and providing training and awareness to cleared employees. He then stated that 3 of 4 volumes of the Special Access

Program (SAP) are now issued, approved, and ready for review, and noted that Volume II, Personnel Security, is pending legal review. He described the next step in the process as seeking broad application across the government, which will require intensive collaboration with all government partners.

(C) The Defense Security Service (DSS) Updates:

Stan Sims, DSS, opened with an update from the government and industry stakeholders meetings, which were held one day prior to the NISPPAC meeting, and noted that their agenda mirrored much of what had already been discussed at the NISPPAC. He described updates provided to the attendees about internal DoD and DSS procedures to help get them through the OPM data breach events. He urged industry to contact their DSS representative to address any unique concerns. He noted that the stakeholders had also been provided an update on the Certification and Accreditation (C&A) process. He then introduced Fred Gortler as a new member of the DSS team, serving in the role of Programs Director and official member of the NISPPAC. Mr. Sims proceeded to review updates from the Office of the Designated Approving Authority's (ODAA) Business Management System, explaining they have released Version 2.2, which will increase system functionality to the industry colleagues. He further explained that in September of 2015 they plan to release Version 2.3 in order to provide more functionality in industrial reporting. He then described discussions with stakeholders about the risk based analysis and mitigation system that DSS is putting in place, emphasizing assessments completion and facility clearance processing prioritizations, and management of the National Interest Determination process. He also explained that they had discussed the automated Department of Defense (DD) Form 254 project, and he introduced Keith Minard, DSS, to provide a more in-depth process description and update. Mr. Minard stated that on June 8, 2015, in partnership with the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, and with inputs from government and industry representatives, they had deployed the initial operating capability of the National Industrial Security Program Contract Classification System (NCCS). He explained that this will provide automated capability for DoD, federal agencies, and industry to create, file, retrieve, analyze, and distribute the DD Form 254 data which is now accessible through a web portal and enables 24/7 access. He noted the processes' ability to facilitate processing and distribution of contract security classification and described its objectives as to improve the security controls and provide a centralized workflow. In addition, he described the near-term objectives as providing enhanced capabilities to produce more intuitive instructions, facility clearance verification through DSS's Industrial Security Facility database, and providing notification capabilities as the process is being created. He described the long-term goal as to increase the business model workflow capabilities to include workflow for special types of information that now require the government customers' approvals and approvals for subcontracts. Kimberly Baugher, Department of State (DOS) asked if there was going to be more guidance for government agencies, or if it was going to be briefed to the government, and/or the "agency contract support" addressed on the website. Mr. Sims responded that there are already available parameters and that DSS would communicate with the Facility Security Officers through its Personnel Security Management Office, where there are numerous critical priority guidance assets, and that regarding government contracting activities, they will reach out whenever an industry partner reports a contract particular issue or whenever there is a contracting criticality issue involving personnel security or facilities. Mr. Sims further

reminded the Committee that each agency has provided a POC for industry-related concerns of this nature, and that DSS would continue to invoke those resources as required. The Chair then called for the combined industry presentation updates.

(D) Combined Industry Presentation Updates:

Tony Ingenito, Industry, began (see attachment 2) by thanking Steve Kipp and Rick Graham for their dedicated service. He announced some changes in the Memorandum of Understanding representatives, which includes J.C. Dodson as the new representative for Aerospace Industries Association (AIA), Klaus Heerwig, now representing the Industrial Security Working Group, and Dennis Arriaga, the new President of the National Classification Management Society. He also spoke to the OPM data breach, stating that this was perhaps an opportune time to address areas of conflicting or inconsistent guidance. He noted that with the e-QIP in temporary cessation, and the growing backlog of clearances, one area of focus should be interim clearances to include the recent changes stating they would not go beyond one year, as well as necessary attention towards out of scope clearances, whether or not an individual could continue to support other classified contracts, as well as other substantive issues. He stated that a key point for industry is reciprocity for those individuals with clearances regardless of being out of scope or in an interim status. In reference to the NISPOM rewrite, he stated they had participated in on-going meetings with customers, agencies, and industry to assist in working through the identified areas needing to be addressed in the rewrite. He stated that they had identified approximately 85 individuals in industry to provide input into the process as well as to ensure effective and thorough representation. Finally, he spoke of progress and suggestions made with the Policy Integration (PIWG), the Personnel Security Clearance (PCLWG), Certification and Accreditation (C&AWG), and SAP (SAPWG) working groups. He thanked DSS for permitting industry participation in the NCCS system definition development and Beta testing. Finally, he expressed appreciation for industry's participation in the National Industrial Security System development process, and anxiously anticipates the assistance it will provide in enhanced senior leadership capabilities. The Chair then called for the working group updates.

(E) Working Group Updates:

PCLWG Updates:

Mr. Pannoni introduced the PCLWG's report by reminding the Committee that the PCLWG would no longer present all the accumulated metric data unless there were some concerning trends. However, he noted that they were continuing to address the OPM security breach, e-adjudication and its relation to usage for industry, and transparency in regards to cases that are assigned to the Defense Office of Hearing and Appeals (DOHA), any or all of which would occasionally require some metrics reporting. As regards DOHA cases, he stated that they would continue to investigate adverse information reporting procedures and how those cases are processed, as well as how the information is shared among government partners and the applicable industry entity that submitted the report. As regards e-adjudication, he pointed out that they would continue to work that issue and hope to see if they can raise the bar to a level that still provides us with efficiencies and recognizes risk, but makes for a more proficient system.

Finally, he described the continued effort to ensure reciprocity of investigative clearance data in an effort to prevent redundancy.

Mr. Sims interjected that DSS has established a front-end system for triaging those incident reports via the Personnel Security Management Office for Industry (PSMO-I) relative to which ones are priority and working those with the Department of Defense Consolidated Adjudication Facility (DoD CAF).

R.B. Peele, DoD CAF, provided the DoD CAF updates (see attachment 3). He stated that while they had inherited a sizable backlog, they had made significant progress, as they have reduced the backlog from an October 2013 high 8.1% to an anticipated June 2015 low of 2.1%. He pointed out that their transition from a multi-version internal electronic management process system to a much more efficient version that would be online in early 2016, coupled with the yet to be known requirements in the forthcoming FIS, prevent them from being able to know the future extent of the timeliness impacts upon their procedures. He then described the CAF's better than originally anticipated compliance with both the Intelligence Reform and Terrorism Prevention Act of 2004 requirements and the 30-day DoD PR requirements, and explained that although they have not yet met all requirements, they have nevertheless made significant progress and will persevere until completion. He then paused in order to reduce some apparent confusion that had come to his attention among members of the Committee in the basic definitions of backlogs. He described backlogs as (1) *pending* (number of active cases minus the average 20-day output), (2) *suspense* (cases that have been in suspense for more than 15 days past their due date), and (3) *second review* (cases in supervisory review for more than 30 days. He concluded his presentation by introducing Linda Boucher, who is to be the new representative of the DoD CAF for the PCLWG.

Mr. Dotson asked, in view of the changes in the new FIS, if the government anticipates seeking relief from Congress on the current backlog clearing targets, or perhaps adjustments against the present measurement criteria. Gary Novotny, Office of the Director of National Intelligence (ODNI), and Lisa Loss, OPM each responded and confirmed that at some point, subsequent to assessing the impact of the new standards, these discussions would need to take place, but that no action had been taken to date. Mr. Dotson pointed that industry would need to be involved in the discussions so that we will be able to gain the additional resources necessary to meet the target requirements. The Chair stated that indeed these discussions must take place, and that we must not forget to fold in the very real factor of increased manpower hours.

Ms. Loss presented an overview of the PCLWG's metrics, especially describing how the computations have been redesigned in order to improve clarity (see attachment 4). She then explained that the government is working with its' contractors to increase capacity, and to encourage them to increase capacity of individuals performing the work. She pointed out that high-volume area vacant positions have been backfilled. Also the government has awarded a contract to support the Federal Field Office in the high-volume DC area, and that there is a current RFP for additional contract support to address the surge, which we define as the number of cases that are in backlog beyond our typical amount of steady state work. Finally, we are exploring areas where we expect to face turnovers due to retirements and other factors, and we are looking at our traditional turnover rates in some of the high volume federal areas. She then

paid special attention to the Secret cleared population, where she pointed to several factors within the program resulting in timeliness impacts, such as the number of individuals we have performing field work, and whether they are federal or contractor employees. She also emphasized the fact that some federal records providers are experiencing delays in providing the records necessary for investigations, likely a result of them transitioning to new ways of doing business themselves and new operating systems, and thus increasing quality from the federal records providers as they modernize their systems, but at the same time incurring normal transitioning delays She then extended the concept to capture tiered investigations to be rolled out as we enter into the Secret cleared level in the fall, that is, those that we used to describe as records-based investigations, even though there is still a requirement for field work. She also noted that that one of the reasons that these cases take longer is that we have not eliminated the challenges associated with records access. Thus, not every secret case will require an expansion to have a subject interview, but many of them will require a field agent to visit a local police department in order to retrieve the records, and this requires addition time and results in reduced capacity. Thus, cases in which you get the same quality record through an automated check require no need to expand procedures, and they move through the process very quickly. However, in about half of the cases we must to send a federal investigator, and this always involves timeliness issues and increases negative impact.

Mr. Novotny continued the timeliness discussion by describing some of the Intelligence Community's (IC) timeliness metrics (see attachment 5). He then introduced *in absentia* Dave Morrison as the new Deputy Associate Director, ODNI, and stated that ODNI had been working with OPM on the data breach by offering inputs to questions that involve the Security Executive Agent in national security cases, and he reminded the membership that the OPM.gov/cybersecurity website previously mentioned by the Chair was indeed an excellent clearing house for information dissemination. Next, he informed the Committee that James Clapper, Director of National Intelligence, believes that the oldest PRs may not necessarily turn out to be the first initiated, but rather he encouraged both federal agencies and industry to take a risk based approach to PRs, and further, that the PR backlog, as a result of the e-Qip stoppage, has recently grown, and that when it came back online ODNI would facilitate initiation and completion. Mr. Novotny then noted that the timeline goal for IC initiations, investigations, and adjudications for Secret clearances was 74 days, but that in the last few quarters they had missed that in both investigation and adjudication time, and he pointed out that the goal for Top Secret was 114 days and PRs was 195 days, which had both been missed in each of the preceding two quarters. The Chair then called for the C&AWG Updates.

C&AWG Updates:

Tracy Brown, DSS, provided the C&AWG updates (see attachment 6). She began by discussing the initiative to get the Cognizant Security Agencies engaged in the working group in order to facilitate an overall National Industrial Security Program (NISP)/C&A picture to ensure reciprocity processes are in place that meet industry's needs. She noted that the C&AWG had evaluated a change management process for DoD CSA-provided guidance, and agreed to update the documentation as needed, and that each release would provide its own implementation and transition plan. She then stated that the Ad-Hoc Risk Management Framework group had been re-integrated into the WG and that through this Risk Management Framework training had been

developed by the Center for the Development of Security Excellence. This product is in the form of a draft DSS Assessment and Authorization Process Manual, and incorporates the risk management framework process. The transition plan is now in the review phase, and we are working to redefine the quarterly reporting criteria. Next, she noted that the DSS authorization timelines have been holding steady at the targeted goal for the last three years with the only spike coming from conducting on-site validations during the government shutdown. She briefly touched on the ODAA Business Management update Version 2.2 that Mr. Sims had described earlier, noting that the update increased functionality by including the ability to add administrative updates to existing plans in the system, and to disestablish self-certified and expired accreditations. In addition, she noted that during the migration some systems were migrated in as System Security Plans (SSP) when in fact they were Master System Security Plans. She explained the functionality was now there to update these, and announced that the next release is tentatively scheduled for early September, 2015. She noted that the most common SSP deficiencies were missing attachments and documentation errors, but that on-site validations were being completed in accordance with established timelines. She reminded the Committee that the most common vulnerabilities during on-site validations continue to be auditing controls and unprotected security objects. The Chair thanked the WG for its continued good work, and encouraged the non-DSS members to continue on the path of including their processes and metrics into this particular approvals' effectiveness view, so that we can sustain the ability to capture this comprehensive picture, especially in view of on-going, concurrent timelines and ever-evolving processes. In response to Mr. Dotson's question as to whether or not they were receiving the Industrial Security Facilities Database data in the appropriate currency cycle, Ms. Brown stated that the information systems security professionals responsible for specific facilities have assured DSS that their data is accurate and timely, but she added the caveat that as the new system comes online industry would be responsible for performing all data updates. The Chair then called for Mr. Pannoni to provide the SAPWG updates.

SAPWG Updates:

Mr. Pannoni updated the Committee on activities regarding the SAPWG by stating that even though they have not held any sessions since the last NISPPAC meeting, there is nevertheless much work going on, and that the DoD policy pieces were coming together, as they have currently updated three of four of their SAP manuals. He also pointed out that extensive measures were being taken to ensure consistency across agencies that have SAP authorities, and explained that moving forward given the cost impact for industry and potential damage to the national security interest, consistent implementation remains the key. Further, he ensured the Committee that the WG will put much thought and effort into getting the key agency personnel to dedicate themselves to developing effective and acceptable SAP policy and procedures, and that all must adopt an attitude of fundamental sharing and cooperation within a risk management framework, as to fail to do so would result in unacceptable costs to both classified information and personnel security clearance processes. Finally, he reiterated that the WG welcomes any thoughts that might in any way facilitate a smooth transition or enhance our knowledge in this area, and especially encouraged all SAP authorization agencies to actively support this vital initiative.

(F) Controlled Unclassified Information:

The Chair then updated the Committee on activities relating to implementation of the CUI program, and began by reminding the Committee that the program contains three moving parts. He described the first of these as the proposed federal regulation for the CUI Program in government, and that it recently concluded its 60 days of public review and comment in the Federal Register. It is the Proposed Rule 32 CFR, Part 2002, and it is the set of requirements that executive branch departments and agencies would need to follow to implement a CUI program in accordance with the executive order. It outlines the requirements for handling, marking, designating, and decontrolling CUI, and sets in place the governance required in an agency and how that governance will relate to the Executive Agent, which is NARA with ISOO administering, and described the efforts now being made to sift through the hundreds of comments that were received. He publically thanked all the government and industry participants who are engaged in cooperatively providing sound analysis and constructive and innovative comments throughout the process. Ultimately, this will result in taking a new revision of the rule, as well as all previous government comments, back to the Office of Management and Budget Office of Information Regulatory Affairs who will then submit the revised rule for government interagency review. He expressed the hope that this will then be the last form of review, and that a final rule will be published later in this calendar year, but promised to update the Committee at the November meeting, regardless of the pace of the process. He then described the second moving part as the National Institute of Standards and Technology (NIST) Special Publication 800-171, which controls systems processing CUI in non-federal organizations and systems, and is essentially a tailored set of recommendations for how to protect CUI in non-federal entities. He described this mechanism as a good, stand-alone set of cyber protections, not yet invoked as a requirement, but which when submitted as a part of a new contract or when otherwise made applicable, is destined to become a Federal Acquisitions Regulations (FAR) rule. Finally, he labeled the FAR rule as moving part number three, and described our strategy as the integration of these pieces into CUI rules and requirements that are understandable and equivalent between executive branch and non-executive branch entities, to include contractors. He further explained that while, from a procedural standpoint, we cannot propose a FAR rule until such time as the federal regulation is effective, we are nevertheless using this time to work on ways to familiarize participants in the federal acquisition policy community with the CUI program and its industry-related needs, including everything in the SP 800-171, as well as any other requirements of the federal rule that will ultimately appear in the FAR rule, including, but not limited to, handling and marking procedures. Therefore, the NIST approach is a model for us in promulgating a FAR rule that ties in the requirements of the federal regulation and this special publication Also, he stressed the importance of understanding that the scope of application of this FAR rule is many times over larger than the NISP, in that there are 300,000-plus entities that do business with federal government entities and potentially many, if not most, will at some point encounter CUI, and thus we have to have a mechanism that acknowledges that scale and deals with it accordingly. Therefore, our expectation, assuming we achieve a federal regulation later this calendar year or early in next calendar year, is that we would then have a proposed FAR rule, which would itself be subjected to all the usual steps that a proposed FAR rule must follow, including socialization with industry groups and public review and comment. Finally, he challenged the Committee to make good use of this time, as we are still many months away from having a FAR rule that implements CUI requirements and therefore you have an excellent opportunity to come to understand what the requirements are

going to be and how they will be communicated, so that you can begin to consider what the impacts might be to your operations. In addition, you have time to examine the parameters of the federal rule and see where the requirements really fall out, especially as those which govern handling, marking, and designating CUI are easily comprehendible, and demonstrate a fair amount of common sense and judgement when applied to physical safeguarding requirements. There is obviously much more complexity in the IT requirements, but even those have been designed with industry implementation in mind, which you will discover as you become familiar with SP 800-171. Finally, he pledged continued updates as we go forward, and acknowledged that there will be a number of industry-related briefings and sessions hosted by Washington, DC-area groups who are active in the regulatory process that will give everyone an opportunity to ask questions and understand the direction of the CUI program.

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 no comments offered.

VI. Closing Remarks and Adjournment:

The Chair reminded everyone that the next NISPPAC meeting is scheduled for November 18, 2015, at NARA. He noted 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. He reiterated that he was grateful for all who attend these meetings at their own expense, and thanked their company leadership for sponsoring their travel. He reminded the members that a dial-in capability will again be available for any who cannot travel to the meetings. The Chair adjourned the meeting at 11:50 a.m.

Attachment #1

Attachment 1

NISPPAC MEETING ATTENDEES/ABSENTEES

The following individuals attended the July 15, 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
• Stephen Lewis	Department of Defense	Member/Presenter
• Kim Baugher	Department of State	Member
• Ryan McCausland	Department of the Air Force	Member
• Jeffrey Bearor	Department of the Navy	Member
• Dennis Hanratty	National Security Agency	Member
• Anna Harrison	Department of Justice	Member
• Scott Ackiss	Department of Homeland Security	Member
• Eric Dorsey	Department of Commerce	Member
• Merton Miller	Office of Personnel Management	Member
• Richard Hohman	Office of the Director of National Intelligence	Member
• Anthony Ingenito	Industry	Member/Presenter
• J. C. Dotson	Industry	Member
• Martin Strones	Industry	Member
• Michelle Sutphin	Industry	Member
• Richard Graham	Industry	Member
• Philip Robinson	Industry	Member
• Steven Kipp	Industry	Member
• Keith Minard	Defense Security Service	Alternate/Presenter
• 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	Alternate
• George Ladner	Central Intelligence Agency	Alternate
• Gary Novotny	Office of the Director of National Intelligence	Alternate/Presenter
• Lisa Loss	Office of Personnel Management	Alternate/Presenter
• Tracy Brown	Defense Security Service	Presenter
• R. B. Peele	Department of Defense	Attendee/Presenter
• Belinda Bugett	Department of Defense	Attendee
• Charlotte Bowen	Department of Defense	Attendee
• Anthony Lougee	Department of Defense	Attendee
• Ebony Morgan	Department of Defense	Attendee
• John Haberkern	Defense Security Service	Attendee
• Fred Gortler	Defense Security Service	Attendee
• Valerie Heil	Department of Defense	Attendee
• Jay Buffington	Defense Security Service	Attendee
• Lisa Gearhart	Defense Security Service	Attendee
• Michael Witt	MOU Representative	Attendee

• Mark Rush	MOU Representative	Attendee
• Dan McGarvey	MOU Representative	Attendee
• Leonard Moss, Jr.	MOU Representative	Attendee
• Carla Peters-Carr	Industry	Attendee
• Linda Ruhnow	Department of Energy	Attendee
• Priscilla Matos	Department of Defense	Attendee
• Glen Clay	Department of Navy	Attendee
• Cheryle Winder	Office of the Director of National Security	Attendee
• Dennis Arriaga	Industry	Attendee
• Kirk Poulsen	Industry	Attendee
• Michael Parham	Industry	Attendee
• Joe Marks	Reporter	Attendee
• Alegra Woodard	Information Security Oversight Office	Attendee
• Robert Tringali	Information Security Oversight Office	Staff
• Michael Manning	Information Security Oversight Office	Staff

Attachment #2

NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

Industry

15 July 2015

Outline

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

National Industrial Security Program

Policy Advisory Committee Industry Members

Members	Company	Term Expires
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
Michelle Sutphin	BAE Systems Platforms & Services	2018
Martin Strones	Strones Enterprises	2018

National Industrial Security Program

Industry MOU Members

AIA *	J.C. Dodson
ASIS	Dan McGarvey
CSSWG	Mark Rush
ISWG *	Klaus Heerwig
NCMS *	Dennis Arriaga
NDIA	Mike Witt
Tech America	Kirk Poulsen

* Change in MOU Rep in June 2015

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 Breech

- Numerous Data Breeches
  - April: 4.2 million records of current & former Federal workers
  - June: 21.5 million BI records of current, former & prospective Federal employees & contractors
- Actions Taken
  - DIA & NRO discontinued use of e-Qip, no plan B at time of decision.
  - OPM suspends e-Qip for processing of new BI cases, no plan B at time of decision
  - OPM and the ODNI work alternative process for BI processing.
- IMPACT
  - Lack of coordinated leadership lead to separate actions from some agencies.
  - Plan B guidance still has not promulgated to industry on process for moving forward.
  - Delay in BI process causing impact on contract for new BI required actions.
- Next Step
  - Need clear policy guidance on Interim Clearances and Out Scope BI's when the system re-opens and backlog grows.
  - Suitability (NACI) may require CAC temporary policy guidance.

Security Policy Update

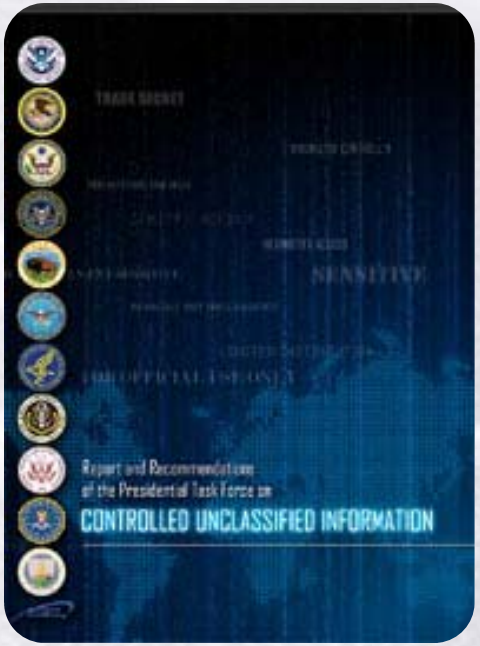
Executive Order #13556

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
  - Continue to monitor development of marking, safeguarding, dissemination and IT Security policy
  - NIST CUI standards developed (SP 800-171).
    - Posted for public comment 18 Nov - 16 Jan 15. 2nd posting due 5/12.
    - Final publication published June 2015
  - 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 Information Security, 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 – Expected 4th Qt FY 2015.

Security Policy Update

Executive Order #13691

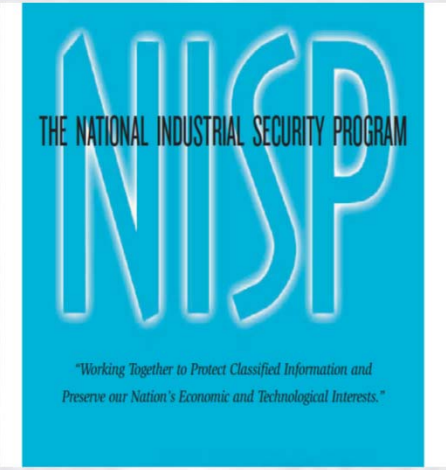
EO # 13691

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.

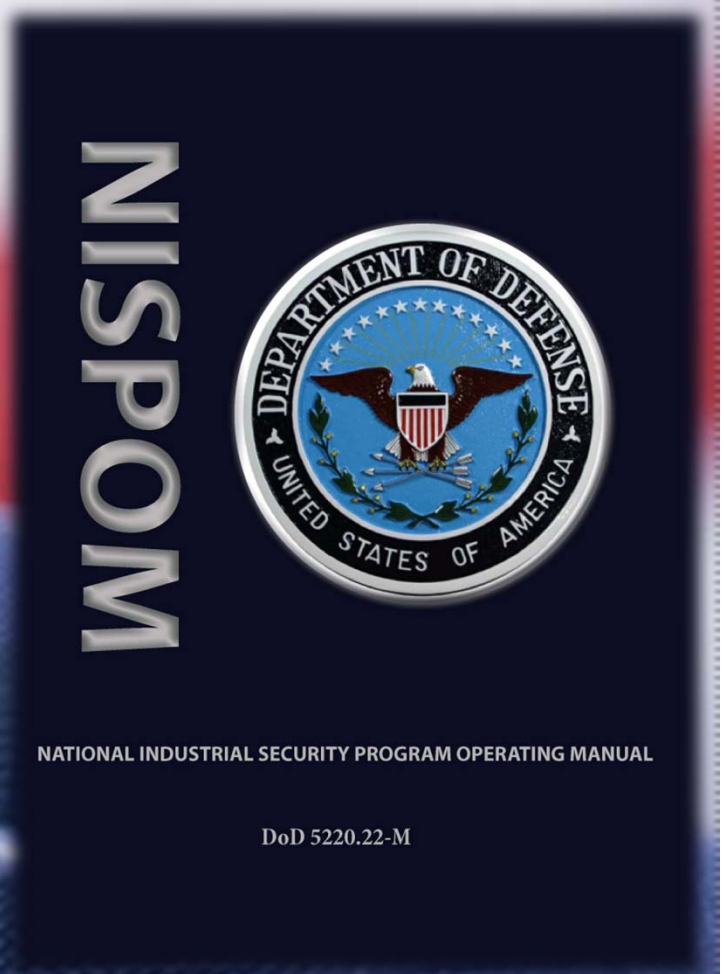


- Amends the National Industrial Security Program (EO 12829)
  - Inserts the Intelligence Reform and Terrorism Prevention Act of 2004.
  - Adds the Secretary of Homeland Security as a cognizant security agency.
    - Drafting NISPOM enclosure addressing Critical Infrastructure Program
- Meeting with 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.

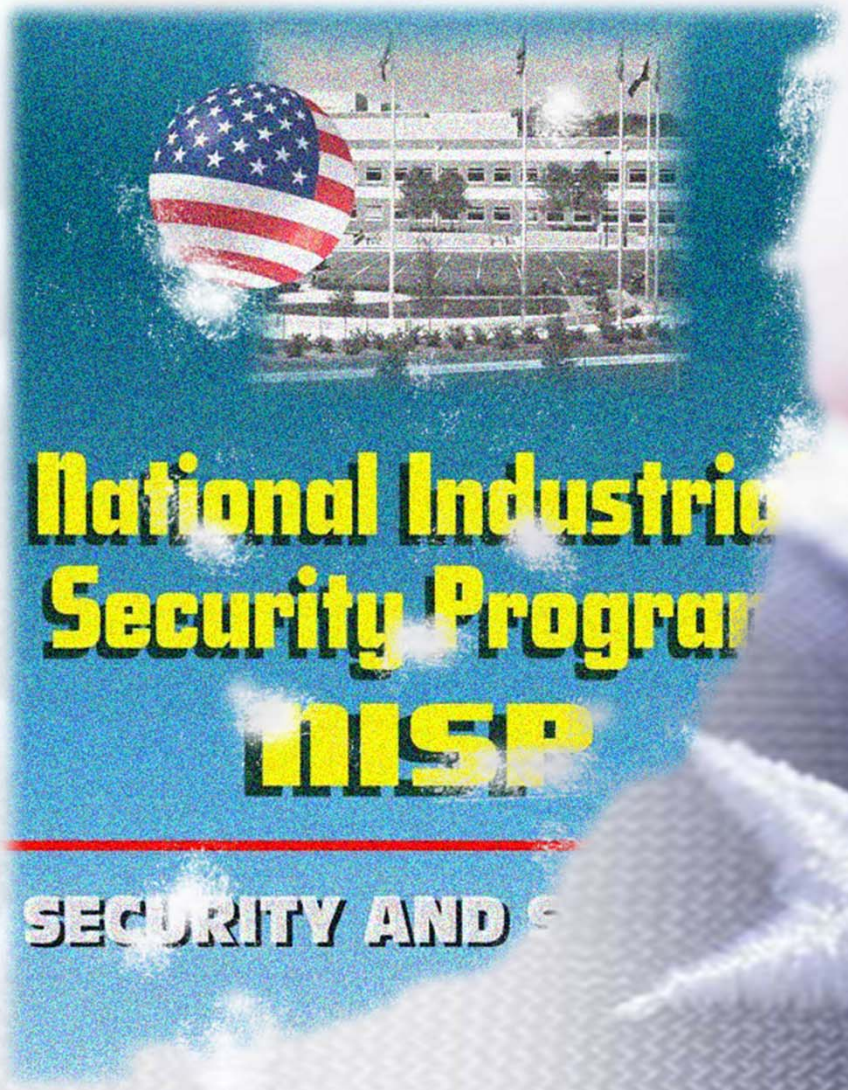
Security Policy Update

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. Conducted 3 meetings to date working thru Bucket 1.
- 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



Fracturing of the NISP



- 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
- Tracking in excess of 55 initiatives

National Industrial Security Program

Policy Advisory Committee Working Groups

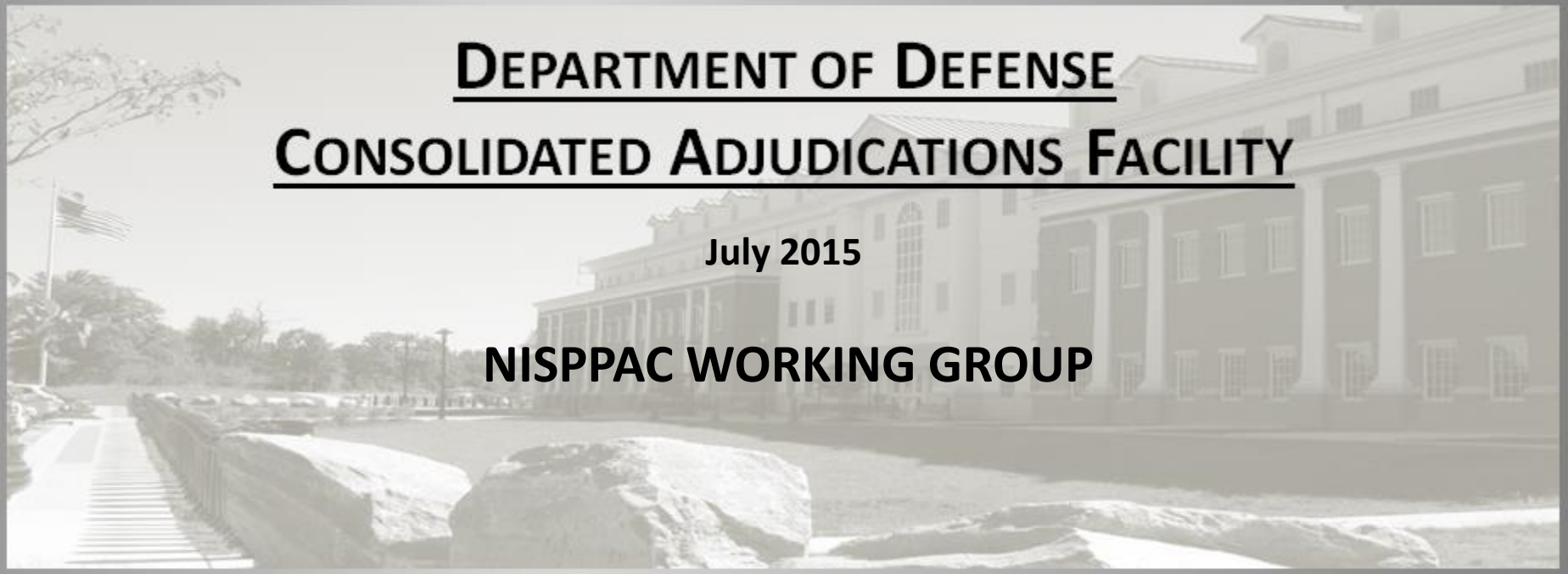
- Personnel Security
  - Working group moving out to address areas of concern.
    - E-adjudication business rules. Ensure aligned with new Federal Investigative Standards. Awaiting ODNI action.
    - DOHA SOR Process. Definitively ID true caseload and aging of those cases.
    - Focused on the e-signature (click-to-sign) testing to address reject submittals.
    - Expecting backlog to grow based on recent OPM Breach.
- 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.
  - Formalize working group established and multiple meetings occurred.
  - Open and honest dialogue. Addressed some high profile accreditation challenges. Presented proposed solution for re-accreditation under JFAN for consideration by SAPCO's. Look forward to future meetings and metric collection to support process inconsistencies.
- Ad-hoc
  - NISP Contractor Classification System (NCCS) – Automated DD254 system
    - Expected to participate in beta test with 25 Industry testers.
    - Beta testing expected to start this week.
  - Development of National Industrial Security System (NISS)
    - Participated on the system requirements phase and standing by for further development meetings.

Attachment #3

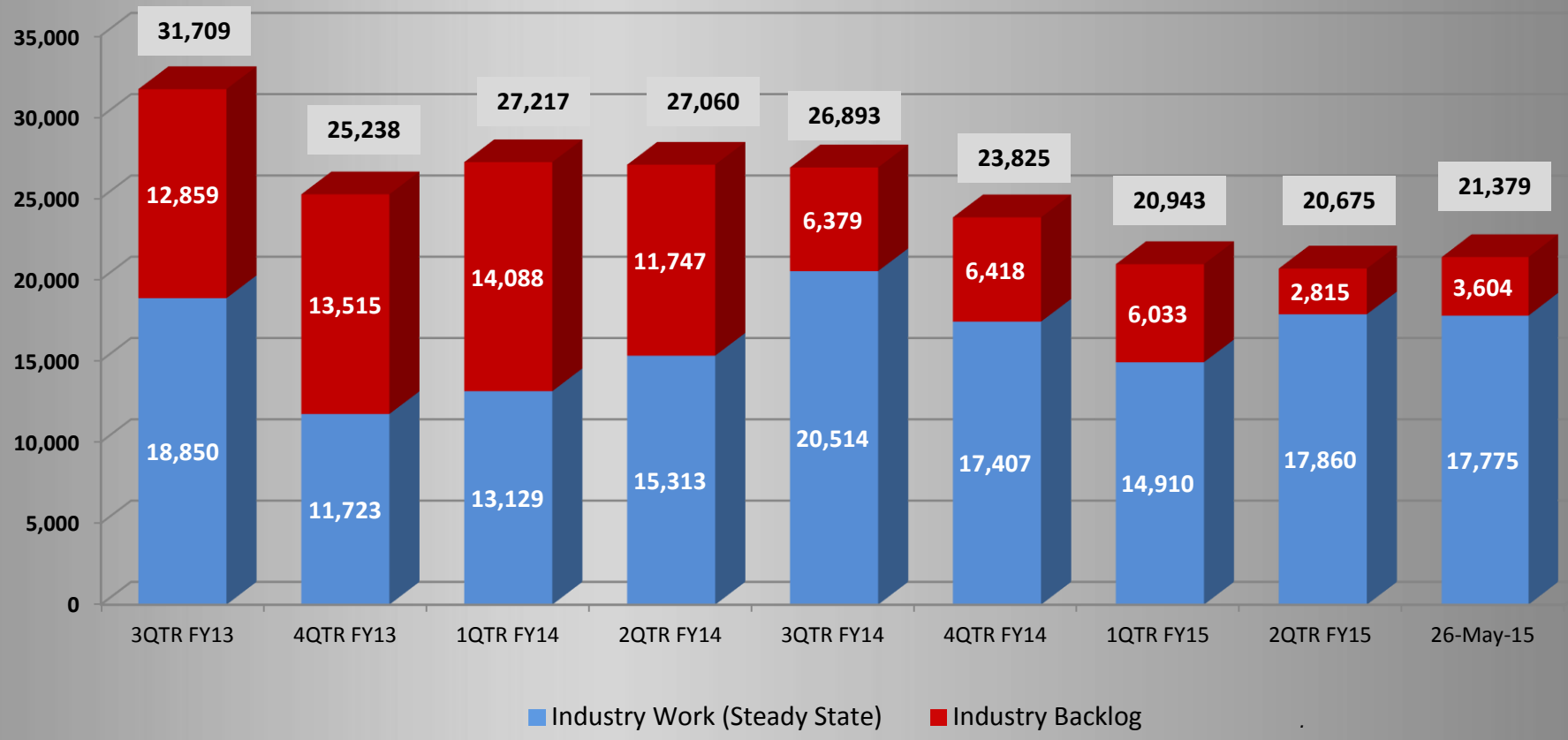


DEPARTMENT OF DEFENSE
CONSOLIDATED ADJUDICATIONS FACILITY

July 2015

NISPPAC WORKING GROUP

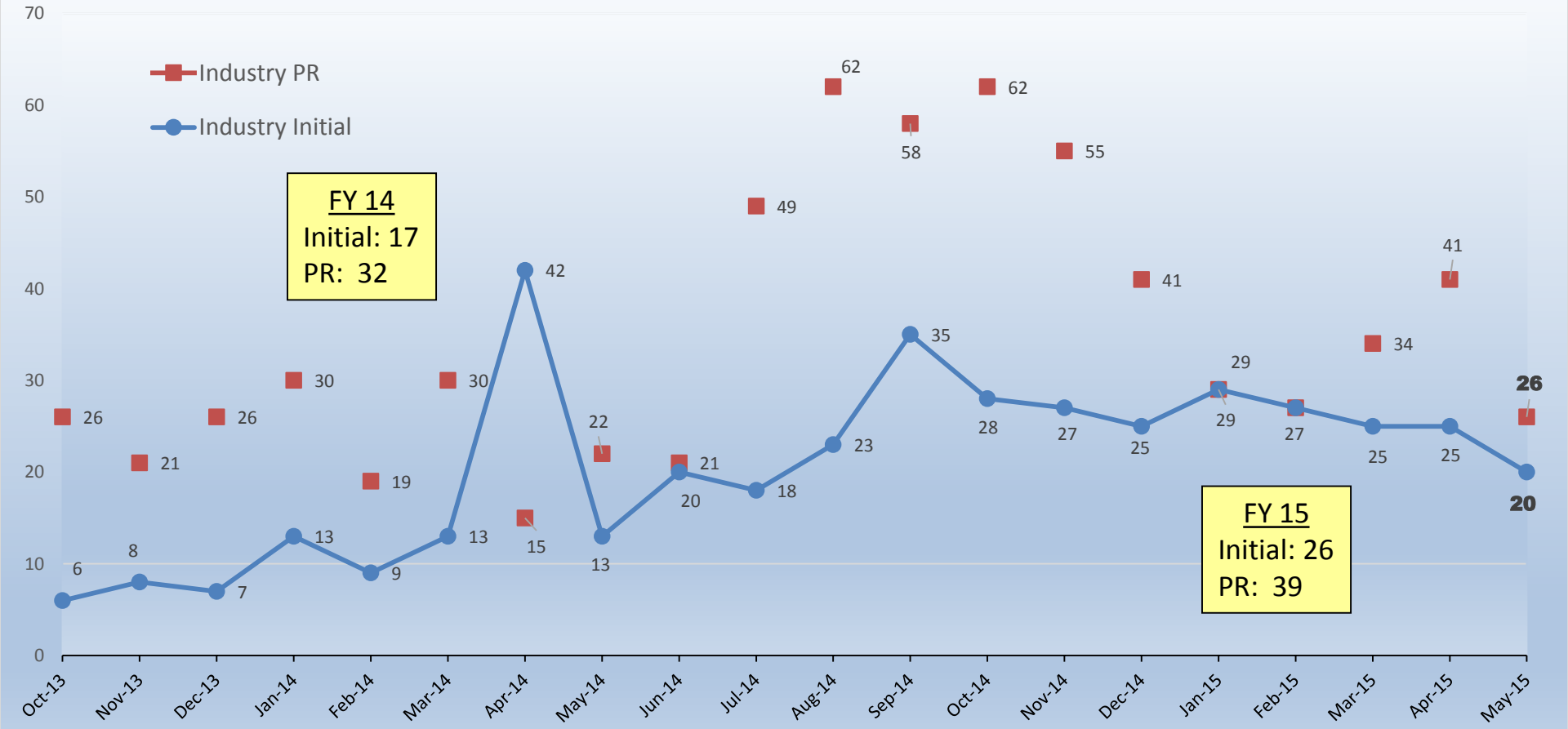
Pending Industrial Workload



- **Backlog likely to endure into 2016**
- **Potential Complications Remain:**
  - **+ FY15 – CATs v4 Deployment to reduce production (est.-20% over 2 mos.)**
  - **+ Full impact of CE pilots and implementation not yet known**
  - **+ 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%
May 15	3,604		2.0%
	-10,000	~ 180,000	

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



- **Both NISP and non-NISP timeliness metrics increased as backlogs addressed**
- **Timeliness to fluctuate throughout FY16 until Industry backlog is fully eliminated**

Definitions

- *Backlog:* cases which have been in the system over a given period of time, further categorized as follows
  - *Pending Backlog* – number of pending cases minus the average twenty (20) day output
  - *Suspense Backlog* – cases that have been in suspense for more than fifteen (15) days past their due date
  - *Second Review Backlog* – cases in second review (supervisory review) for more than 30 days

- *Steady State:* standard work (i.e. Work In Progress or WIP) minus the backlog

DoD CAF
Bldg. 600, 10th Street, FGGM

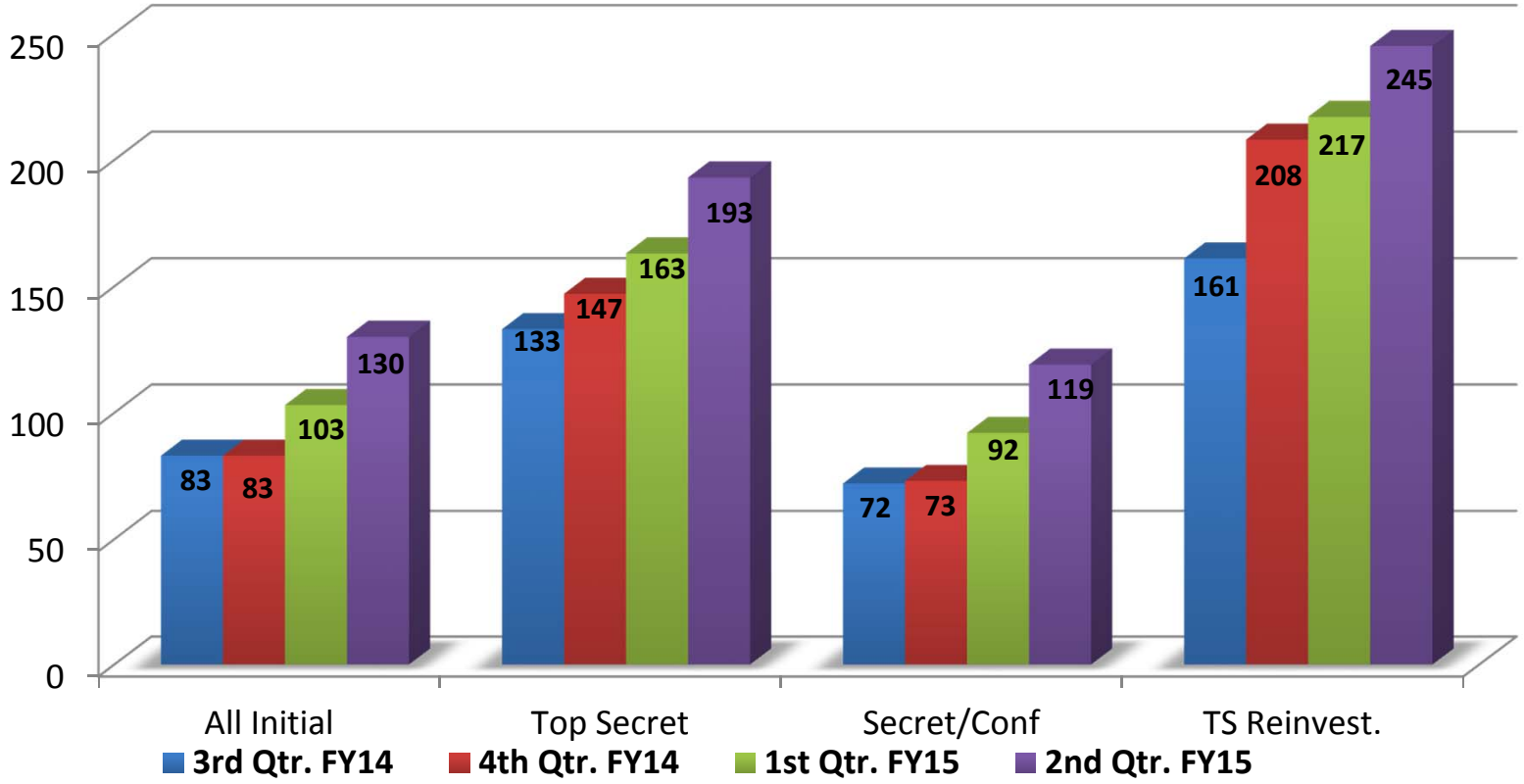
Attachment #4

a New Day for Federal Service

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

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

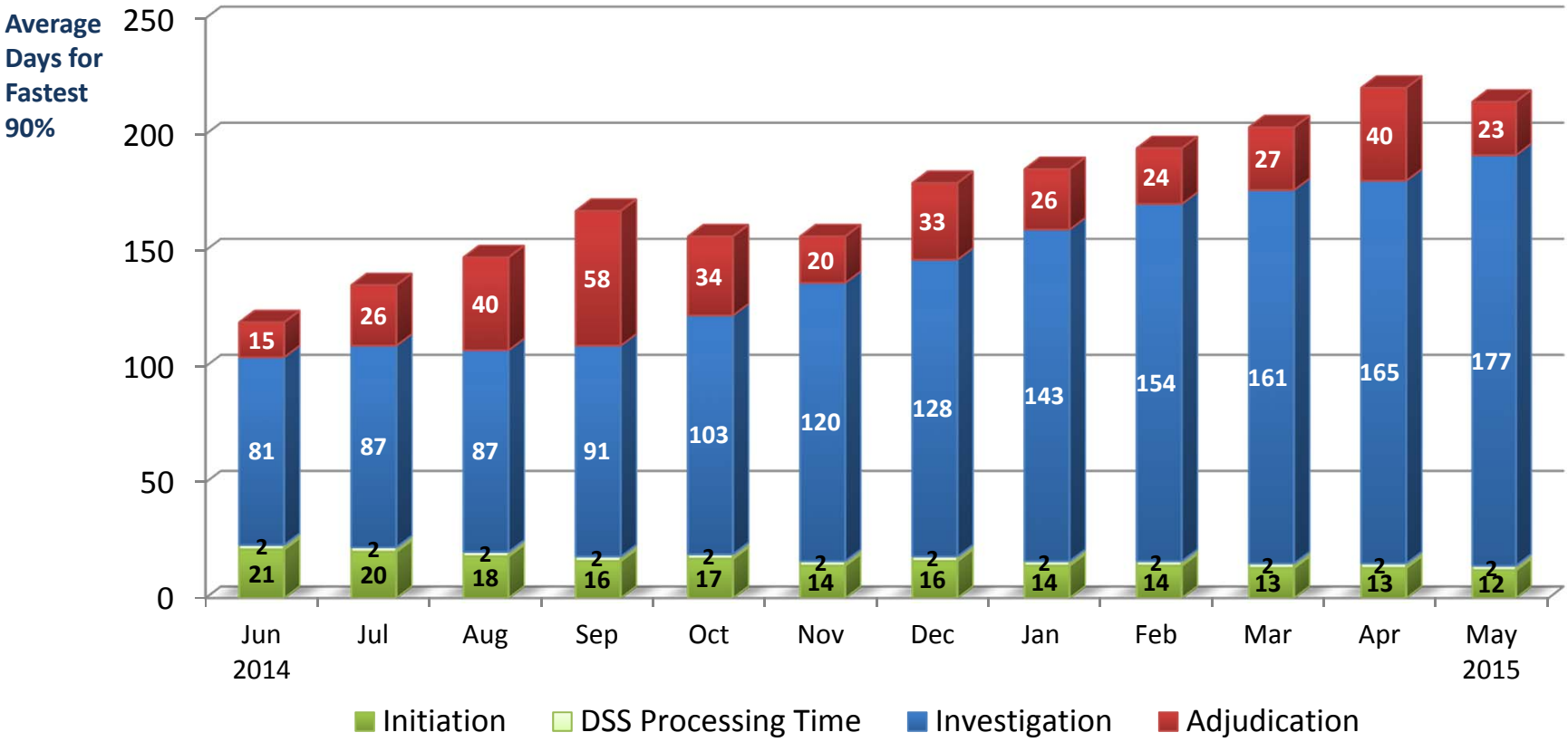
Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 3rd Q FY14	21,661	4,023	17,638	11,641
Adjudication actions taken – 4th Q FY14	18,938	2,824	16,114	7,671
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

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

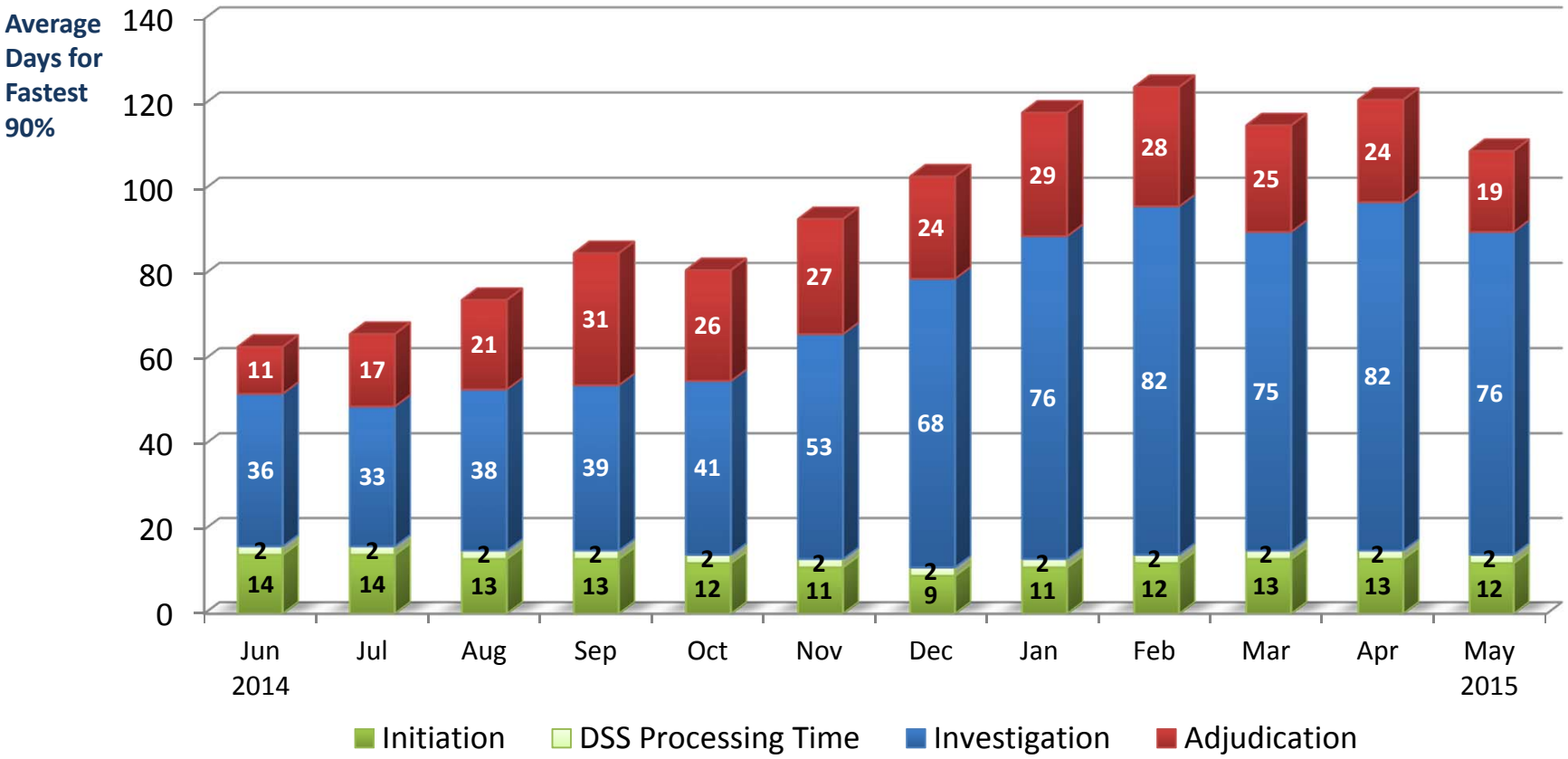
Industry's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



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

	Jun 2014	Jul 2014	Aug 2014	Sept 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Apr 2015	May 2015
100% of Reported Adjudications	1,481	1,103	932	800	1,206	933	983	1,045	988	954	817	966
Average Days for fastest 90%	119 days	135 days	147 days	167 days	156 days	156 days	179 days	185 days	194 days	203 days	220 days	214 days

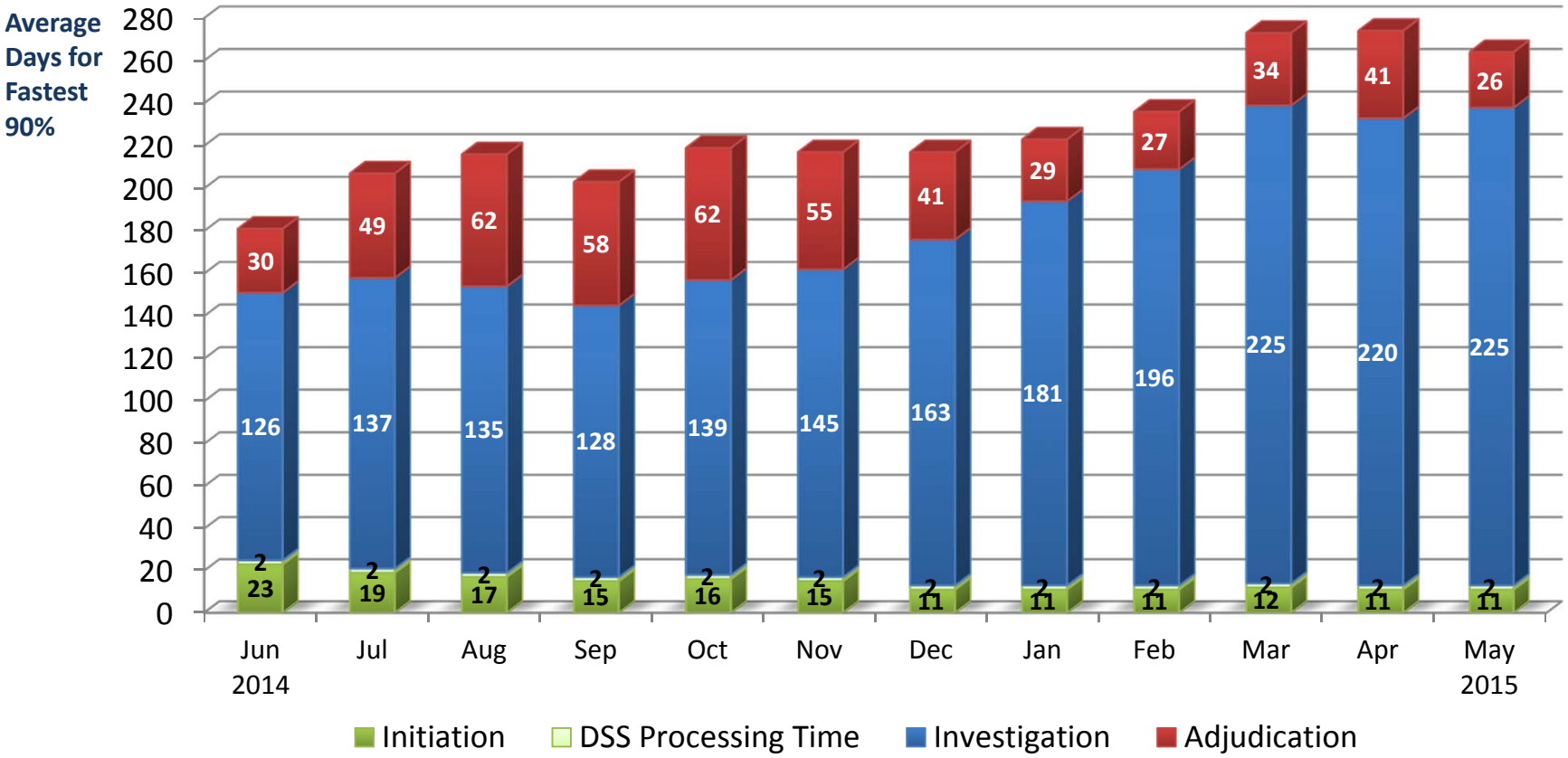
Industry's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



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

	Jun 2014	Jul 2014	Aug 2014	Sept 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Apr 2015	May 2015
100% of Reported Adjudications	5,463	5,993	5,621	4,510	5,293	4,978	5,579	5,358	4,916	5,620	5,002	5,287
Average Days for fastest 90%	63 days	66 days	74 days	85 days	81 days	93 days	103 days	118 days	124 days	115 days	121 days	109 days

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



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

	Jun 2014	Jul 2014	Aug 2014	Sept 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015	Feb 2015	Mar 2015	Apr 2015	May 2015
100% of Reported Adjudications	3,358	2,566	2,334	2,792	3,079	3,084	2,168	2,321	2,442	2,745	2,597	1,985
Average Days for fastest 90%	181 days	207 days	216 days	203 days	219 days	217 days	217 days	223 days	236 days	273 days	274 days	264 days

Attachment #5

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Industry Performance Metrics

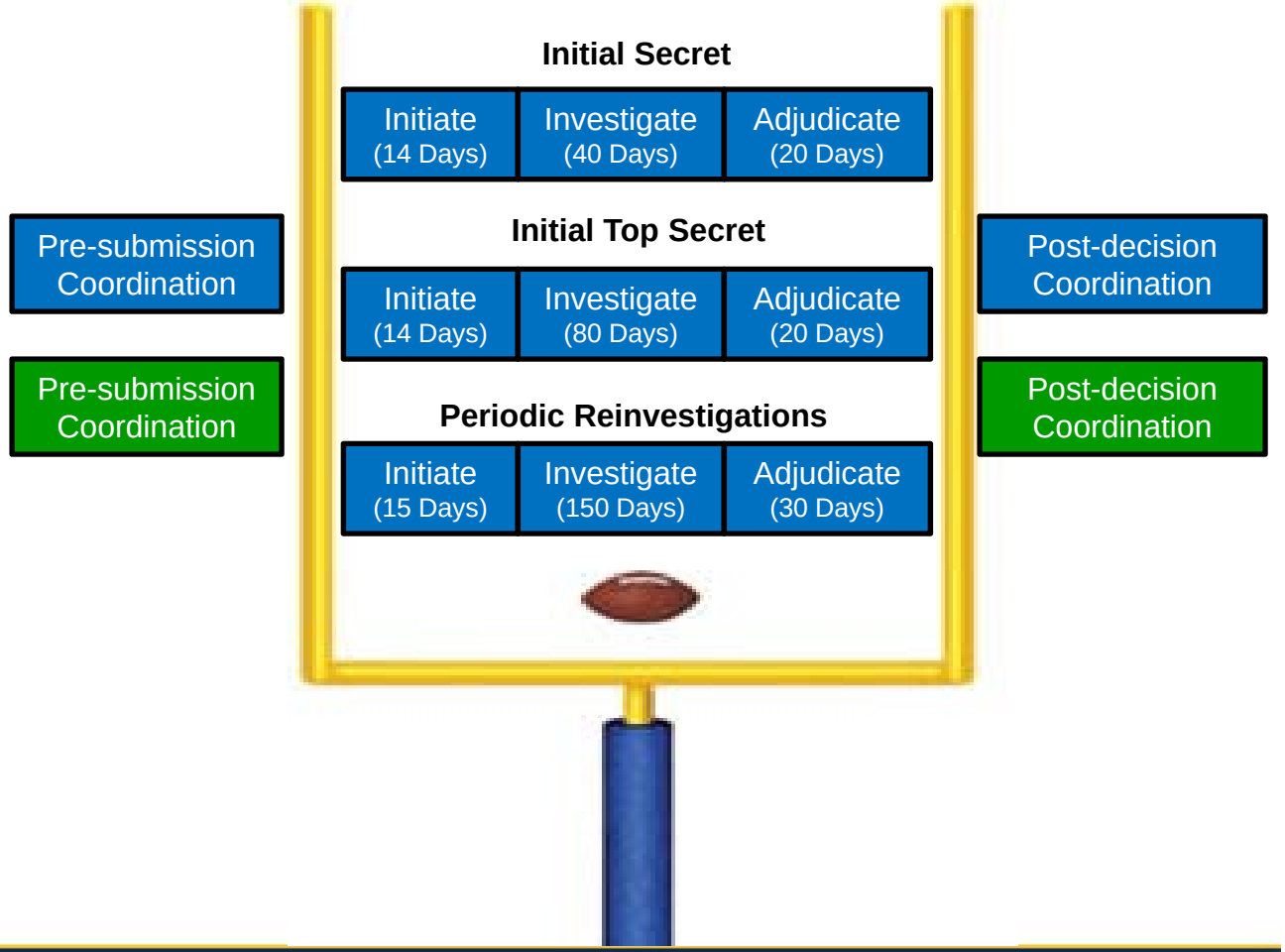
NCSC/Special Security Directorate

LEADING INTELLIGENCE INTEGRATION

15 July 2015

Performance Accountability Council (PAC) Security Clearance Methodology

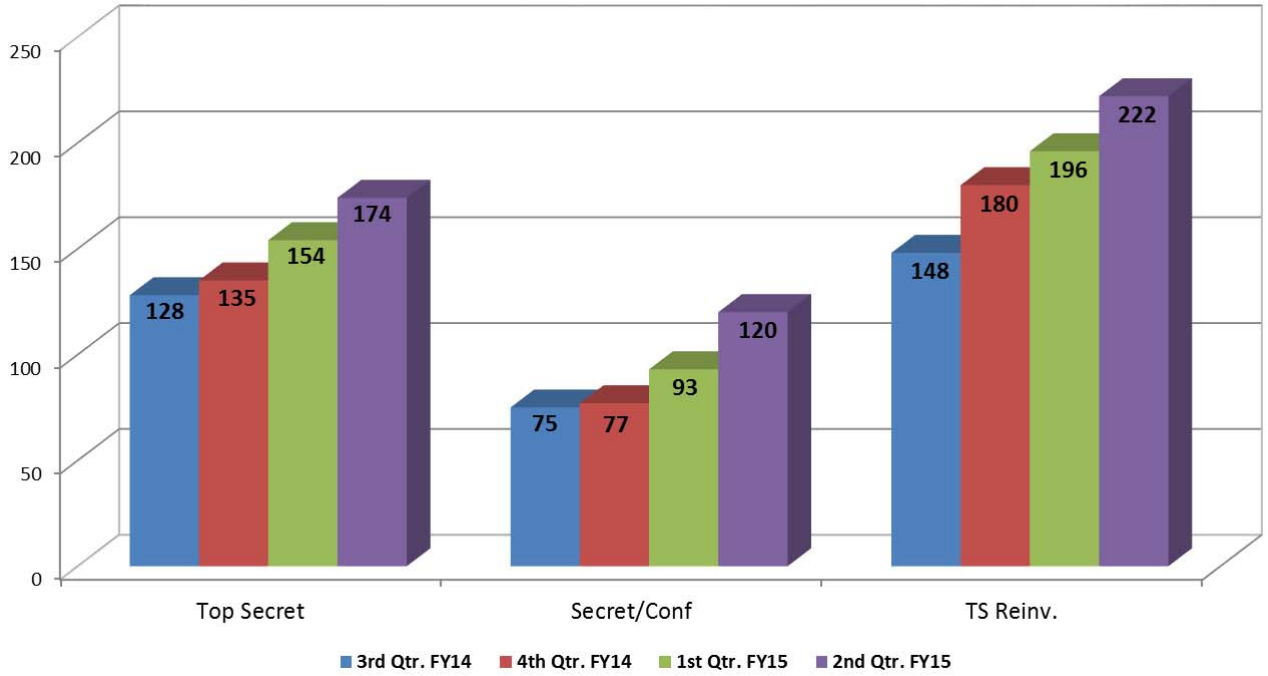
- Data on the following slides reflects security clearance timeliness performance on Contractor cases. DoD Industry data is provided by OPM. IC Contractor data is provided by the following IC agencies: CIA, DIA, FBI, NGA, NRO, NSA and Dept. of State.
- Timeliness data is being provided to report how long contractor cases are taking - not contractor performance
- As shown in the diagram, 'Pre/Post' casework is not considered in the PAC Timeliness Methodology



Timeliness Performance Metrics for IC/DSS

Industry Personnel Submission, Investigation & Adjudication* Time

Average Days of Fastest 90% of Reported Clearance Decisions Made

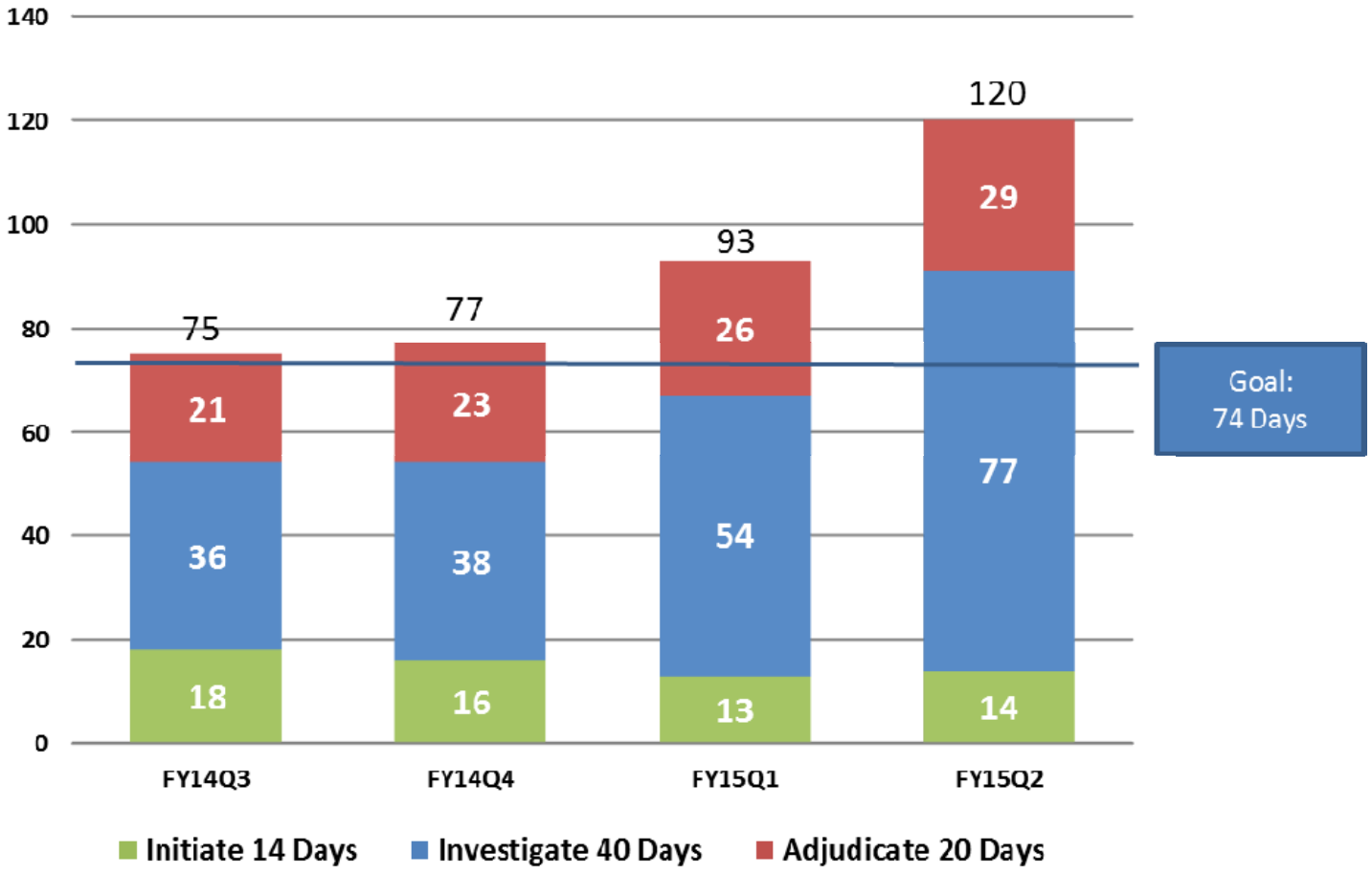


	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 3rd Q FY14	5,324	17,655	12.276
Adjudication actions taken – 4th Q FY14	4,419	16,227	9,174
Adjudication actions taken – 1st Q FY15	4,253	15,650	9,699
Adjudication actions taken – 2nd Q FY15	4,628	17,938	9,652

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

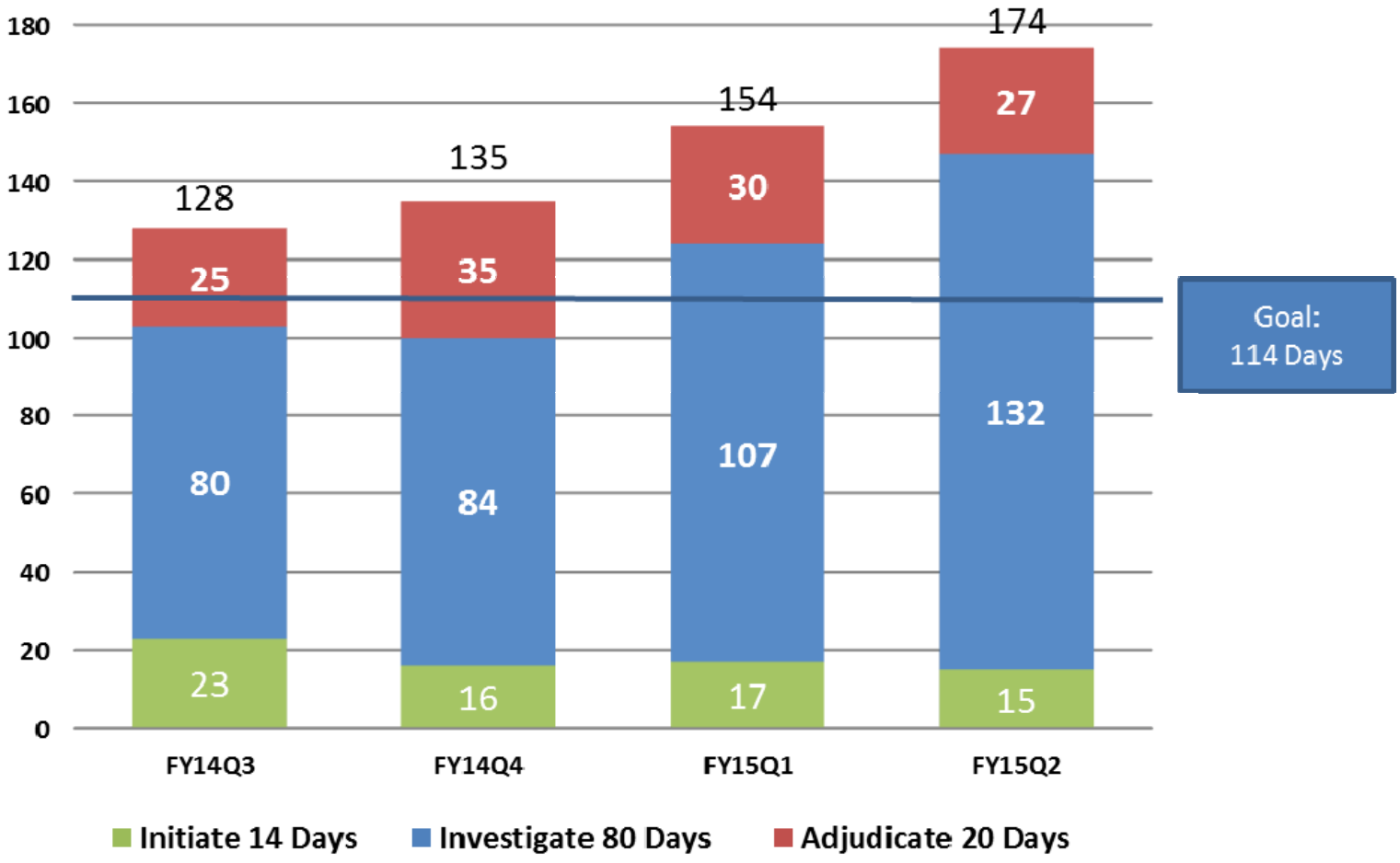
IC and DoD Industry – Secret Clearances

Average Days of Fastest 90% of Reported Clearance Decisions Made



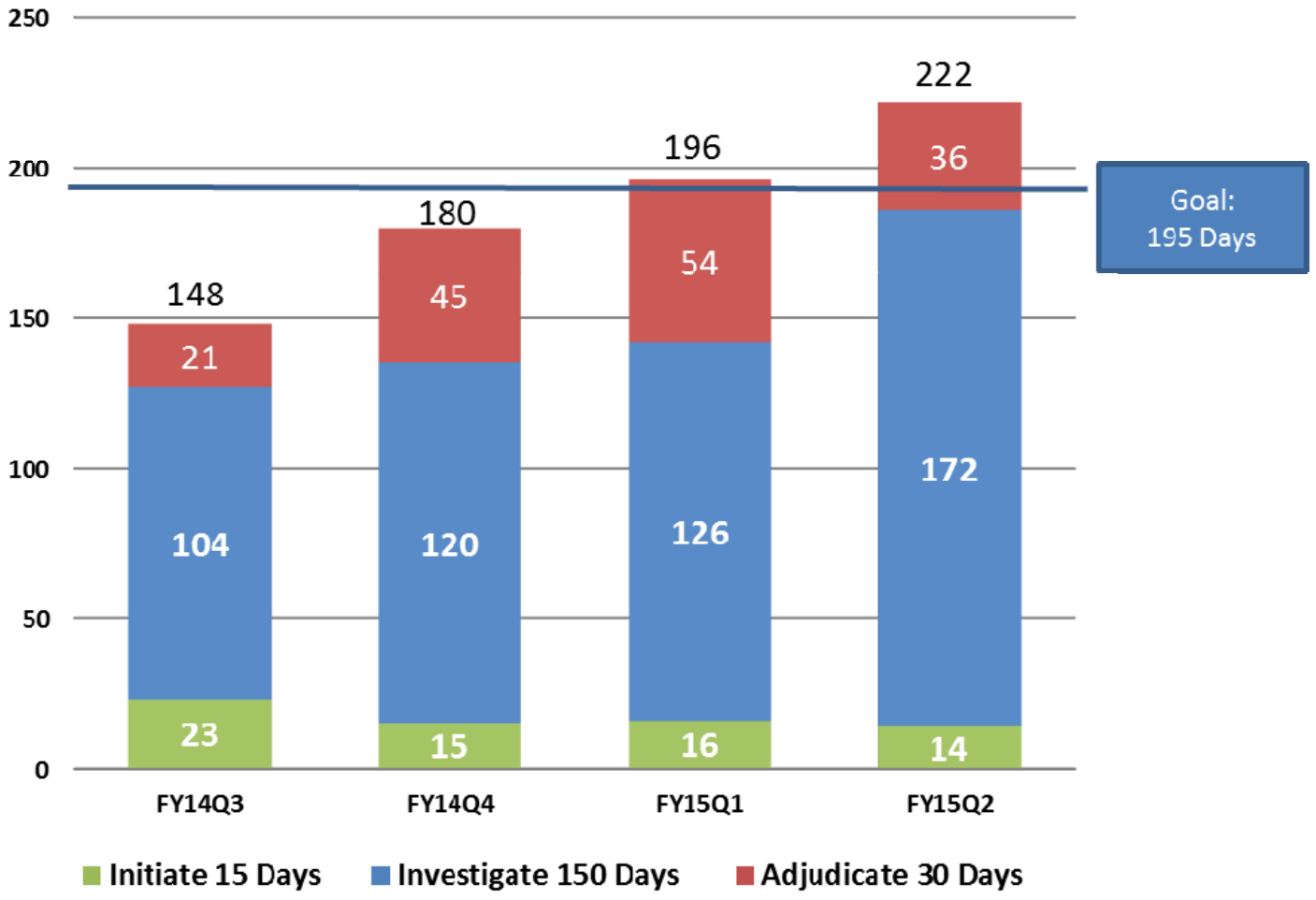
IC and DoD Industry - Top Secret Clearances

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



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: 301-227-8797
Email: Nilda.Figueroa@dni.gov

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

Attachment #6

NISPPAC C&A Working Group Update for the Committee

June 2015

Working Group Initiatives

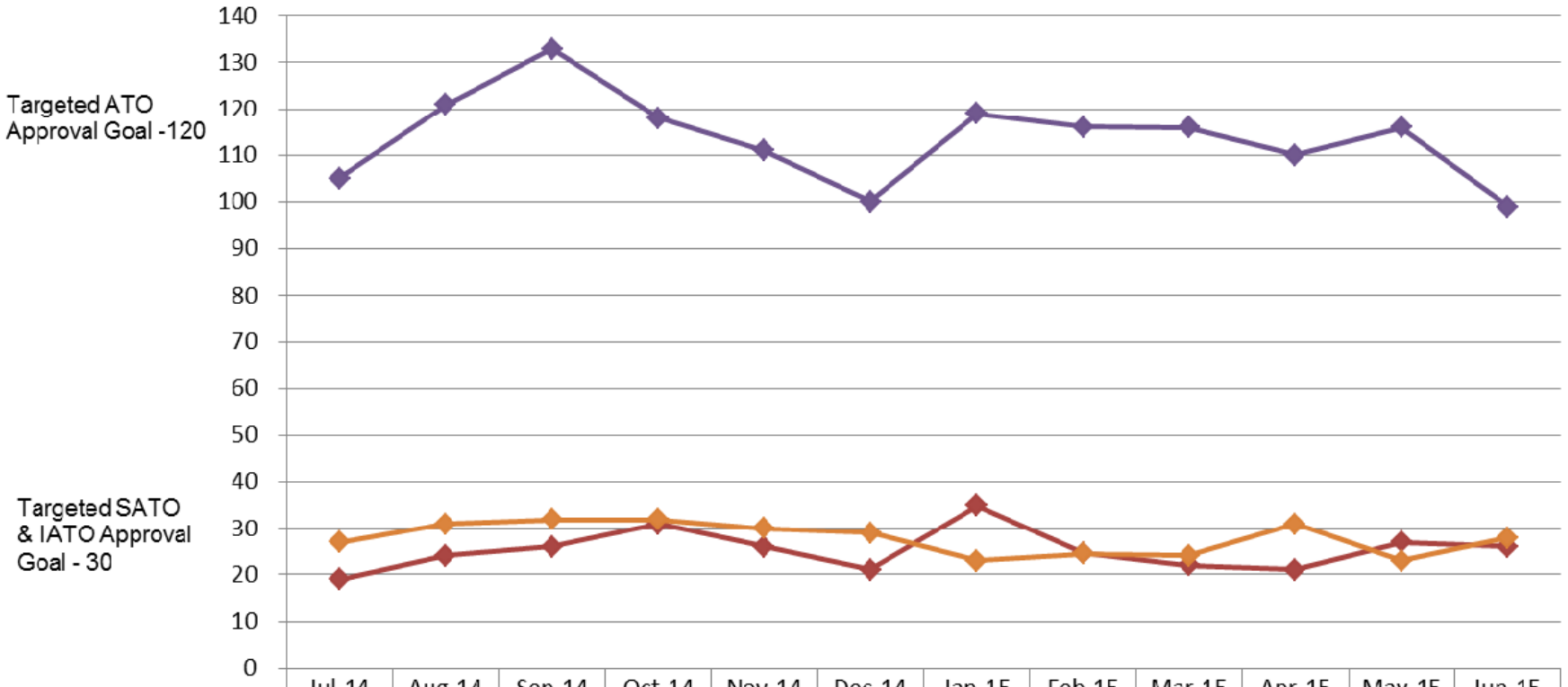
- Integrating other CSAs into the WG to establish an overall NISP C&A picture and ensure reciprocal processes are in place. Initial request for a review of their processes and metrics has been sent

- Evaluating a proposed Change Management Process for the DoD CSA provided guidance to implement appropriately timed changes based on the risk

- The Ad HOC Risk Management Framework (RMF) has been integrated back into the C&A Working Group

- Working to re-define the C&A Working Group Quarterly Reporting Criteria

DSS ODAA Approval Timeliness



	Jul-14	Aug-14	Sep-14	Oct-14	Nov-14	Dec-14	Jan-15	Feb-15	Mar-15	Apr-15	May-15	Jun-15
IATO Amount	122	121	185	189	201	157	185	185	172	173	193	195
IATO Timeliness	19	24	26	31	26	21	35	25	22	21	27	26
Reg ATO Amount	122	105	127	181	137	107	101	134	146	143	163	121
ATO Timeliness	105	121	133	118	111	100	119	116	116	110	116	99
SATO Amount	88	116	122	150	109	102	83	118	93	106	122	122
SATO Timeliness	27	31	32	32	30	29	23	25	24	31	23	28

ODAA Business Management System Update (OBMS)

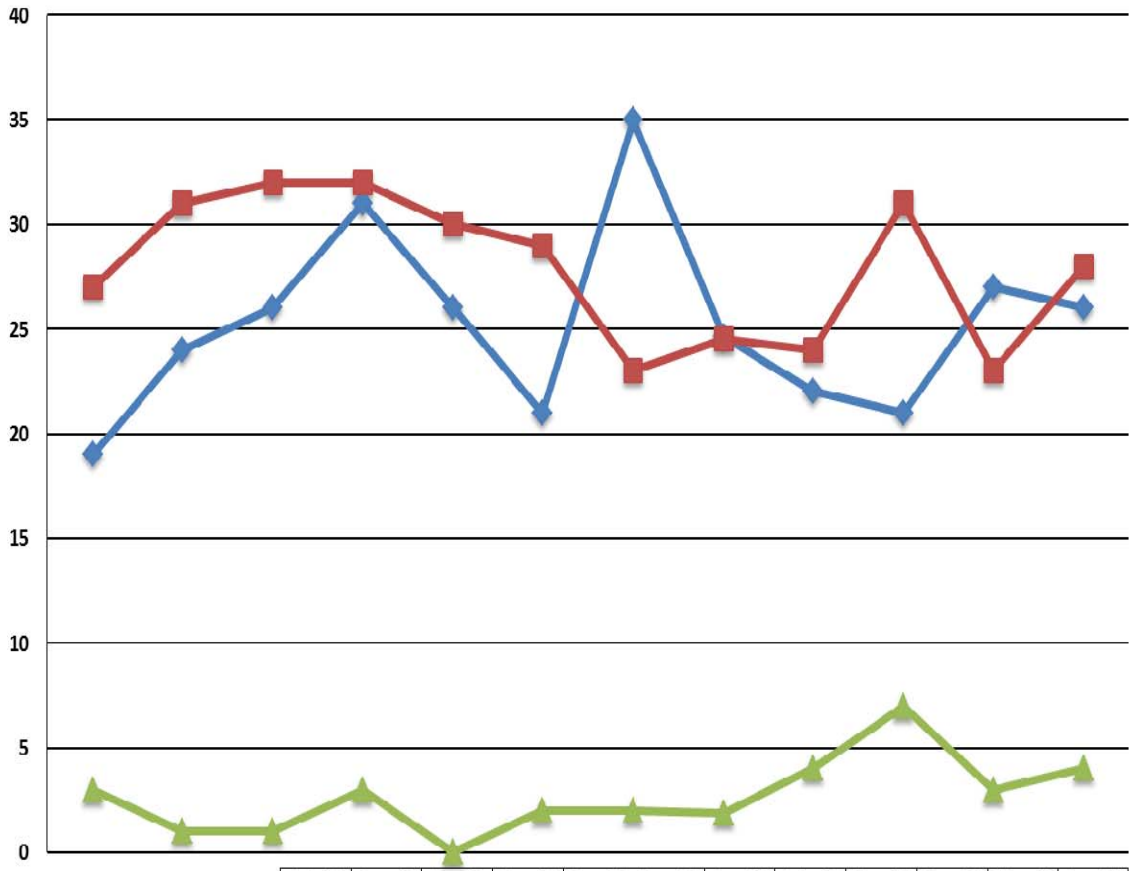
- OBMS Version 2.2 was deployed on June 15, 2015
- New Functional Includes:
  - Ability to perform Administrative Edit/Updates to System Security Plans
  - Ability to Disestablish Self-Certified and Expired Accreditations
  - Ability for Internal Users to Edit Plan Types (SSP/MSSP)
  - Ability to resubmit cancelled and denied plans
  - Ability for OBMS to pull updated Facility Data from ISFD
- DSS has transitioned to using OBMS and all system accreditations are being processed within the application
- The next release is tentatively scheduled for early September 2015.

Takeaways:

- Security Plans are being processed and reviewed IAW established timelines and goals
- Most common deficiencies in SSPs include missing attachments and documentation errors
- Onsite Validations are being completed IAW established timelines and goals
- Most common vulnerabilities identified during system validation include Auditing Controls, not protecting Security Relevant Objects and SSP documentation not reflecting how system is configured

Back-Up Slides

Security Plan Review Results from July 2014- June 2015



	Jul-14	Aug-14	Sep-14	Oct-14	Nov-14	Dec-14	Jan-15	Feb-15	Mar-15	Apr-15	May-15	Jun-15
Time from DSS Reciept of plans to Granting of IATOs	19	24	26	31	26	21	35	25	22	21	27	26
Time from DSS Reciept of plans to Granting of SATOs	27	31	32	32	30	29	23	25	24	31	23	28
Industry Response Time to DSS Questions, Comments	3	1	1	3	0	2	2	2	4	7	3	4
Second IATOs	4	10	11	13	11	9	8	8	20	24	30	15

3584 System security plans (SSPs) were accepted and reviewed during the preceding 12 months.

2078 Interim approvals to operate (IATOs) were issued during the preceding 12 month period, it took an average of 26 days to issue an IATO after a plan was submitted.

1331 “Straight to ATO (SATO)” were processed during the preceding 12 months, it took an average of 28 days to issue the ATO.

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

631 of the SSPs (18%) were granted IATO with corrections required.

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

Denials: 156 of the SSPs (5%) were received and reviewed, but denied IATO until corrections were made to the plan.

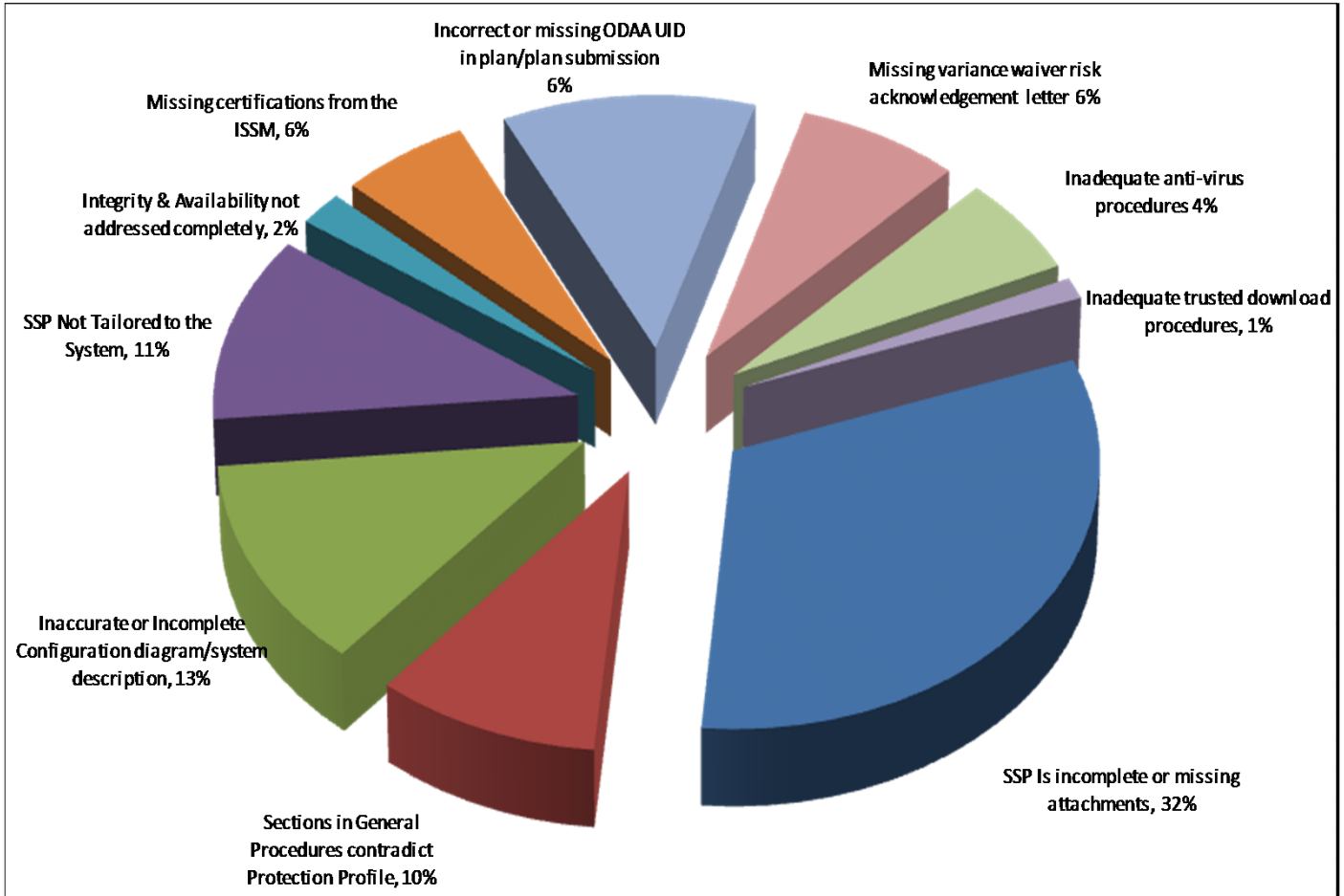
Rejections: 19 of the SSPs (1%) were not submitted in accordance with requirements and were not entered into the ODAA process. These SSPs were returned to the ISSM with guidance for submitting properly and processed upon resubmission.

Last Months Snapshot: June 2015

195 IATOs were granted with an average turnaround time of 26 days

122 SATOs were granted with an average turnaround time of 28 days

Common Deficiencies in Security Plans from July 2014- June 2015



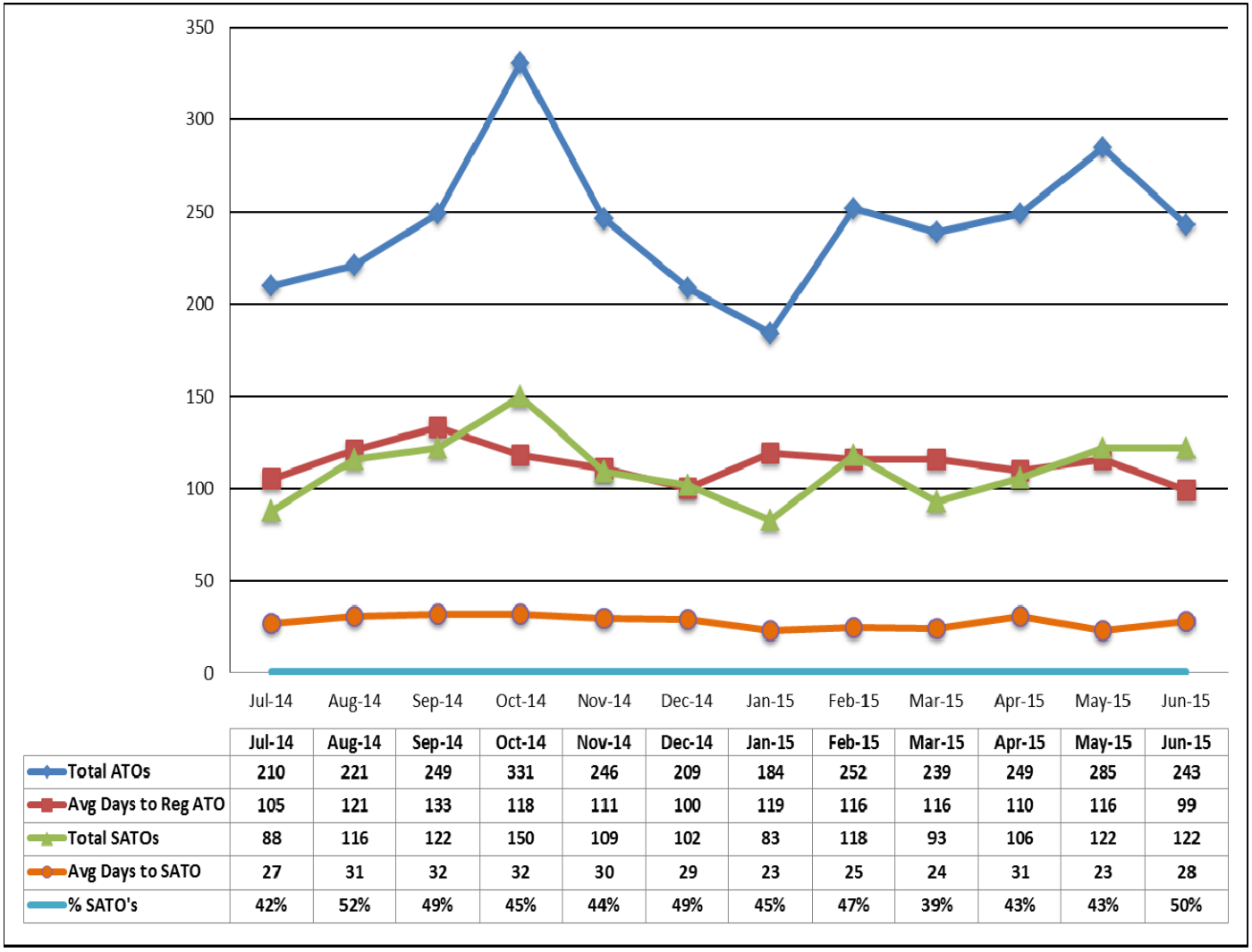
	Jul-14	Aug-14	Sep-14	Oct-14	Nov-14	Dec-14	Jan-15	Feb-15	Mar-15	Apr-15	May-15	Jun-15
# Deficiencies	102	69	86	137	128	101	162	122	106	94	108	88
# Plans w/ Deficiencies	64	56	73	95	109	64	81	75	63	50	76	65
# Plans Reviewed	228	247	317	357	322	279	286	309	281	298	331	329
Avg Deficiency per Plan	0.45	0.28	0.27	0.38	0.40	0.36	0.57	0.39	0.38	0.32	0.33	0.27
Denials	14	10	10	18	12	17	14	5	14	17	15	10
Rejections	4	0	0	0	0	3	4	1	2	2	1	2

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 July 2014- June 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 46% of all ATOs being straight to ATO.



	Jul-14	Aug-14	Sep-14	Oct-14	Nov-14	Dec-14	Jan-15	Feb-15	Mar-15	Apr-15	May-15	Jun-15
Total ATOs	210	221	249	331	246	209	184	252	239	249	285	243
Avg Days to Reg ATO	105	121	133	118	111	100	119	116	116	110	116	99
Total SATOs	88	116	122	150	109	102	83	118	93	106	122	122
Avg Days to SATO	27	31	32	32	30	29	23	25	24	31	23	28
% SATO's	42%	52%	49%	45%	44%	49%	45%	47%	39%	43%	43%	50%

2808 completed validation visits we completed during the preceding 12 months

1587 systems were processed from IATO to ATO status during the preceding 12 months, it took 114 days on average to process a system from IATO to ATO

1331 systems were processed Straight to ATO status during the preceding 12 months, it took 28 days on average to process a system Straight to ATO

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

2122 systems (76%) had no vulnerabilities identified.

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

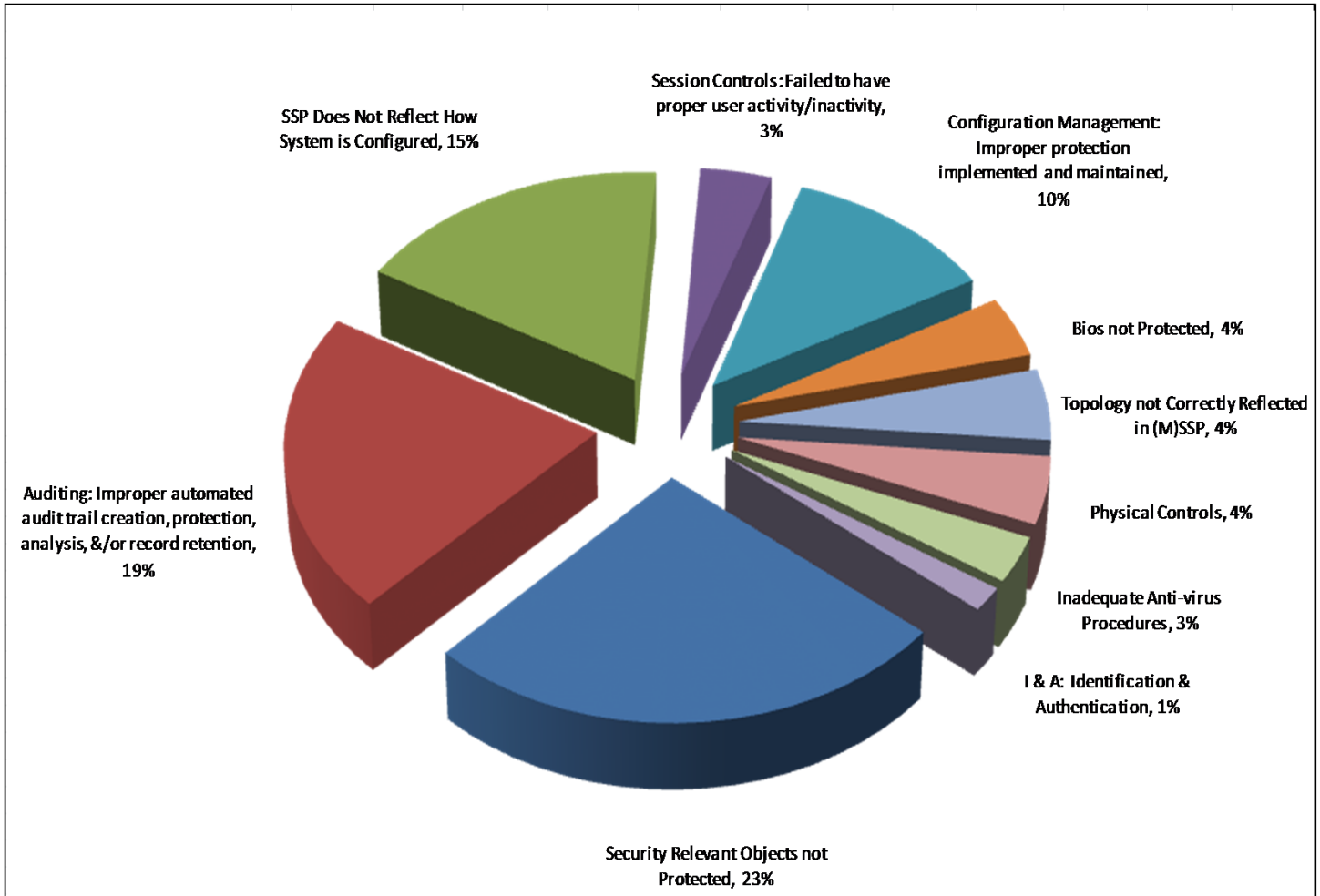
39 systems (1%) had significant vulnerabilities identified, resulting in a second validation visit to the site after corrections were made.

Last Months Snapshot: June 2015

121 ATOs were granted with an average turnaround time of 199 days

122 SATOs were granted with an average turnaround time of 28 days

Common Vulnerabilities found during System Validations from July 2014- June 2015



	Jul-14	Aug-14	Sep-14	Oct-14	Nov-14	Dec-14	Jan-15	Feb-15	Mar-15	Apr-15	May-15	Jun-15
# Vulnerabilities	77	53	81	121	60	48	65	71	51	64	61	52
# Onsites w/ vulnerabilities	52	59	64	108	66	44	44	49	37	53	54	56
# Onsites	212	211	238	327	226	192	171	253	229	238	276	235
Avg Vulnerability per Onsite	0.36	0.25	0.34	0.37	0.27	0.25	0.38	0.28	0.22	0.27	0.22	0.22

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