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

The NISPPAC held its 50th meeting on Wednesday, March 18, 2015, from 10:00 a.m. until noon at the National Archives and Records Administration (NARA), 700 Pennsylvania Avenue, NW, Washington, DC 20408. John Fitzpatrick, Director, Information Security Oversight Office (ISOO) chaired the meeting. Minutes of this meeting were certified on June 17, 2015.

I. Welcome and Administrative Matters

After introductions of those in attendance, Mr. Fitzpatrick welcomed everyone and reminded them that NISPPAC meetings are recorded events and that minutes of the meeting will be provided at a later date. He reminded those present that the primary function of the NISPPAC is to provide an opportunity for the engagement of industry representatives and national level policy officials from key agencies in a dialogue about the state of the National Industrial Security Program (NISP). He emphasized that ISOO and all of the government officials who participate in this process, are continuously grateful for the dedication of industry professionals who sacrifice time from their busy corporate lives to participate in this activity. He then asked Greg Pannoni, ISOO and the NISPPAC Designated Federal Official (DFO), to review the Committee's old business. (See attachment 1 for a list of those in attendance.)

II. Old Business

Mr. Panonni noted there were two action items from the November 19, 2014 NISPPAC meeting. He explained that the first item was the creation of a working group to resolve the myriad of challenges to implementation between the policies of the NISP and other government programs. He stated that the working groups' purpose was to foster integration of policies that impact the NISP. He advised that the Policy Integration Working Group (PIWG) met for the first time on January 29th, 2015. He stated that the second item concerned reestablishing the ad hoc Special Access Program (SAP) Working Group (SAPWG) which reconvened at the request of industry.

III. Reports and Updates

(A) DoD Update:

Valerie Heil, Office of the Under Secretary for Intelligence, OUSDI, began the DoD update noting that the draft of the NISP Operating Manual (NISPOM) Conforming Change 2 (CC2) was in coordination with the NISP Cognizant Security Agencies (CSAs). She emphasized that their goal was to publish the NISPOM change by the end of July 2015. Ms. Heil explained the next step after they receive concurrence from the NISP CSAs would be a legal sufficiency review with the DoD Office of General Council (OGC). She advised that she would have a status update in May to assess if the planned July publication date was still viable. She noted that DoD had centralized its' processing of National Interest Determinations (NIDs) for companies that are

cleared under a special security agreement (SSA) via internal guidance called a Directive Type Memoranda (DTM) and that the new process would be explained during the Defense Security Service (DSS) update.

(B) DSS Update:

Stan Sims, DSS Director, stated that he hosted government and industry stakeholder meetings earlier in the week which focused on topics including the NISP Contract Classification System (NCCS), which is the automated DD-254 (Contract Security Classification Specification), CC2 and its addition of insider threat program requirements. He updated the Committee on efforts to automate the DD-254, and noted that they had been successful in partnering with DoD Acquisition, Technology and Logistics (AT&L) to put the application into the Wide Area Workflow, which is used by all DoD acquisition and contract professionals. Mr. Sims advised that they had just completed beta testing with over 80 people in industry and government and expected initial operational capability by the end of April 2015, and full operational capability by the end of November 2015. He noted that NCCS would provide the ability to increase supply chain risk management because the DD-254s for subcontracts will now be interconnected to their prime contracts. He informed that once CC2 is published, industry will have 180 days to implement that policy.

Mr. Sims transitioned to explaining that the NID DTM signed on February 11th by the OUSDI allows for the centralized processing of NIDs. He explained that a NID is necessitated when a foreign-owned company under an SSA requires access to proscribed information, (TOP Secret, Restricted Data, SAP, Communications Security (COMSEC), or Sensitive Compartmented Information (SCI)). He explained that DSS will be the hub for the centralized processing of NIDs for DoD, and indicated that DSS would do an assessment and propose a decision to the DoD government contracting activity (GCA) to either approve or deny the NID. He noted that the goal was to complete routine NIDs in 30 days. He continued noting that the Performance Accountability Council (PAC) and the Program Management Office (PMO) had discussions about reductions in security clearances and regarding how to clear the backlog of periodic reinvestigations (PRs). He noted that the backlog of overdue PRs was reduced from 50,000 as reported last year to below 4,000.

(C) Combined Industry Presentation

Tony Ingenito, Industry, began his presentation (see attachment 2) by identifying changes in representatives from the Memorandum of Understanding (MOU) organizations. He noted that the Aerospace Industries Association (AIA) is now represented by Keith Waddell and that Dan McGarvey is now the representative for the American Society for Industrial Security (ASIS). He noted that the review and feedback on National Institute for Standards and Technology (NIST) Special Publication (SP) 800-171 didn't raise any significant concerns, and that Industry was awaiting development of the Federal Acquisition Regulation (FAR) clause and insider threat

requirements in CC2. He spoke regarding the impacts of Executive Order (E.O.) 13691 "Promoting Private Sector Cybersecurity Information Sharing," and the resulting changes to E.O. 12829, "National Industrial Security Program." He thanked the Chair for the opportunity to meet with DoD and DHS regarding those changes. He noted that the SAPWG had reconvened and the meeting brought insight into DoD's Volume 1 of the SAP manual pertinent to general procedures and that Volume 3 was currently under DoD legal review. He indicated that the Personal Security Clearance Working Group (PCLWG) was awaiting the Office of the Director for National Intelligence, (ODNI) action in regard to e-Adjudication threshold changes. He noted the PCLWG also examined the Defense Office of Hearings and Appeals (DOHA) and the DoD Central Adjudication Facility (CAF) processes to identify cases that required assignment to DOHA versus those cases that need more adjudicative action by the CAF. Mr. Ingenito acknowledged the work of the Certification and Accreditation (CAWG) working group on suggesting that XP end of life guidance be published on the DSS website. He indicated that the CAWG was also working with the early development of the Risk Management Framework (RMF) from DoD and he touched on the testing for the automated DD-254 and advised that over 25 industry subject matter experts (SME) were eager to participate in the beta test.

(D) PCLWG Report

Mr. Pannoni introduced the PCLWG's report (see attachment 3) by indicating that the backlog of PCL investigations had been reduced from 51,000 PRs to less than 4,000 in one year. He stated that under the Intelligence Reform and Terrorism Prevention Act (IRTPA), the goal is that investigations are to be initiated in 14 days or less but that was not met for fiscal year (FY) 14 due to the government shutdown in October 2013. He stated that testing of click-to sign on the electronic Questionnaire for Investigation Processing (e-Qip) was being worked by the Office of Personnel Management, (OPM) and DoD to help eliminate some of the rejections due to signed releases failing to arrive in time to meet OPM submission timeframes. He reminded the Committee that DSS had advised that Joint Personnel Adjudication System (JPAS) accounts were being turned off if they have had no activity for over a 30 day period. He advised that e-adjudication business rules were under review, with consideration being given to lowering the thresholds in several areas. He indicated that the PCLWG was working with industry, the CSAs and the PAC to review this issue and make recommendations for changes.

Next, Ned Fish, DoD CAF, (see attachment 4) stated that in 2013 there was a growing backlog of approximately 14,000 industry clearance cases. He noted that DOHA had worked through 5,000 of those cases to reduce the number to approximately 3,400 and that about8% of their annual workload on industry clearances was in that backlog, which is now below 2% and still shrinking. He estimated that in early FY 16 they would eliminate that backlog. He indicated that impending changes to federal investigative standards could impact the backlog and that working to change the e-adjudication criteria would be important to reducing the backlog. He stated it was important to increase the number of cases e-adjudicated, while not undermining the capability they have now. He announced that they should be deploying the Case Adjudication

Tracking System (CATS) later this year and anticipated few issues as employees are being trained on the new system. He also stated that 500-day-old-cases are still skewing the 20-day adjudicative timeline and would continue to do so until they eliminate the backlog.

Lisa Loss, OPM, stated that there have been impacts to investigation timeliness due primarily to contract issues with their largest contractor that resulted in a stop work order. . She noted that cases that were in the process of being worked by that contractor had been frozen which caused a buildup of backlogged cases. She indicated that over 75% of those cases not completed were PRs. She noted there were 54,000 cases pending at the time of the stop work order and that they had closed over 40,000 of those. She added that while other contractors providing investigative services had increased their capacity, they are still not seeing the capacity they had prior to the stop work order. She stated that while they were working with their existing contractors to increase capacity, they had begun to backfill federal investigator positions, and have been bringing in some reemployed annuitants to help increase investigative capacity. She stated that they have regular meetings with DoD, ODNI, and other stakeholders through the background investigation stakeholders group, and that there appeared to be an overall increase in effort to eliminate overdue PRs and initial investigations from both industry and government. She also spoke about the OPM data breach and the issues arising from that, as well as the credit monitoring being provided.

(E) CAWG Report

Tracy Brown, DSS, began her presentation (see attachment 5) stating that the CAWG was working with the CSAs to gather details on their process for certification and accreditation of the information systems they approve for industry. She noted that they were evaluating the change management process with CSAs and providing them the DSS Office of the Designated Approval Authority (ODAA) process manual. She stated that as other CSAs were integrated they would identify their common processes. She stated an ad hoc working group to integrate the RMF requirements into the NISP CAWG process had been established and this group was planning to develop a common baseline to review implementation strategies and communications plans. She discussed the DSS ODAA CAWG process approval timeline and noted that the metrics were positive. She indicated that during on site reviews DSS is finding audit controls and security relevant objects not being protected. She discussed the ODAA Business Management System (OBMS) which is designed to automate the CAWG process and indicated that its implementation was on track. Mr. Fitzpatrick opined that the shift to the RMF was a significant change management challenge for the government as well as industry. He encouraged those interested, who were not a part of the working group, to consider joining because that is where the preponderance of classification processing occurs.

(F) PIWG Report and CUI Update

Mr. Fitzpatrick stated that the recently created PIWG which resulted from an action item from the last Committee meeting was an effort to bring into the NISPPAC conversation a discussion about the numerous security policies being implemented and their impact on NISP industry and their government partners. He noted the need to bring all parties together to discuss policy issues because the world of industrial security is more complex and complicated than it was when the NISP was created in 1993. He added that this view had broadened from a singular idea in the original NISP to include: critical infrastructure programs, cyber security, CUI, and the insider threat programs. He advised that industry had expressed concern about the fracturing of the NISP, and that these concerns and expansion of responsibilities led to the creation of the PIWG. He stated that this group was the right NISP body to continue government and industry dialogue to identify the issues and propose solutions. He commented that Mr. Ingenito had reported that industry was tracking over 50 separate initiatives impacting the NISP and that industry had done a good job of bringing the MOU groups together to voice their observations and concerns. He reminded the members that the NISP was constructed to help address concerns whether they arise from industry or government, and to build a true partnership between both entities. He noted that there was an increase in joint meetings relative to the NISP and government/industry interests.

He described a three part strategy in regards to CUI implementation that included the primary initiatives in 2015, the directive for implementing the CUI E.O., which is in a mature state of government review and comment, having passed through the Office of Management and Budget (OMB) interagency process. He advised that after the OMB review there would be provisions for public comments and that members of the NISP would be notified of that event. He advised that it would be very important for industry to review and comment during this time. He stated the second part of the strategy would be the NIST Special Publication 800-171 that has already been through one round of public review and comment, and he anticipated the second review and comment period to begin by the end of March 2015. He reiterated the importance of industry's comments during the public comment period as a way of capturing perspectives from outside of the government. He noted the importance of coming together and having a discussion of the comments and the directive regulatory language to ensure everyone understands and is working together. He reiterated the importance of the NIST Special Publication as the standard for what the government expects from industry when dealing with systems with this applicability. He noted that this NIST publication doesn't have any authority unless it is attached to a contract, and that it could be invoked by any GCA. He advised that the third part of the strategy would be a standard FAR clause for CUI that would relay the IT requirements portion of the contract. He explained the process was designed to navigate the implementation of the NIST RMF guidance in a corporate environment where there would be the need for more flexibility and different ways to approach the same concepts of protection. He noted it would allow one to draw a contrast with the Defense Federal Acquisition Regulation (DFAR) supplement on safeguarding control technical information (CTI), which is a DoD rule that provides guidance for a category that will be CUI. He noted that the title for the NIST Special Publication is "Effectively Implementing

CUI for Non-Federal Partners in Non-Federal Organizations and IT Systems." He summarized that the goal of all of the procurement authorities is to ensure this strategy is kept integrated and that there is clarity regarding what is needed by contracting and security communities.

(G) SAPWG Report

Mr. Pannoni informed the Committee that the SAPWG had met once since the last NISPPAC meeting, and that it was addressing numerous issues including access eligibility and the RMF requirements. He explained that there were numerous vulnerabilities inherent in SAPs and that the normal eligibility determination requirements are considered insufficient, so SAPs can extend access requirements as necessary. He advised that this extra scrutiny shouldn't be viewed as an automatic license for a program security officer to go beyond the baseline in establishing security requirements that are extensive and may be difficult to implement. He stated that the DoD NISPOM supplement will remain in effect until such time as not only CC2 is published, but also the four DoD volumes of the SAP Manual. He stated that he did not have a timeframe for the completion of Volume 3, (physical security) and Volume 1 (general requirements) which are both within DoD legal sufficiency review. He explained that Volume 2 (Personnel Security) is with the DoD Counterintelligence (CI) office and will subsequently undergo a legal sufficiency review. He noted that the CSAs have raised the question that when the NISPOM supplement is replaced, will they have to follow Appendix D under CC2 to the NISPOM, which seems to lack the detail of the current NISPOM Supplement. Mr. Pannoni advised that Appendix D refers to each agency's own directives by and large for implementation, and noted that getting all agencies on the same page would be a challenge as each agency can have additional policies, authorities and prerogatives depending on their specific SAP requirements. He advised that the SAPWG had identified plans for moving forward, such as the establishment of sound and reasonable standards that are collectively agreed to by all the CSAs. He noted that the group identified some impediments in the DoD Joint Special Access Program Implementation Guide (JSIG) relating to its structure and the need for more education and training for both government and industry personnel. Mr. Pannoni stated that the JSIG includes the RMF which provides some latitude for implementation of the requirements as well as the tailoring out of requirements. He noted that the SAPWG planned to meet again in May. Ms. Heil clarified that while there was no timeframe mentioned for publication of NISPOM CC2 and the DoD SAP policy issuances, OUSDI was closely monitoring the process and working closely with their Office of General Council. She advised that while these are a priority, they do know that they will not publish NISPOM CC2 until all four SAP volumes have been published. The Chair noted that it was important to find consistency across programs to prevent the continuing escalation of requirements over time, and commended the SAPWG for the dedication they brought to this issue.

(H) Impact of E.O. 13691 on the NISP

The Chair advised that on February 13th the President signed E.O. 13691, which has direct implications for the NISP. He explained that as E.O. 12829, is the primary NISP policy document for a single, cohesive and integrated program, E.O. 13691 is now the primary policy document for improving cyber security posture and its contribution to the national interest and national security. He noted that E.O. 13691 intends to create an environment that promotes cyber security information sharing among partners and entities that are both federal and non-federal, that are US and non-US, and that the national interest and national security are served by the strongest possible cyber security partners with the government. He opined that making them stronger involves information sharing, and that the information sharing can be and should be private sector to private sector, government to private sector and in some instances it can be government-classified information to select entities. Mr. Fitzpatrick noted that E.O. 13691 sets up a new mechanism and promotes the creation of Information Sharing and Analysis Organizations (ISAOs), and a way for the government to foster them for their own purposes. He detailed that within an energy, financial services, or transportation sector, or any of the critical infrastructure sectors, the entities that work in those areas should be talking to each other to promote the security and the strength of the cyber security programs, and that when a government entity engages with a private entity in a legally binding agreement that involves classified information, they invoke the NISP. He noted that the Secretary of Homeland Security has for five years had the authority to pick private sector individuals, and approve them for security clearances, and to provide them with threat information they need to perform their jobs. He explained that E.O. 13691 builds upon this existing authority to clear individuals and it states that there are times that DHS will engage in an agreement with a company, organization, or entity and obligate that entity to sharing information that includes classified data. He stated that this was normally accomplished by the NISP, where companies that engage in classified contracts sign up knowing there will be a cost and infrastructure requirement to meet those requirements. He noted, however, that in the cyber environment, where there are money free obligations being built, and where there is no remuneration to a company to join into one of these information-sharing alliances, and to benefit from the context provided by an alliance to an ISAO, even when the benefit provided by access to classified threat information will not offset what it takes to build a NISP type infrastructure. The Chair advised that a secondary impact of DHS needing to make the decisions it needs in regards to creating ISAOs and to have the program be as strong as the President envisioned, are addressed in E.O. 13691amendments to E.O. 12829, which make DHS a NISP CSA in partnership with other CSAs in the realm of critical infrastructure protection programs. He noted it gives them the responsibility of adding to the NISPOM portion of the guidance that will be implemented for all, relative to these new kinds of approvals. He stated that as a CSA, DHS would continue to operate through an agency memorandum of understanding with DoD to prevent duplication of effort and cost. The Chair mentioned the reference Ms. Heil made to the NISPOM rewrite, regarding setting up a process for DoD and DHS to make these new efforts work, and noted that they were going through the

process to get those procedures authorized by the Executive Office of the President; and once completed they will be made available, and DHS and DSS will begin to work them.

IV. General Open Forum/Discussion

The Chair opened the meeting to comments from the attendees, and requested inputs on any issues or topics impacting the Committee. There were no comments offered by those in attendance.

V. Closing Remarks and Adjournment

The Chair reminded everyone that the next NISPPAC meeting is scheduled for July 15th at 10:00 a.m. in the Archivists Reception room. He noted that the budget forecast for FY 2015 maintains the status quo with previous budgets, and that as such there will be no travel funds available for our industry representatives. He reiterated that he was grateful for all who attend the meetings on their own, and thanked their company leadership for sponsoring their travel. He reminded the members that a dial-in capability will again be available for any who cannot travel to the meetings. The Chair adjourned the meeting at 11:57 a.m.

Attachment #1

Attachment 1

NISPPAC MEETING ATTENDEES/ABSENTEES

The following individuals attended the March 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
• Stephen Lewis	Department of Defense	Member
• Kim Baugher	Department of State	Member
• David Lowy	Department of the Air Force	Member
• Jeffrey Bearor	Department of the Navy	Member
• Jeff Moon	National Security Agency	Member
• Anna Harrison	Department of Justice	Member
• Kathy Healey	National Aeronautics & Space Administration	Member
• Marc Brooks	Department of Energy	Member
• Scott Ackiss	Department of Homeland Security	Member
• Anthony Ingenito	Industry	Member/Presenter
• Martin Strones	Industry	Member
• William Davidson	Industry	Member
• Michelle Sutphin	Industry	Member
• Richard Graham	Industry	Member
• Philip Robinson	Industry	Member
• Steven Kipp	Industry	Member
• Keith Minard	Defense Security Service	Alternate
• Eric Dorsey	Department of Commerce	Alternate
• Anthony Smith	Department of Homeland Security	Alternate
• Mark Nolan	Department of the Army	Alternate
• Brent Younger	Department of the Air Force	Alternate
• Valerie Heil	Department of Defense	Alternate/Presenter
• Valerie Kerben	Nuclear Regulatory Commission	Alternate
• Kathleen Branch	Department of Defense	Alternate
• George Ladner	Central Intelligence Agency	Alternate
• Richard Hohman	Office of the Director of National Intelligence	Alternate
• Zudayyah Taylor-Dunn	National Aeronautics & Space Administration	Alternate
• Lisa Loss	Office of Personnel Management	Presenter
• Edward Fish	Department of Defense	Presenter
• Laura Hickman	Defense Security Service	Presenter
• Tracy Brown	Defense Security Service	Presenter
• Gary Novotny	Office of the Director of National Intelligence	Attendee
• Michael Witt	MOU Representative	Attendee
• Mark Rush	MOU Representative	Attendee
• Kirk Poulsen	MOU Representative	Attendee
• Dan McGarvey	MOU Representative	Attendee
• Leonard Moss, Jr.	MOU Representative	Attendee

• Igor Gardner	Department of Defense	Attendee
• Priscilla Matos	Department of Defense	Attendee
• Kenneth Campbell	Central intelligence Agency	Attendee
• Charlie Rogers	Department of Homeland Security	Attendee
• Lisa Loss	Office of Personnel Management	Attendee
• Glen Clay	Department of Navy	Attendee
• Mitch Lawrence	Industry	Attendee
• Mark Ryan	Industry	Attendee
• Mark Theby	Industry	Attendee
• Jim Euton	Industry	Attendee
• Richard Ray	Industry	Attendee
• Michael Scheimer	Industry	Attendee
• Dick Weaver	Industry	Attendee
• Lloyd Gant	Industry	Attendee
• Sarah Ballard	Industry	Attendee
• Stacy Woodard	Industry	Attendee
• Susan McCathern	Industry	Attendee
• Rhonda Peyton	Industry	Attendee
• Dennis Arriaga	Industry	Attendee
• John Dean	Industry	Attendee
• Mary Albright	Industry	Attendee
• Jim Martin	Industry	Attendee
• Carla Whitehorn	Industry	Attendee
• Ricky Velez	Industry	Attendee
• Norman Pashoran	Industry	Attendee
• Joe Marks	Reporter	Attendee
• Alegra Woodard	Information Security Oversight Office	Attendee
• David Best	Information Security Oversight Office	Staff
• Robert Tringali	Information Security Oversight Office	Staff
• Joseph Taylor	Information Security Oversight Office	Staff
• Michael Manning	Information Security Oversight Office	Staff

Attachment #2

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

Industry

18 March 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	American Systems Corp.	2018
Martin Strones	Strones Enterprises	2018

National Industrial Security Program

Industry MOU Members

AIA *	Keith Waddell
ASIS *	Dan McGarvey
CSSWG	Mark Rush
ISWG	Karen Duprey
NCMS	Leonard Moss
NDIA	Mike Witt
Tech America	Kirk Poulsen

* Change in MOU Rep in Jan 2015

Security Policy Update

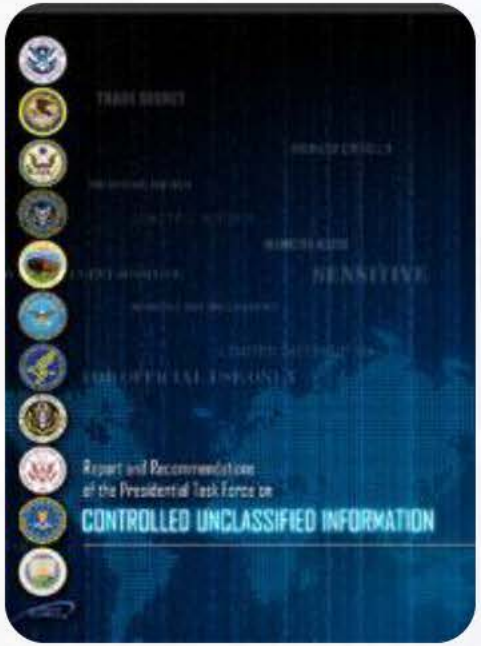
Executive Order #13556

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. thru 16 Jan 15.
    - Initial feedback from industry were no significant concerns.
    - Awaiting any feedback.
  - 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.

Security Policy Update

Executive Order #13691

EO # 13691

Promoting Private Sector Cybersecurity Information Sharing

13 February 2015

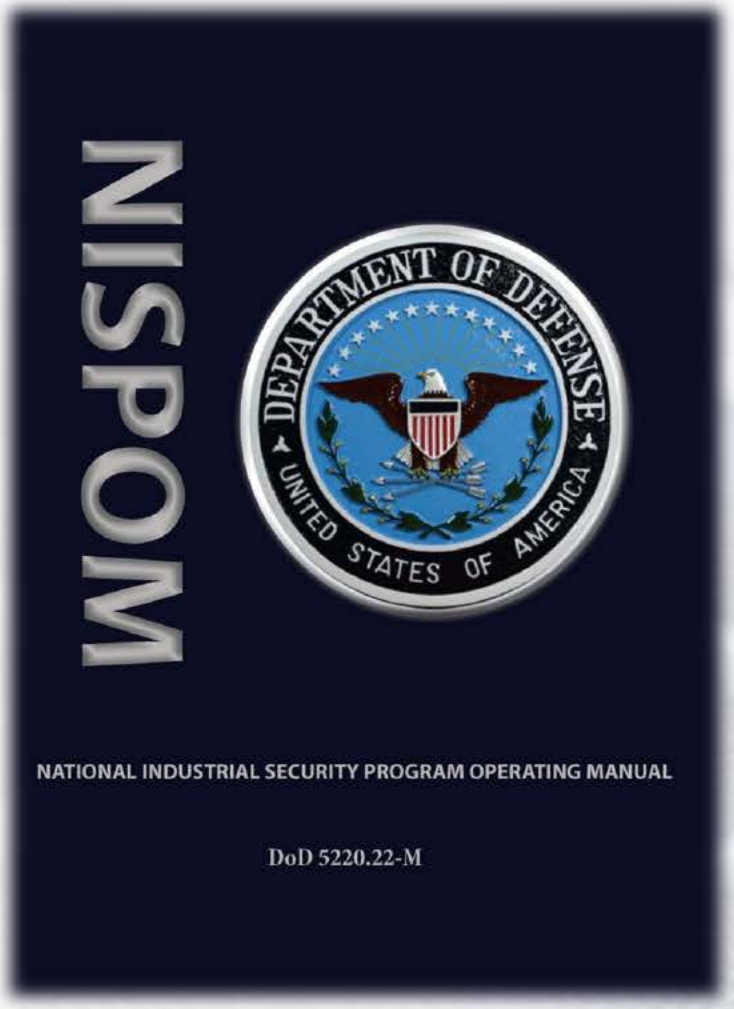
Department of Homeland Security

- 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.

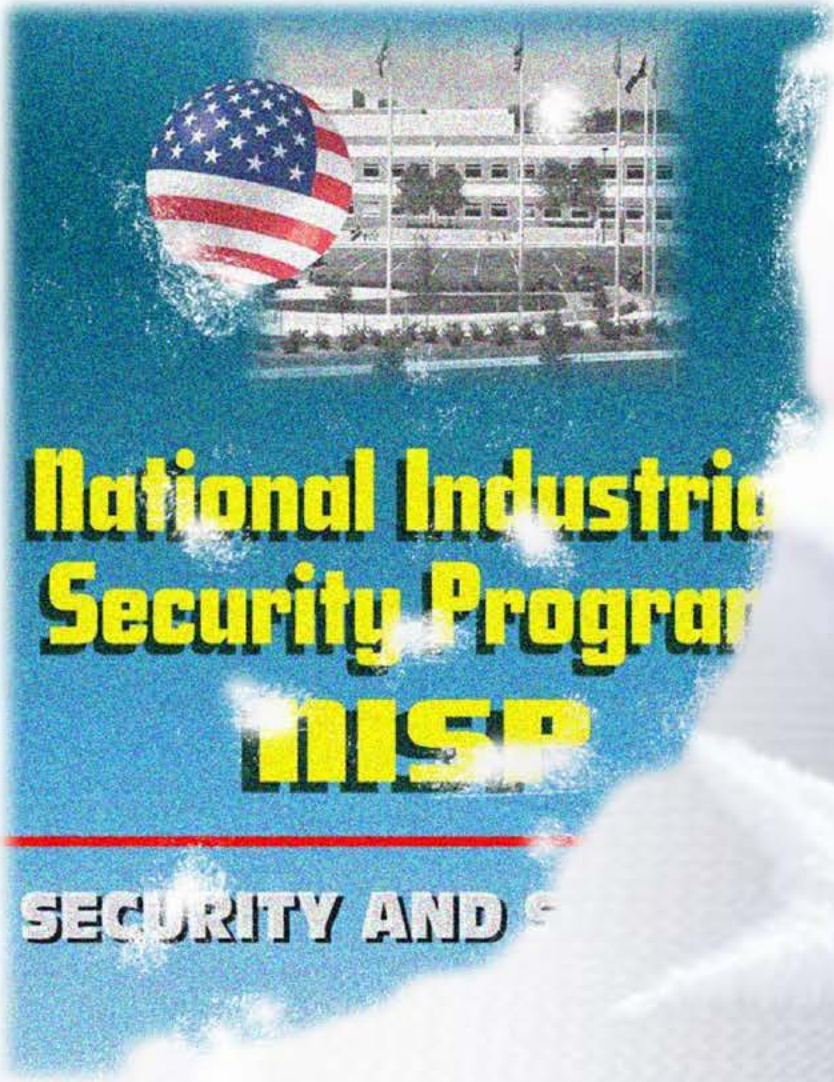
Security Policy Update

Industrial Security Policy Modernization



- National Industrial Security Program Operating Manual revision and update
  - Industry provided comments on draft Jun/July 2010
  - Expecting re-review of draft as next version progresses
- Department of Defense Special Access Program Manual development
  - Vol 1 (General procedures) and Vol 3 (Physical Sec) in legal review
  - Special Access Program (SAP) Supplement being eliminated upon publication of 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.
- 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 50 initiatives
- NISPPAC Policy Integration working group established with initial kick-off meeting

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.
    - Good progress in Sequestration backlog recovery plan.
    - Focused on the e-signature (click-to-sign) testing to address reject submittals.
- Automated Information System Certification and Accreditation
  - Provided DSS & OSD suggested XP End of Life guidance to mitigate the impacts across existing programs, including testing equipment. Guidance promulgated out to industry community.
  - Working group beginning collaborate on incorporating the Risk Management Framework (RMF) into future process manual updates. Early collaboration on this initiative will be key to successful transition.

National Industrial Security Program

Policy Advisory Committee Working Groups (cont.)

- 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.
- SAP Working Group
  - Numerous situations with inconsistent guidance and implementation of changes relating to JSIG (RMF), TPI and PerSec.
  - Formalize working group established and initial meeting held.
  - Open and honest dialogue. Look forward to future meetings and metric collection to support process inconsistencies.

Attachment #3

NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE

Personnel Security Clearance (PCL) Working Group Report

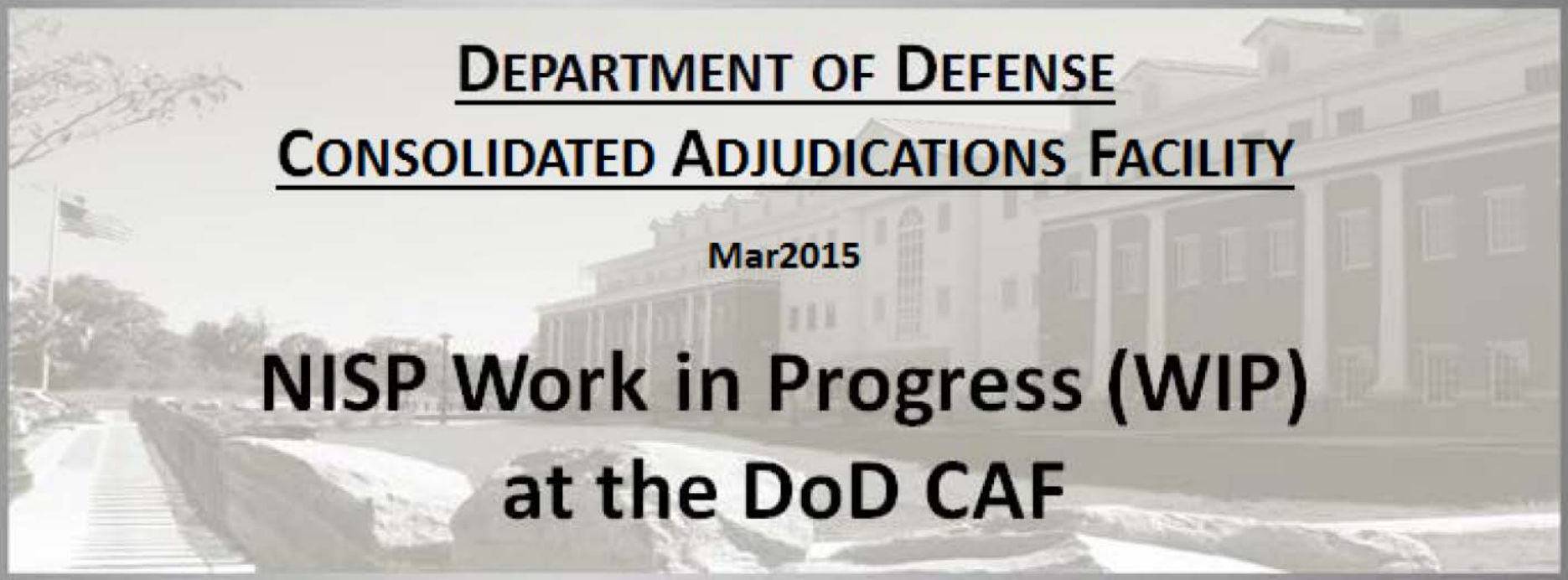
March 18, 2015

Personnel Security Working Group (PCLWG) Report

OPM Performance metrics data for DoD, DOE, NRC, as well as the PSMO update are in folders and will be posted with NISPPAC minutes. Highlights 3/4/2015 meeting included:

- **PSMO reports:**
  - **PSI Initiation: IRTPA 14 days; Industry did not meet in FY14.**
  - **Industry Overdue PR inventory down due to Data Quality Initiative. Now at <4000 cases down from 51,000 in March 14**
  - **Testing Click to sign e-QIP release forms**
  - **JPAS accounts-keep active-(Inactivated >30 days. Deleted > 45)**
- **Discussion of "e-adjudication business rules"- impact of raising thresholds (OUSDI & DODCAF working with OPM & ODNI to address issues).**
- **A DoD initiated "data quality initiative" that would change case files with "at DOHA" annotation to "Pending Adjudication".**

Attachment #4

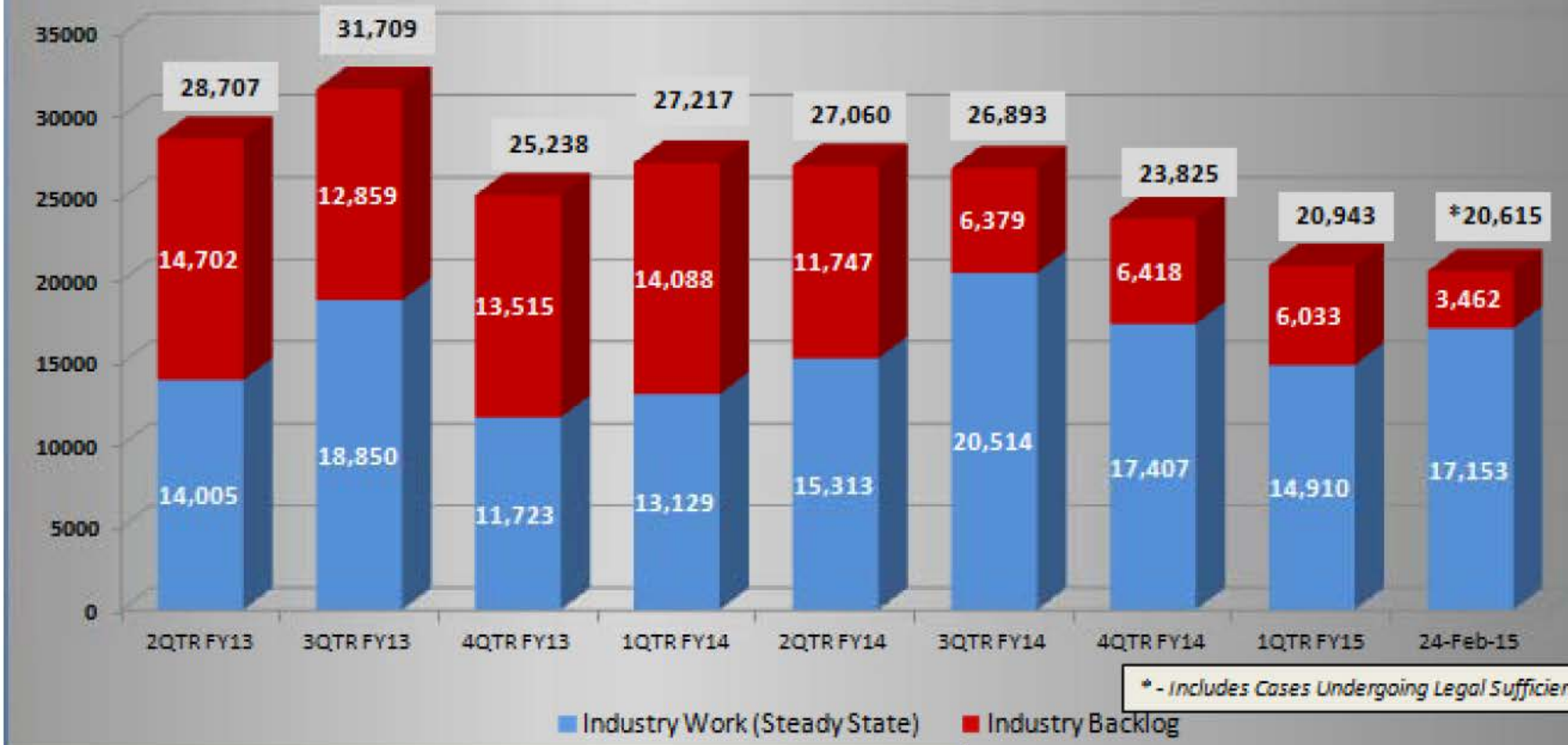


DEPARTMENT OF DEFENSE
CONSOLIDATED ADJUDICATIONS FACILITY

Mar2015

NISP Work in Progress (WIP) at the DoD CAF

DoD CAF NISP WIP



*- *Includes Cases Undergoing Legal Sufficiency Review*

- **Backlog likely to endure into early 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%
February 15	3,462		1.9%
	-10,053	~ 180,000	

Industry
Intelligence Reform and Terrorism Prevention Act Performance FY13-FY15 to Date

- Both NISP and non-NISP timeliness metrics increased as backlogs addressed
- Timeliness to fluctuate throughout FY15 until Industry backlog is fully eliminated

DoD CAF
Bldg. 600, 10th Street, FGGM

Attachment #5

NISPPAC C&A Working Group Update for the Committee

March 2015

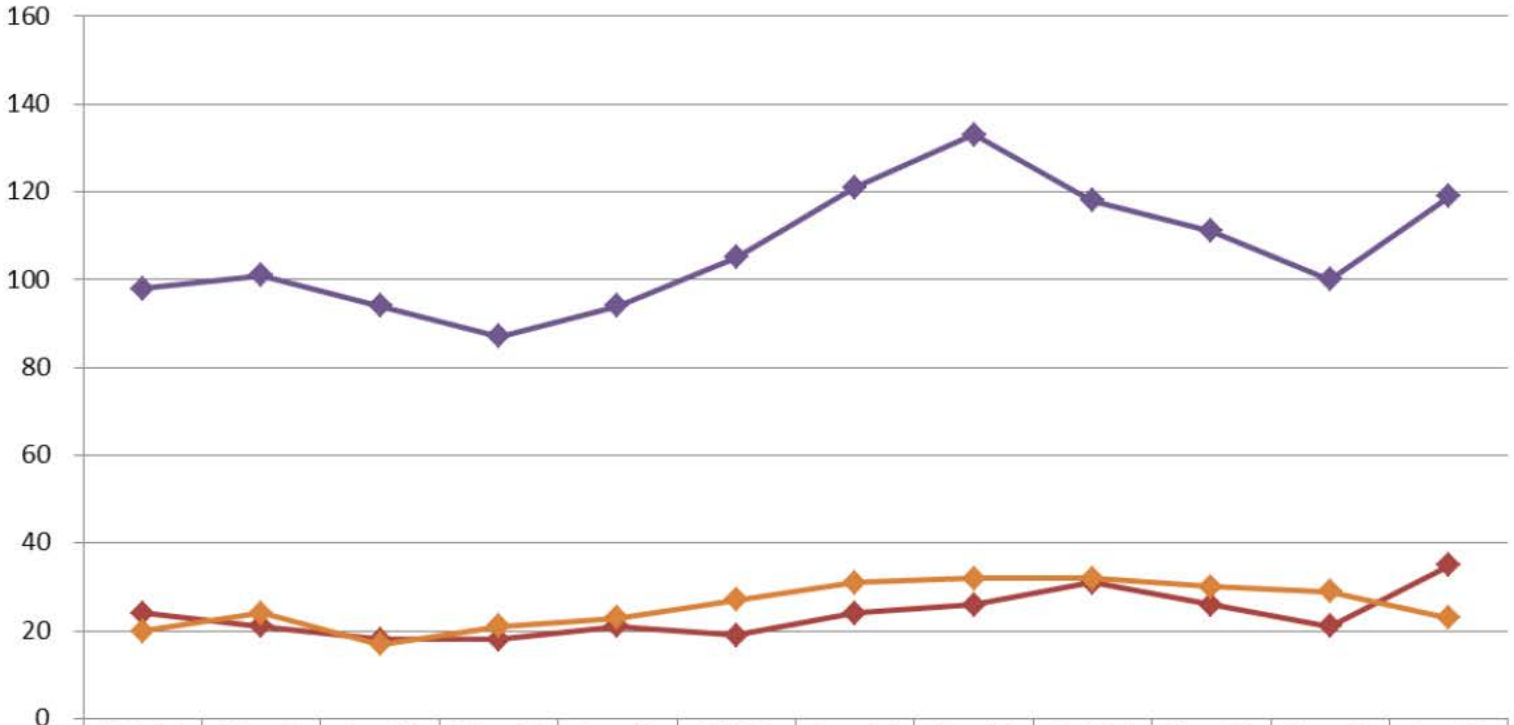
Working Group Initiatives

- 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 C&A WG has stood up an Ad Hoc Risk Management Framework (RMF) WG to integrate RMF into the NISP

DSS ODAA Approval Timeliness



	Feb-14	Mar-14	Apr-14	May-14	Jun-14	Jul-14	Aug-14	Sep-14	Oct-14	Nov-14	Dec-14	Jan-15
IATO Amount	179	213	204	270	120	122	121	185	189	201	157	185
IATO Timeliness	24	21	18	18	21	19	24	26	31	26	21	35
Reg ATO Amount	171	212	191	187	164	122	105	127	181	137	107	101
ATO Timeliness	98	101	94	87	94	105	121	133	118	111	100	119
SATO Amount	151	148	128	121	120	88	116	122	150	109	102	83
SATO Timeliness	20	24	17	21	23	27	31	32	32	30	29	23

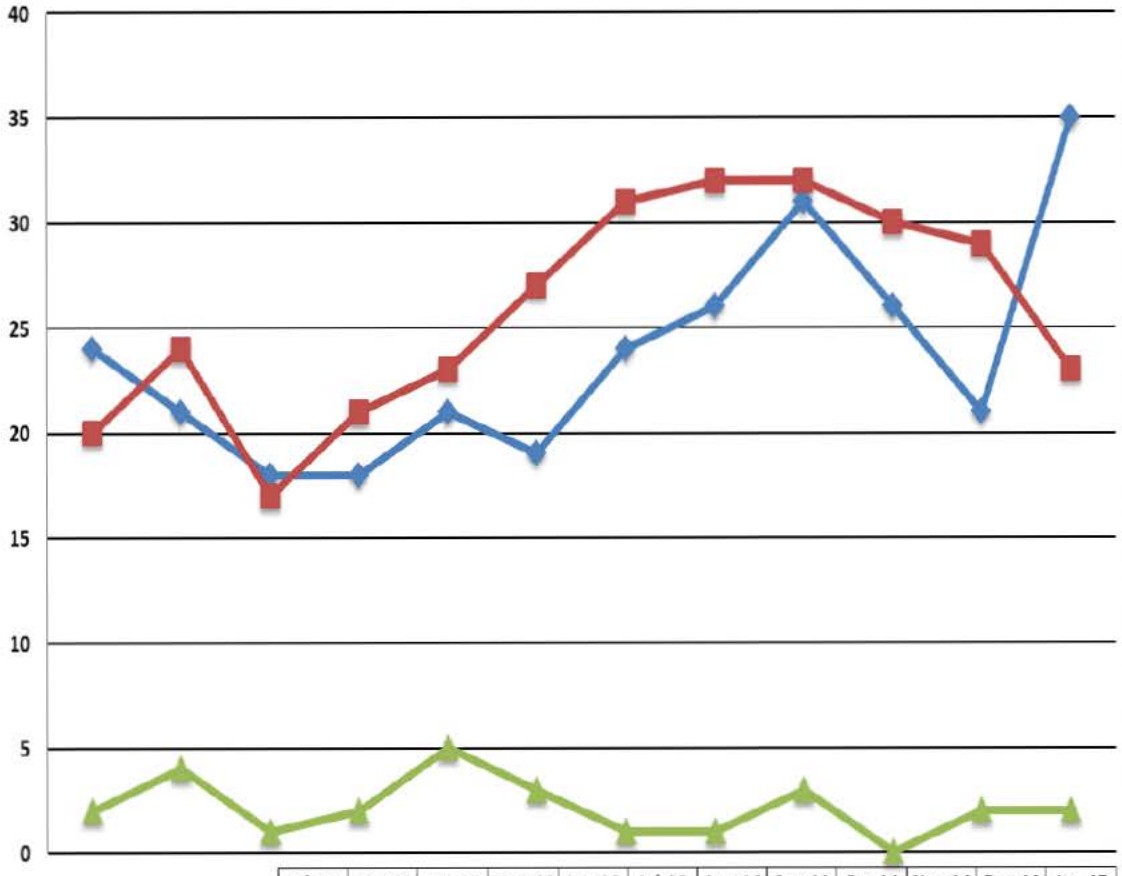
Takeaways:

- 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 Feb 2014- Jan 2015



	Feb-14	Mar-14	Apr-14	May-14	Jun-14	Jul-14	Aug-14	Sep-14	Oct-14	Nov-14	Dec-14	Jan-15
Time from DSS Reciept of plans to Granting of IATOs	24	21	18	18	21	19	24	26	31	26	21	35
Time from DSS Reciept of plans to Granting of SATOs	20	24	17	21	23	27	31	32	32	30	29	23
Industry Response Time to DSS Questions, Comments	2	4	1	2	5	3	1	1	3	0	2	2
Second IATOs	5	9	5	8	4	4	10	11	13	11	9	8

3858 System security plans (SSPs) were accepted and reviewed during the preceding 12 months.

2146 Interim approvals to operate (IATOs) were issued during the preceding 12 month period, it took an average of 24 days to issue an IATO after a plan was submitted.

1438 "Straight to ATO (SATO)" were processed during the preceding 12 months, it took an average of 26 days to issue the ATO.

998 of the SSPs (26%) required some level of correction prior to conducting the onsite validation.

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

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

Denials: 232 of the SSPs (6%) were received and reviewed, but denied IATO until corrections were made to the plan.

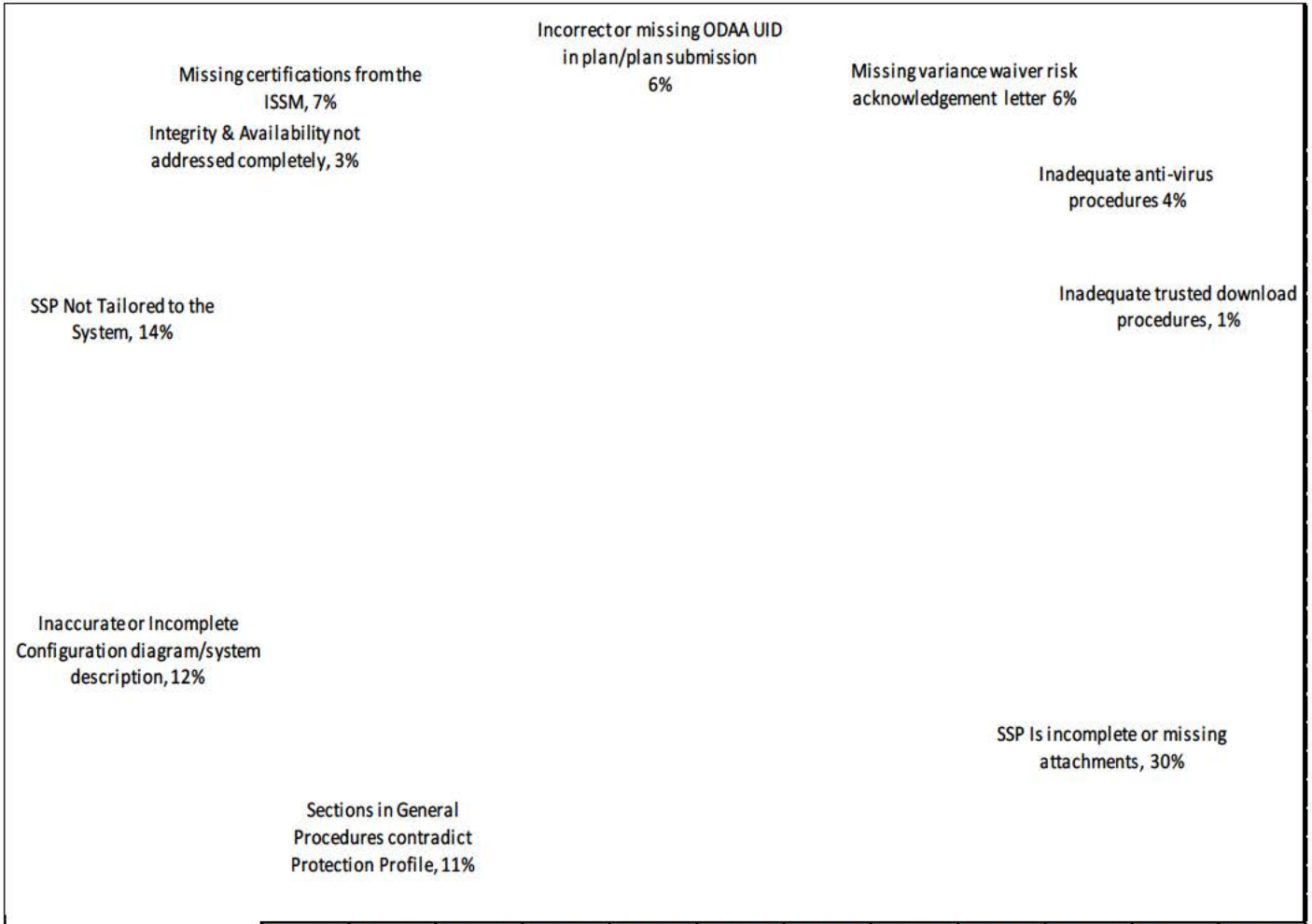
Rejections: 42 of the SSPs (1%) were not submitted in accordance with requirements and were not entered into the ODAA process. These SSPs were returned to the ISSM with guidance for submitting properly and processed upon resubmission.

Last Months Snapshot: Jan 2015

185 IATOs were granted with an average turnaround time of 35 days

83 SATOs were granted with an average turnaround time of 23 days

Common Deficiencies in Security Plans from Feb 2014- Jan 2015



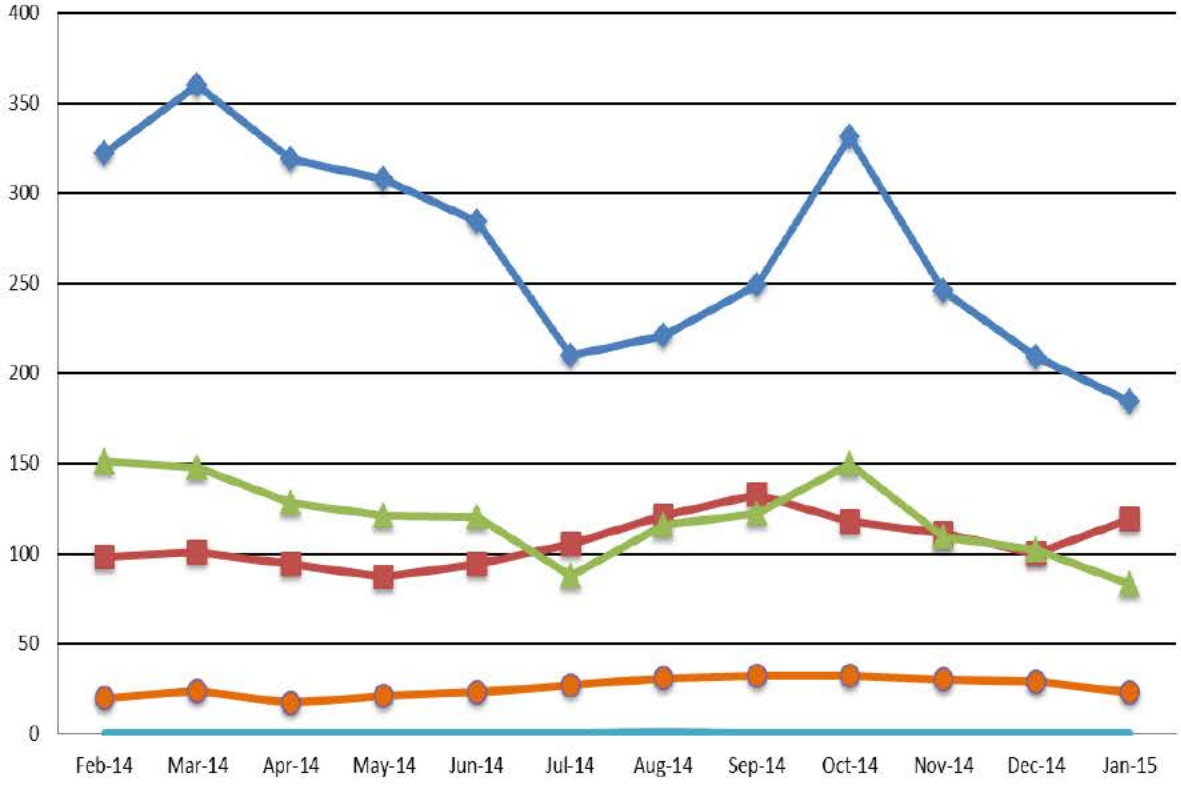
	Feb-14	Mar-14	Apr-14	May-14	Jun-14	Jul-14	Aug-14	Sep-14	Oct-14	Nov-14	Dec-14	Jan-15
# Deficiencies	146	178	179	258	154	102	69	86	137	128	101	162
# Plans w/ Deficiencies	89	92	90	140	87	64	56	73	95	109	64	81
# Plans Reviewed	357	396	363	431	275	228	247	317	357	322	279	286
Avg Deficiency per Plan	0.41	0.45	0.49	0.60	0.56	0.45	0.28	0.27	0.38	0.40	0.36	0.57
Denials	22	31	28	30	26	14	10	10	18	12	17	14
Rejections	5	4	3	10	9	4	0	0	0	0	3	4

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 Feb 2014- Jan 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 44% of all ATOs being straight to ATO.



	Feb-14	Mar-14	Apr-14	May-14	Jun-14	Jul-14	Aug-14	Sep-14	Oct-14	Nov-14	Dec-14	Jan-15
Total ATOs	322	360	319	308	284	210	221	249	331	246	209	184
Avg Days to Reg ATO	98	101	94	87	94	105	121	133	118	111	100	119
Total SATOs	151	148	128	121	120	88	116	122	150	109	102	83
Avg Days to SATO	20	24	17	21	23	27	31	32	32	30	29	23
% SATO's	47%	41%	40%	39%	42%	42%	52%	49%	45%	44%	49%	45%

3084 completed validation visits we completed during the preceding 12 months

1805 systems were processed from IATO to ATO status during the preceding 12 months, it took 105 days on average to process a system from IATO to ATO

1438 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, (44%) of ATOs were for systems processed Straight to ATO

2252 systems (73%) had no vulnerabilities identified.

776 systems (25%) had minor vulnerabilities identified that were corrected while onsite.

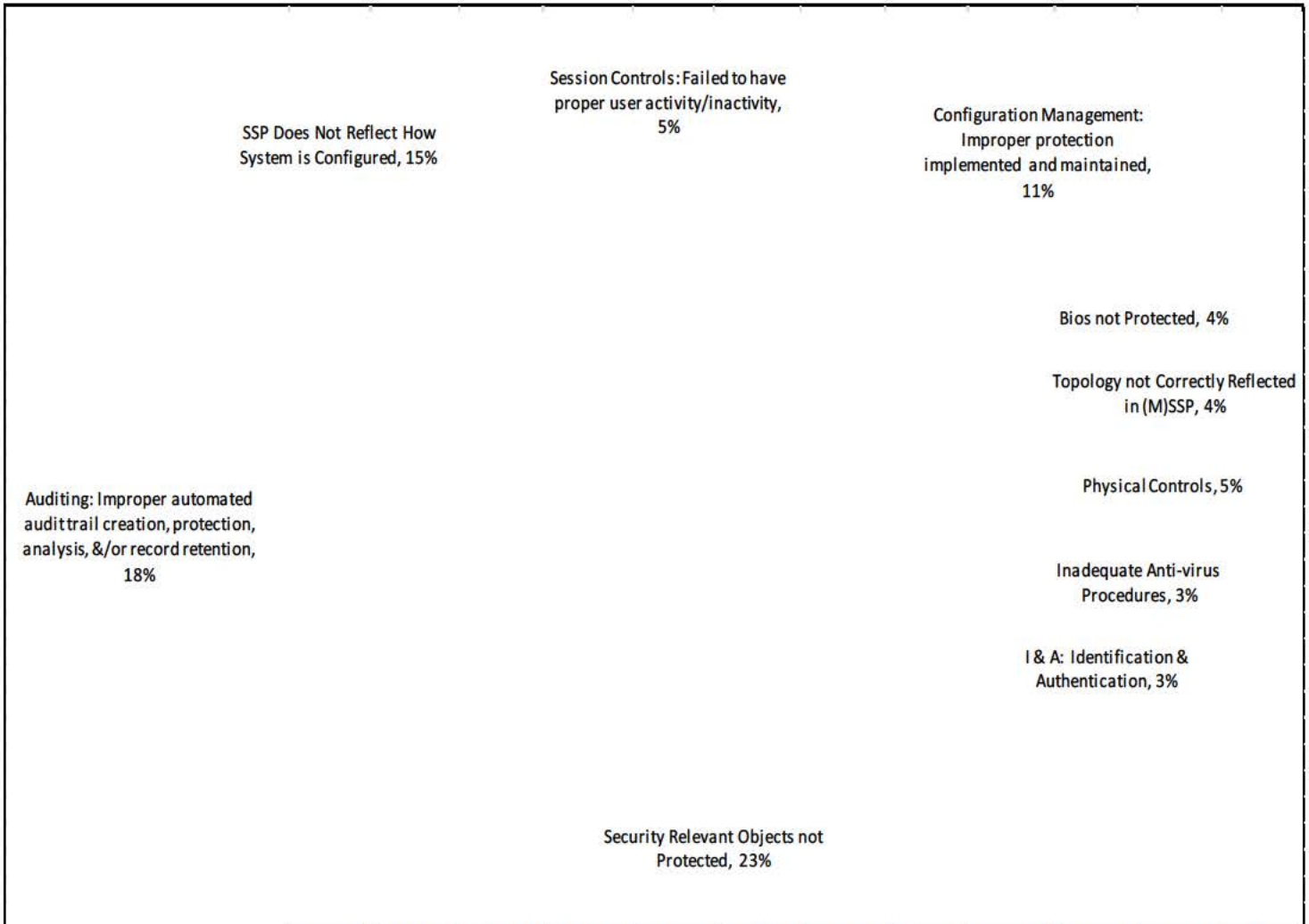
56 systems (2%) had significant vulnerabilities identified, resulting in a second validation visit to the site after corrections were made.

Last Months Snapshot: Jan 2015

101 ATOs were granted with an average turnaround time of 119 days

83 SATOs were granted with an average turnaround time of 23 days

Common Vulnerabilities found during System Validations from Feb 2014- Jan 2015



	Feb-14	Mar-14	Apr-14	May-14	Jun-14	Jul-14	Aug-14	Sep-14	Oct-14	Nov-14	Dec-14	Jan-15
# Vulnerabilities	114	133	96	76	114	77	53	81	121	60	48	65
# Onsites w/ vulnerabilities	78	90	81	62	84	52	59	64	108	66	44	44
# Onsites	309	342	295	301	260	212	211	238	327	226	192	171
Avg Vulnerability per Onsite	0.37	0.39	0.33	0.25	0.44	0.36	0.25	0.34	0.37	0.27	0.25	0.38

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

DoD CSA Provided Guidance
ODAA Process Manual – Working Group Initiative

- IP Policy presented the C&A working group with a proposed change management process for the ODAA Process Manual to make it a living document

- Change Management Team (CMT) made up of Industry (NISPPAC C&A Member), ODAA, and Policy (Lead)

  - Provides clarification to processes and policies in timely fashion

  - Designate transition appropriate for each change based on risk/resources

  - Responsive to new cyber threats and vulnerabilities

  - Allows for quicker integration of DoD and Federal standards

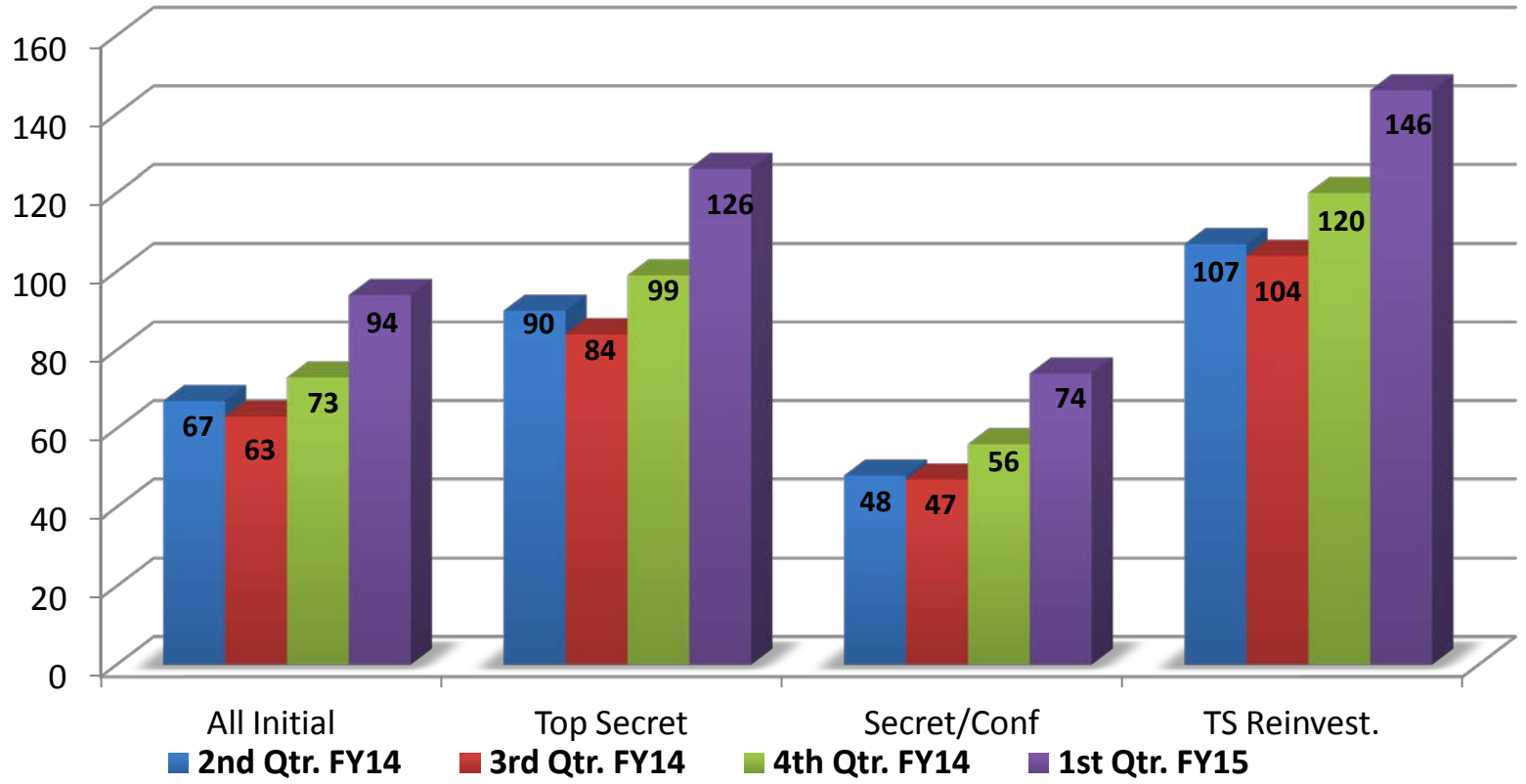
  - Working group members reviewing for comment - initial reception was good

a New Day for Federal Service

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

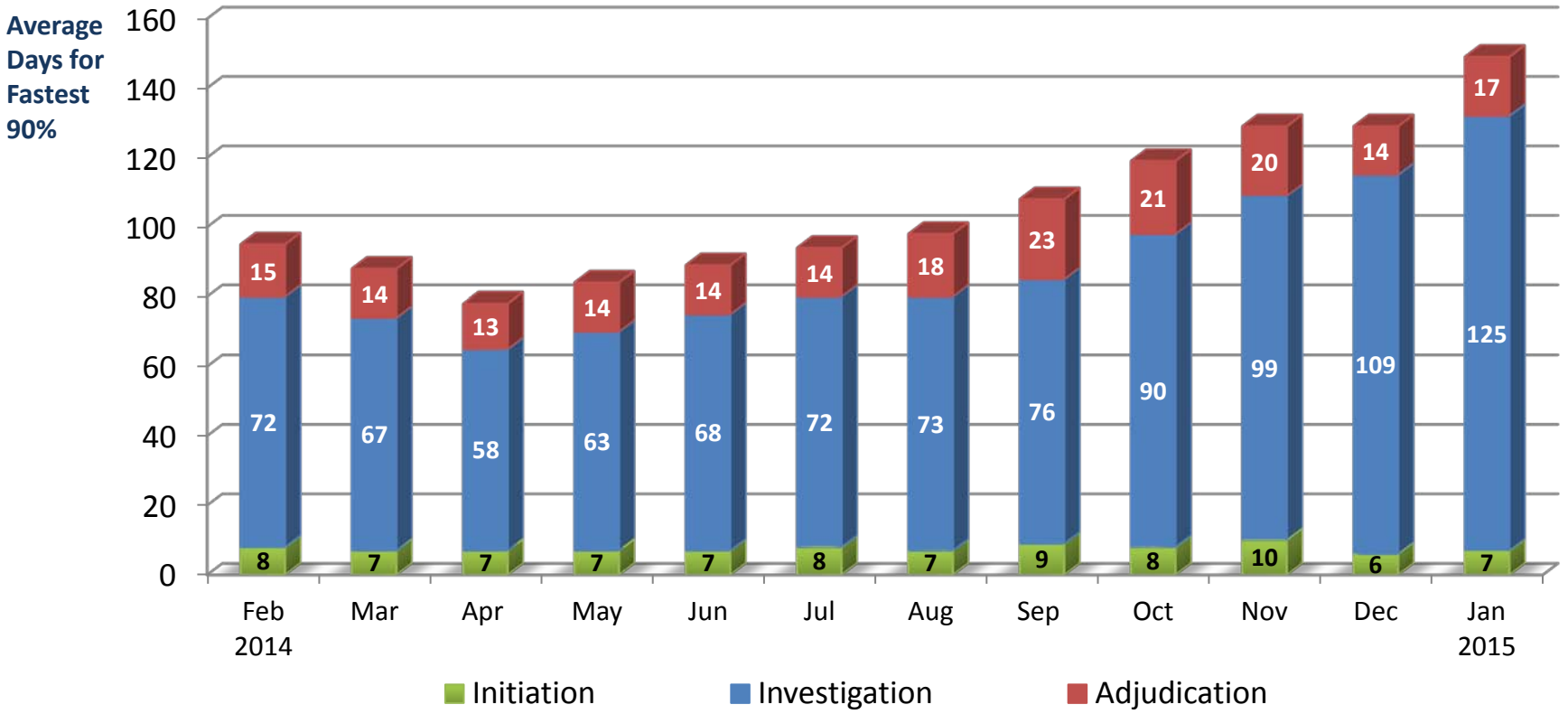
Timeliness Performance Metrics for DOE's Personnel Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 2nd Q FY14	1,547	724	823	2,578
Adjudication actions taken – 3rd Q FY14	1,515	695	820	2,619
Adjudication actions taken – 4th Q FY14	1,311	559	752	2,250
Adjudication actions taken – 1st Q FY15	1,431	552	879	1,338

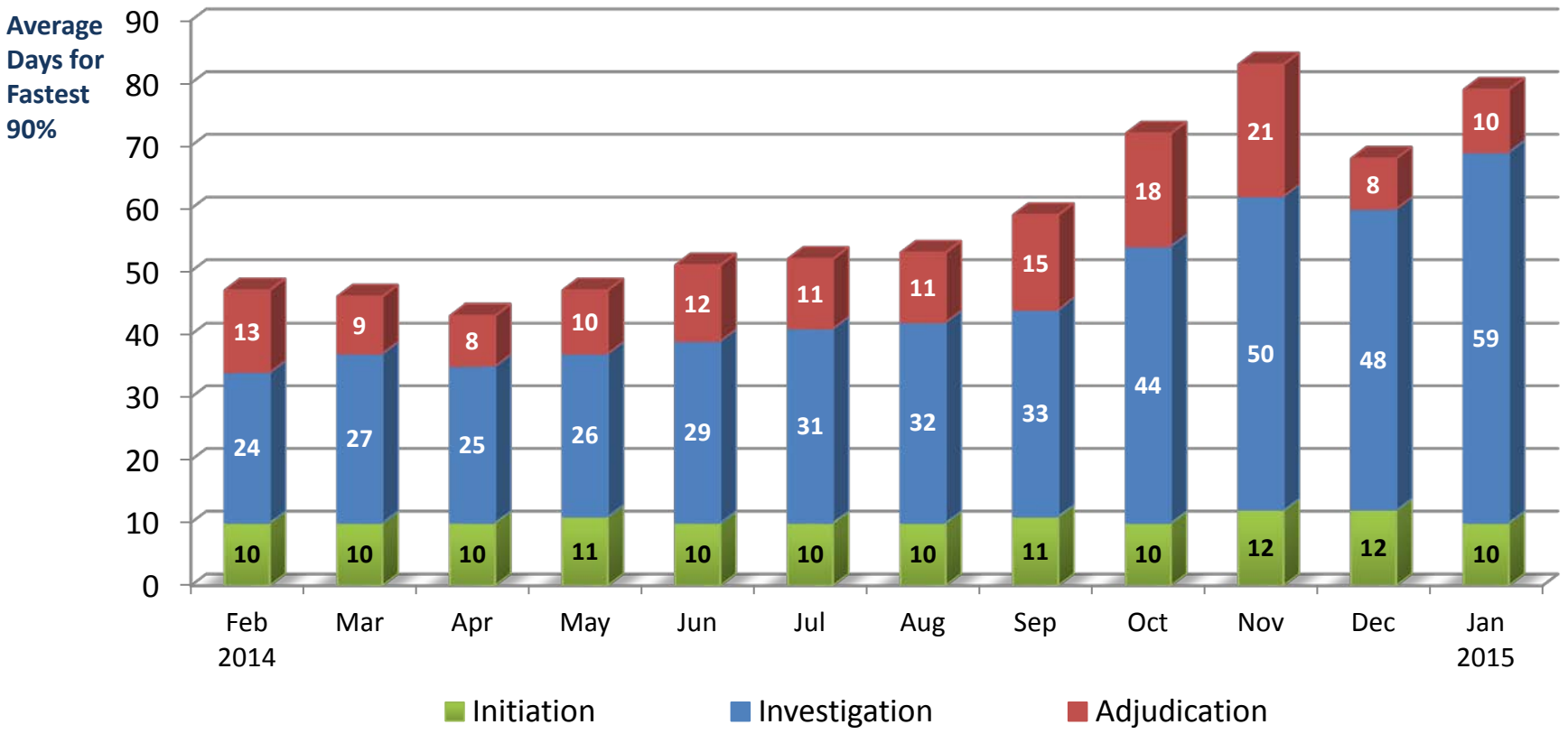
DOE's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



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

	Feb 2014	Mar 2014	Apr 2014	May 2014	Jun 2014	Jul 2014	Aug 2014	Sep 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015
100% of Reported Adjudications	221	239	219	261	204	219	204	118	171	191	184	152
Average Days for fastest 90%	95 days	88 days	78 days	84 days	89 days	94 days	98 days	108 days	119 days	129 days	129 days	149 days

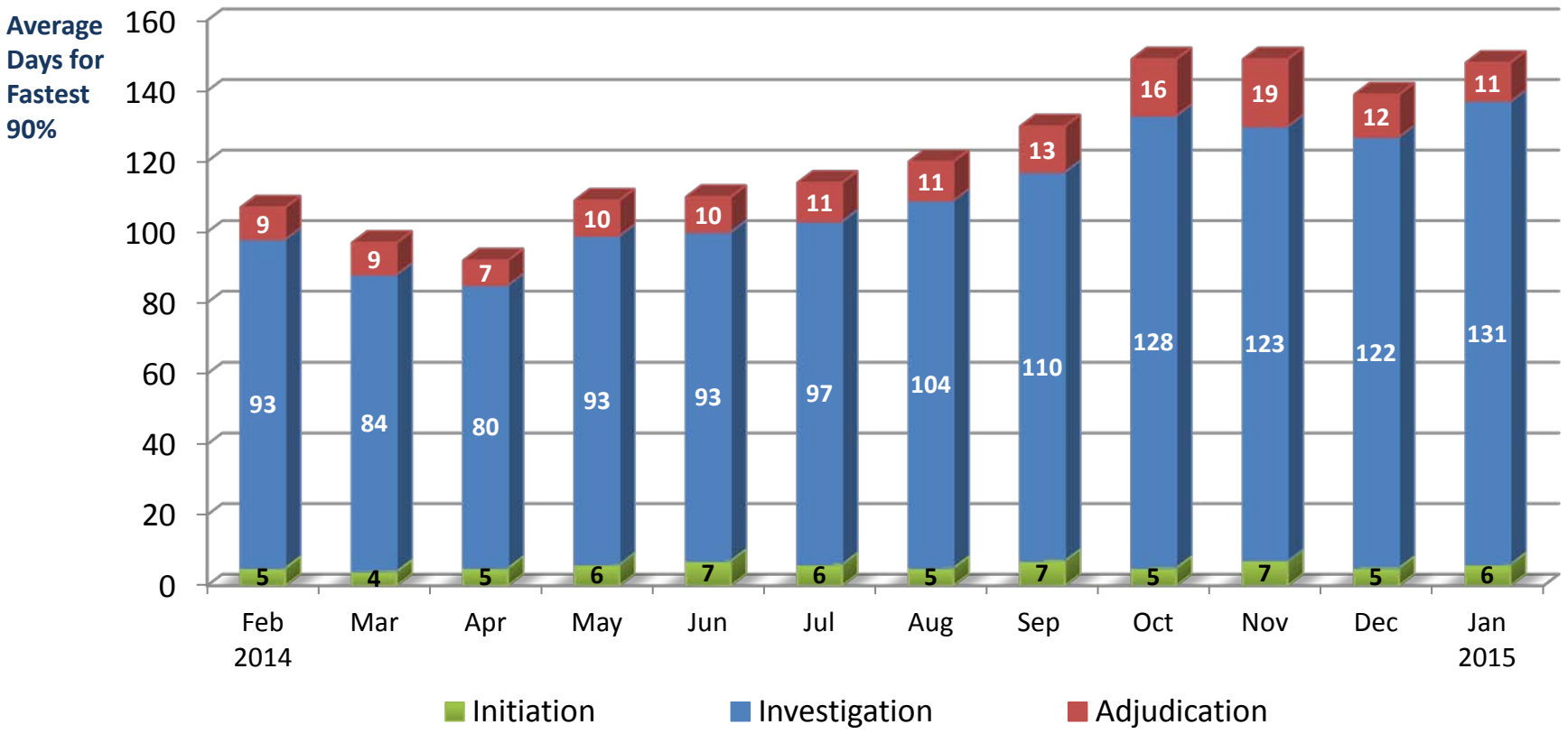
DOE's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



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

	Feb 2014	Mar 2014	Apr 2014	May 2014	Jun 2014	Jul 2014	Aug 2014	Sep 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015
100% of Reported Adjudications	280	263	289	241	251	353	166	184	238	305	326	263
Average Days for fastest 90%	47 days	46 days	43 days	47 days	51 days	52 days	53 days	59 days	72 days	83 days	68 days	79 days

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



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

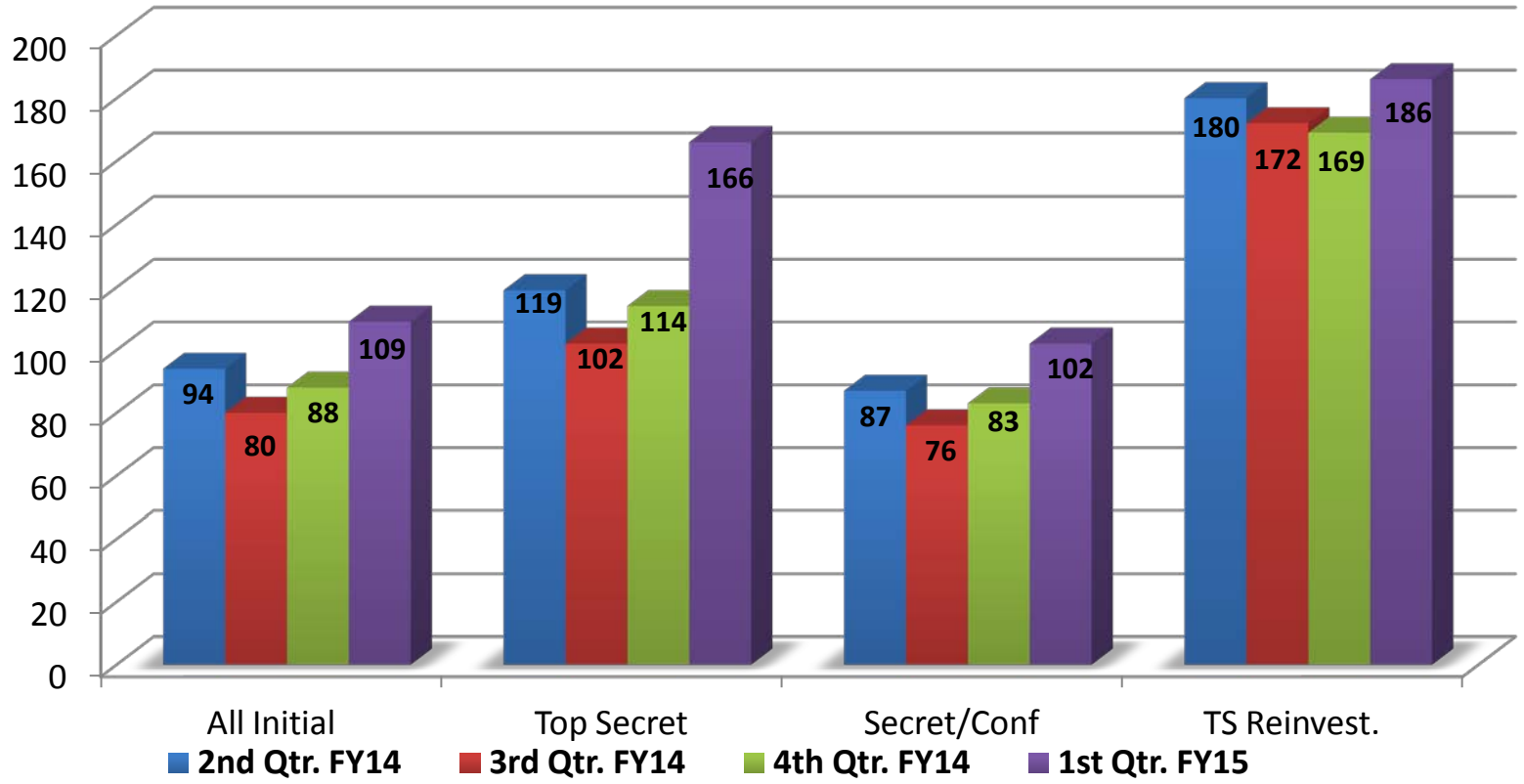
	Feb 2014	Mar 2014	Apr 2014	May 2014	Jun 2014	Jul 2014	Aug 2014	Sep 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015
100% of Reported Adjudications	970	861	860	876	854	834	842	553	510	382	440	475
Average Days for fastest 90%	107 days	97 days	92 days	109 days	110 days	114 days	120 days	130 days	149 days	149 days	139 days	148 days

a New Day for Federal Service

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

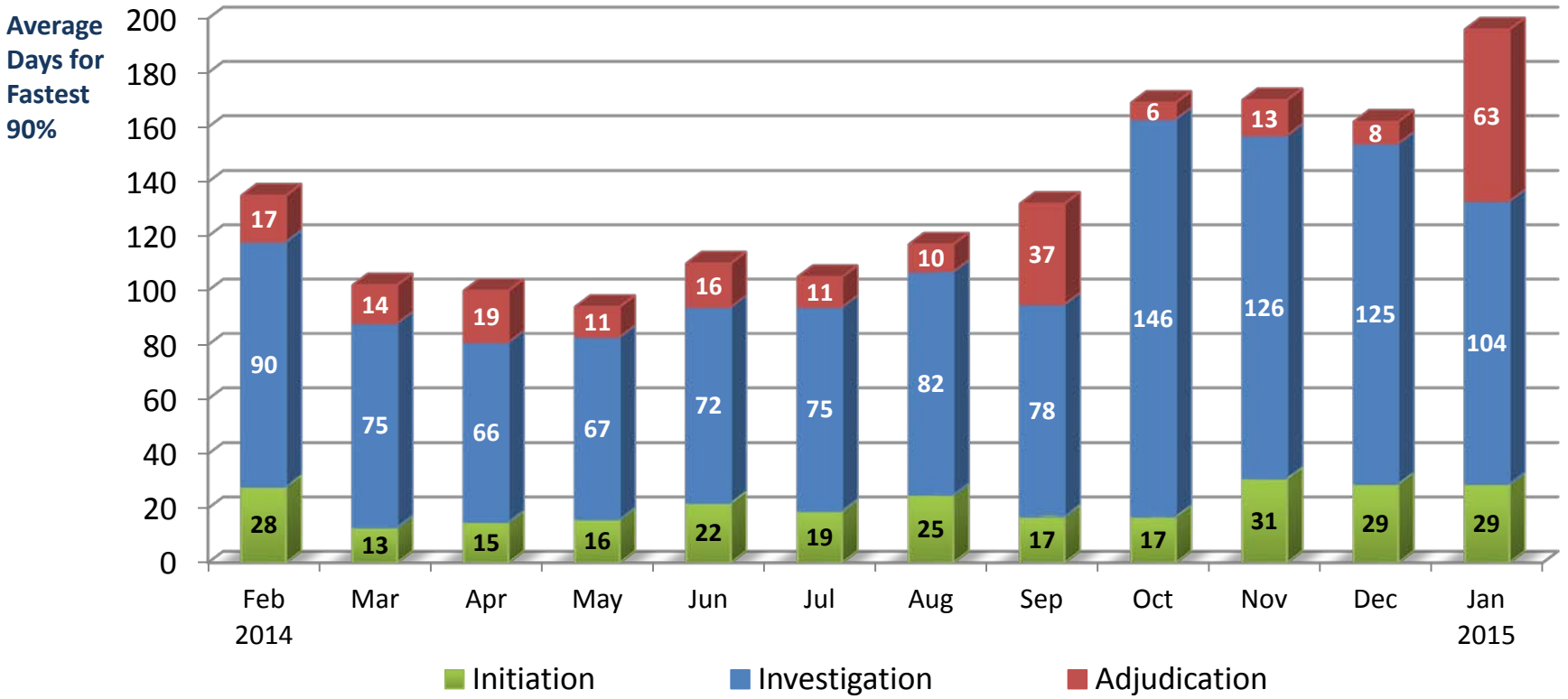
Timeliness Performance Metrics for NRC's Personnel Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 2nd Q FY14	208	53	155	52
Adjudication actions taken – 3rd Q FY14	219	36	183	61
Adjudication actions taken – 4th Q FY14	185	33	152	28
Adjudication actions taken – 1st Q FY15	138	16	122	18

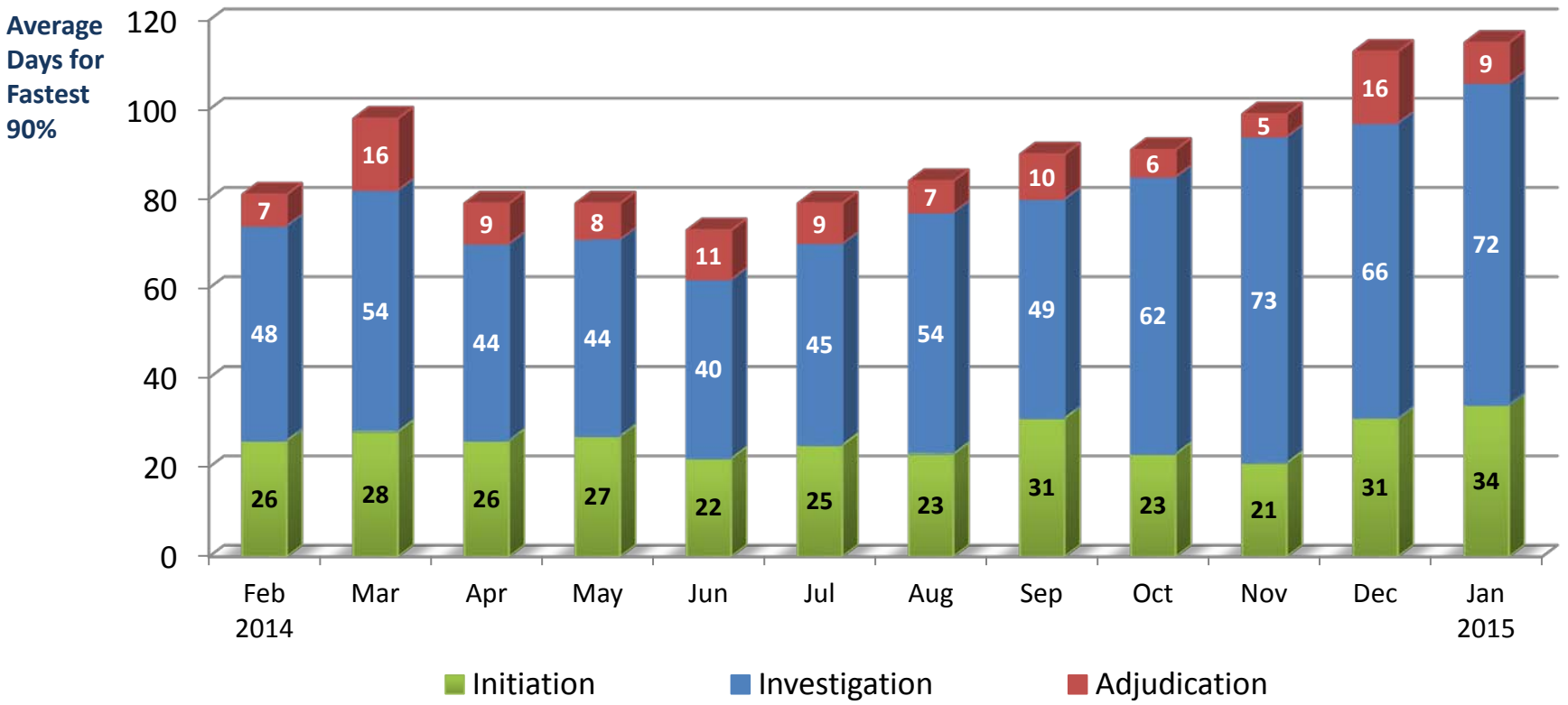
NRC's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



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

	Feb 2014	Mar 2014	Apr 2014	May 2014	Jun 2014	Jul 2014	Aug 2014	Sep 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015
100% of Reported Adjudications	11	16	16	9	10	12	16	5	6	4	6	2
Average Days for fastest 90%	135 days	102 days	100 days	94 days	110 days	105 days	117 days	132 days	169 days	170 days	162 days	196 days

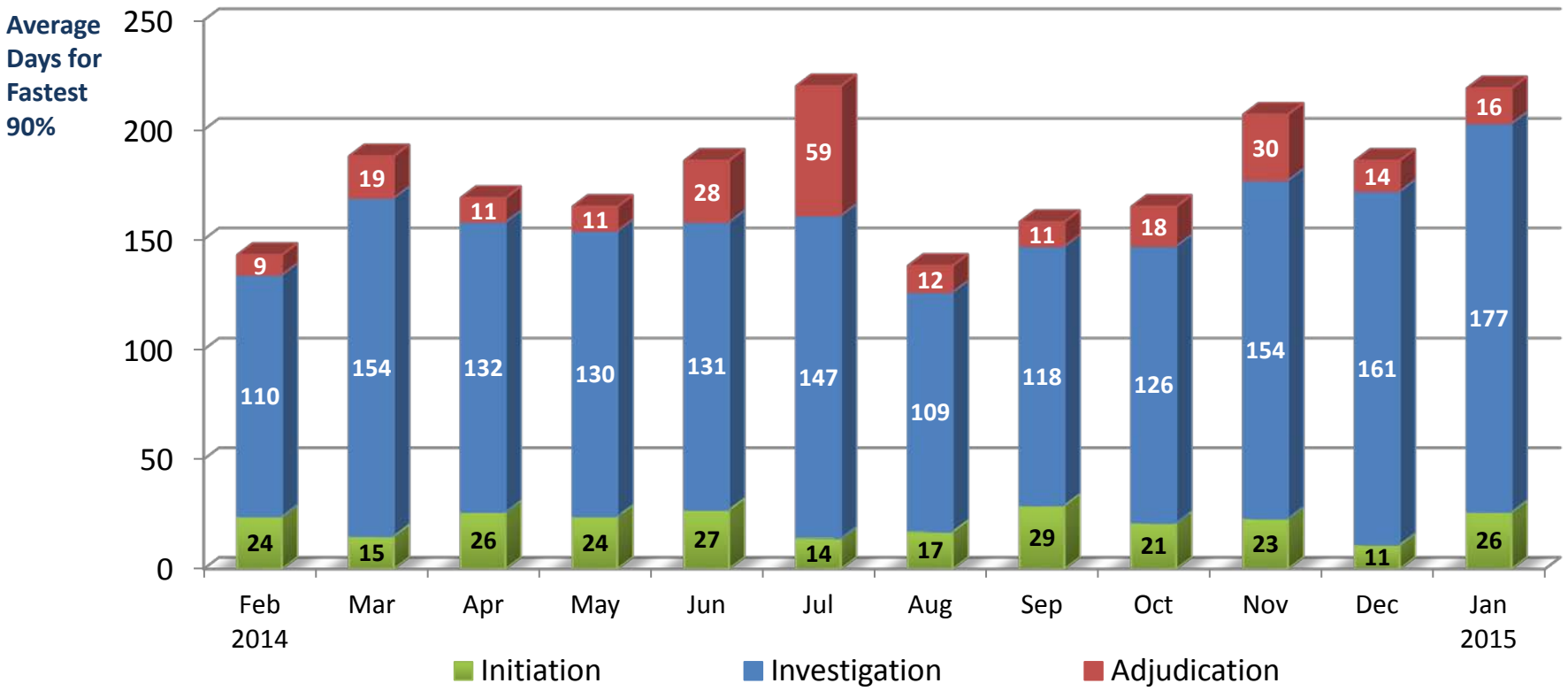
NRC's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



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

	Feb 2014	Mar 2014	Apr 2014	May 2014	Jun 2014	Jul 2014	Aug 2014	Sep 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015
100% of Reported Adjudications	55	60	52	54	75	77	41	34	30	40	52	29
Average Days for fastest 90%	81 days	98 days	79 days	79 days	73 days	79 days	84 days	90 days	91 days	99 days	113 days	115 days

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



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

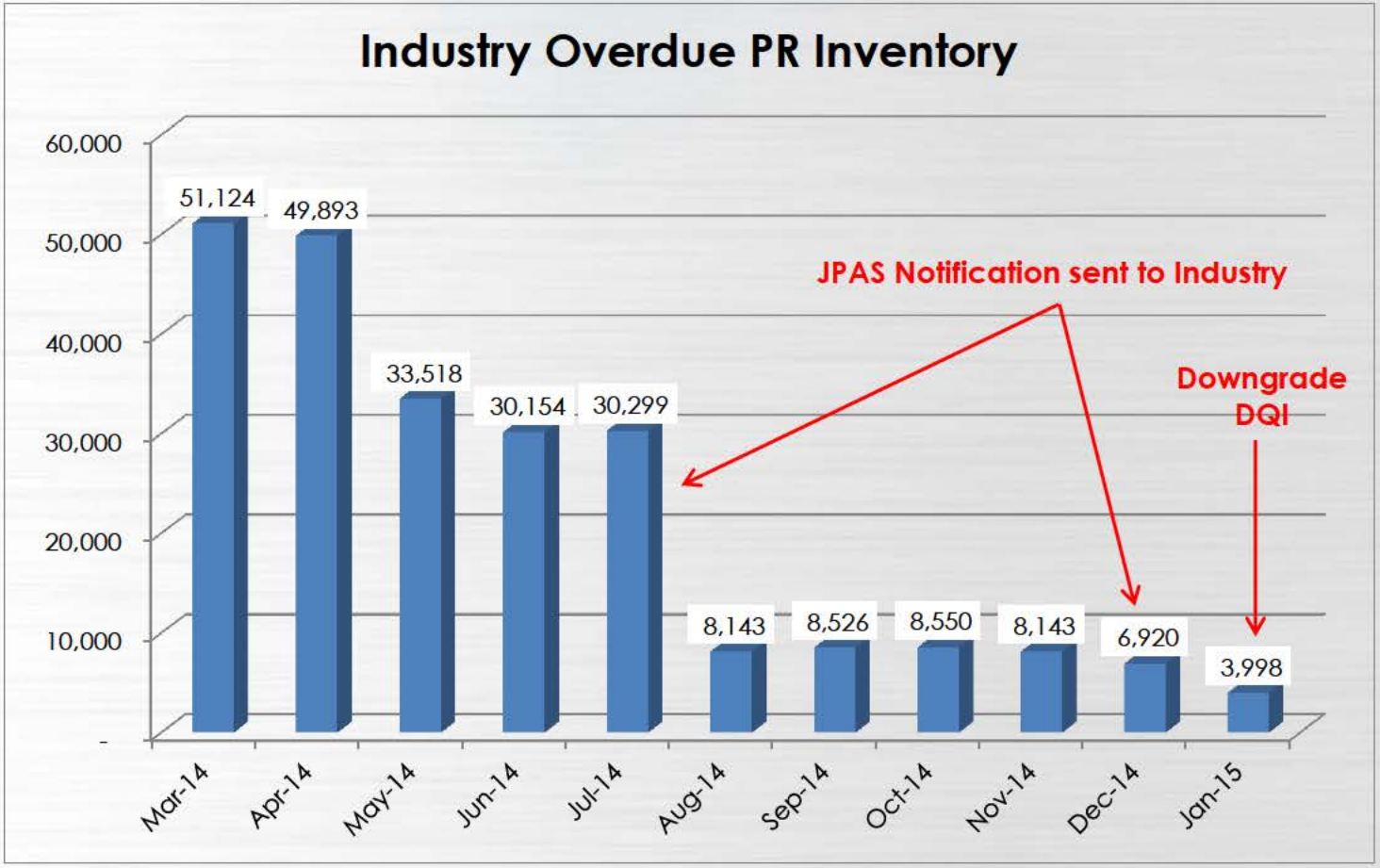
	Feb 2014	Mar 2014	Apr 2014	May 2014	Jun 2014	Jul 2014	Aug 2014	Sep 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015
100% of Reported Adjudications	26	9	24	18	18	14	9	5	6	5	7	8
Average Days for fastest 90%	143 days	188 days	169 days	165 days	186 days	204 days	138 days	158 days	165 days	207 days	186 days	219 days

Personnel Security Management Office for Industry (PSMO-I)

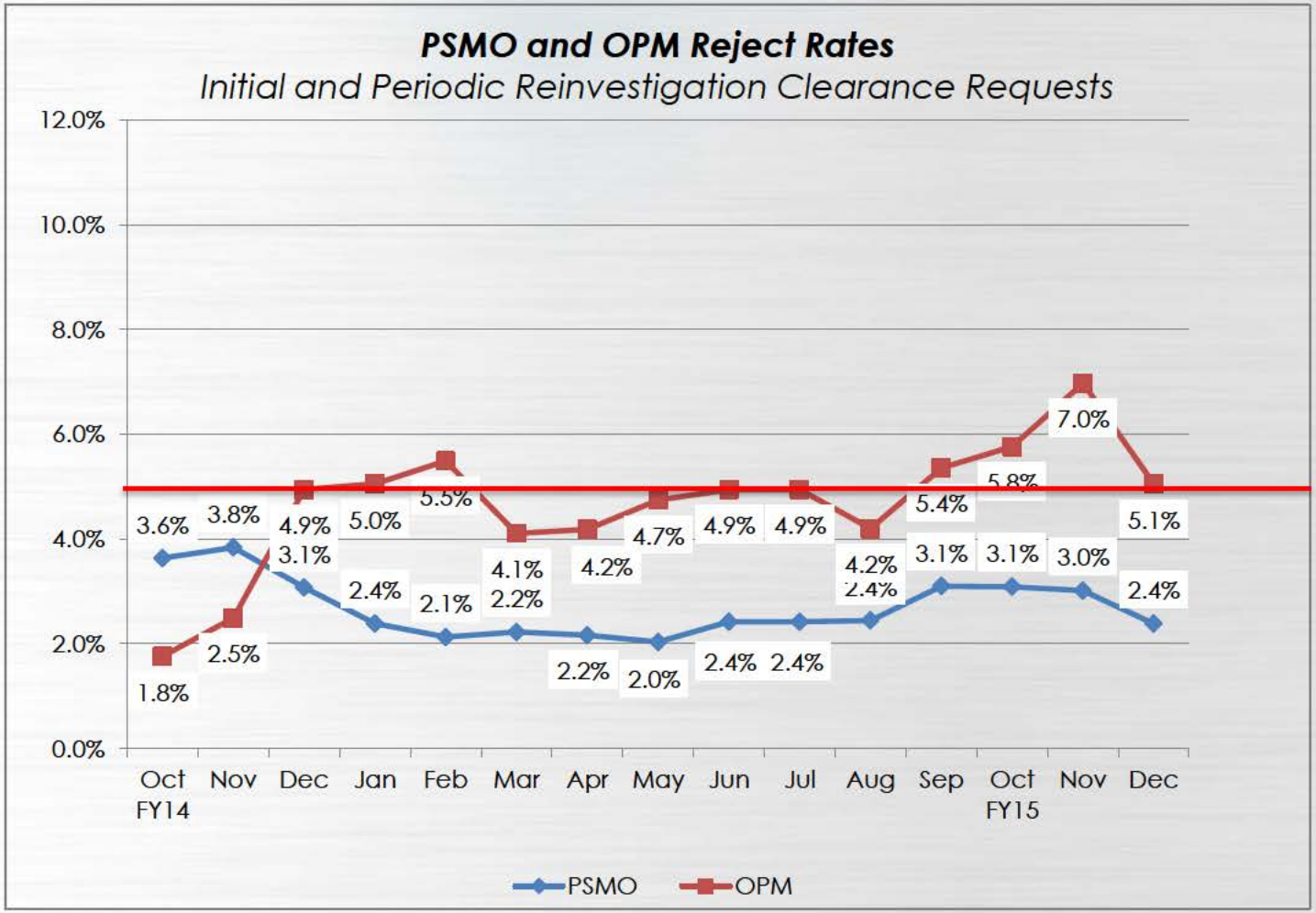
NISPPAC

March 2015

Overdue PRs

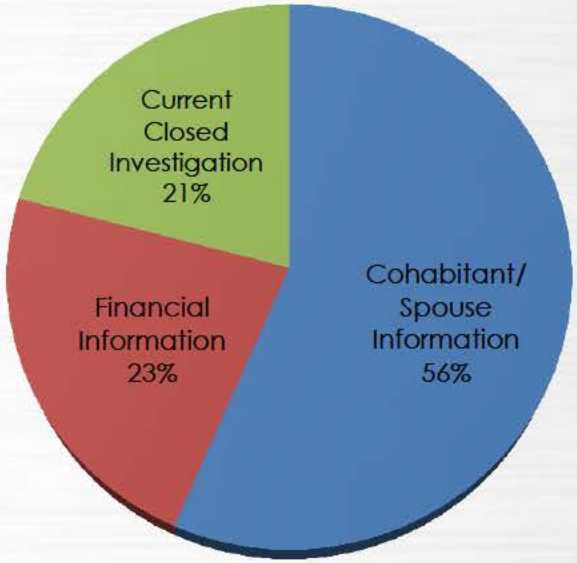

Industry Overdue PR Inventory
60,000
50,000
40,000
30,000
20,000
10,000
-
51,124
49,893
33,518
30,154
30,299
8,143
8,526
8,550
8,143
6,920
3,998
JPAS Notification sent to Industry
Downgrade DQI
Mar-14
Apr-14
May-14
Jun-14
Jul-14
Aug-14
Sep-14
Oct-14
Nov-14
Dec-14
Jan-15

e-QIP Reject Rates

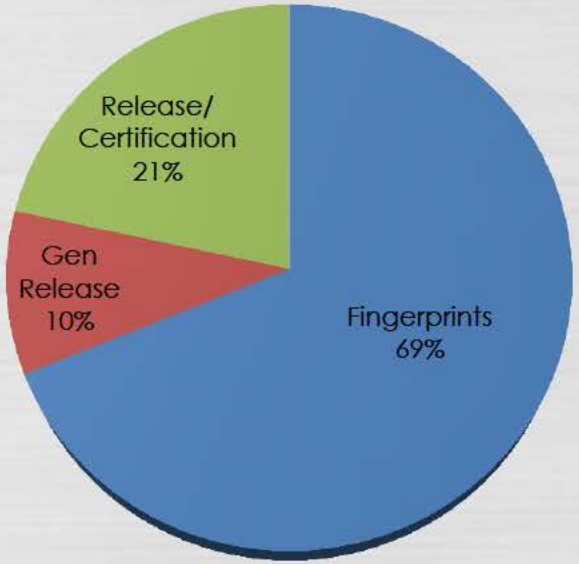


e-QIP Rejection Reasons

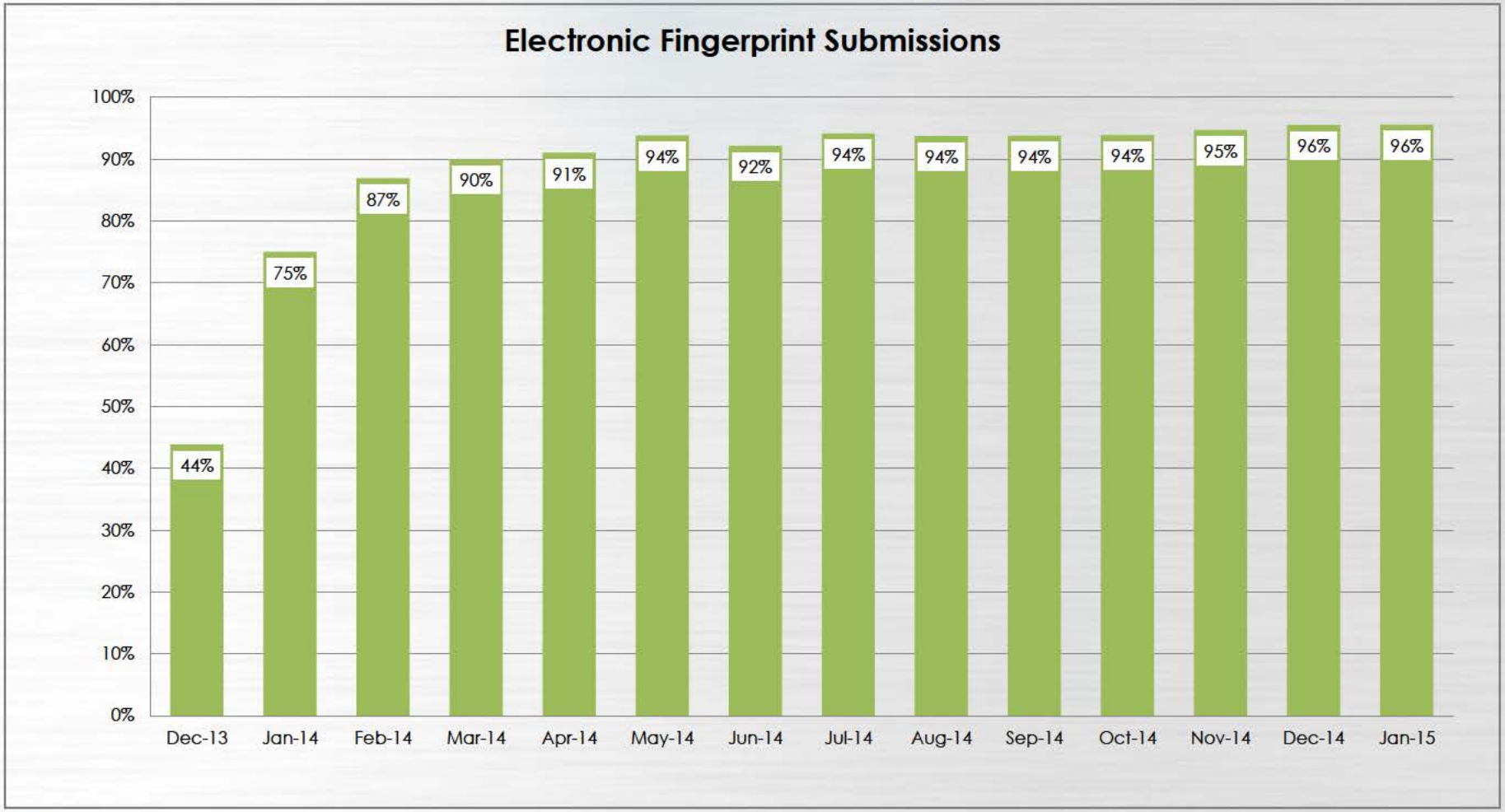
PSMO-I FY15
as of Dec 31 2014



OPM FY15
as of Dec 31 2014

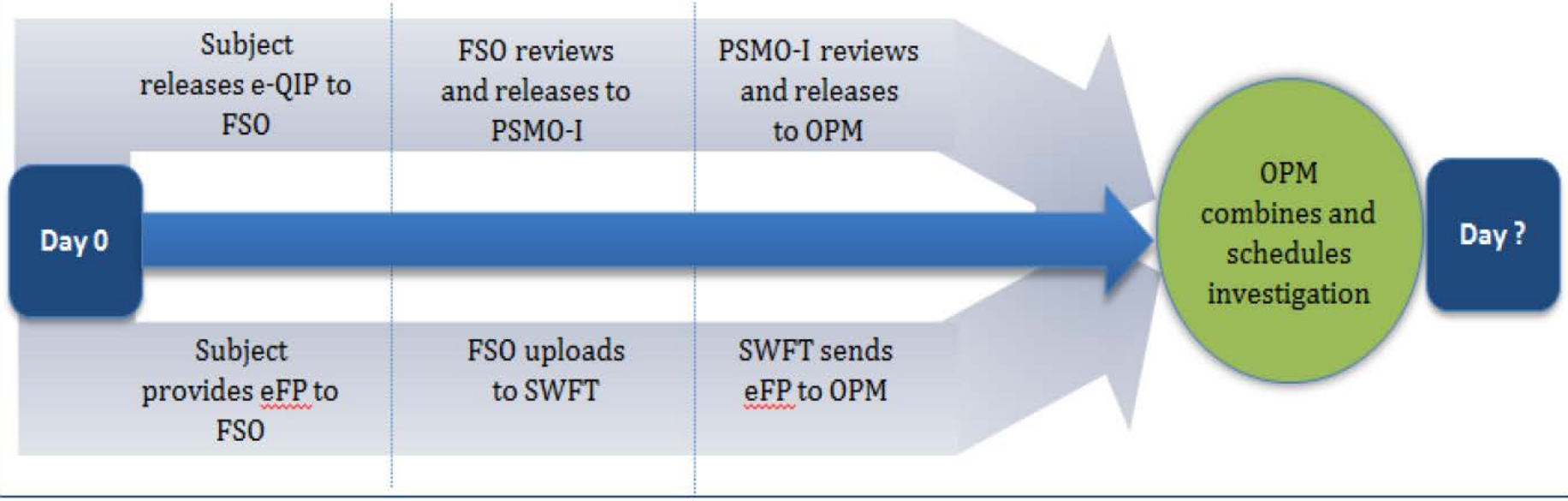


eFP Submissions



PSI-I Initiation = Shared Timeline

Initiation IRTPA Goal 90% <14 days

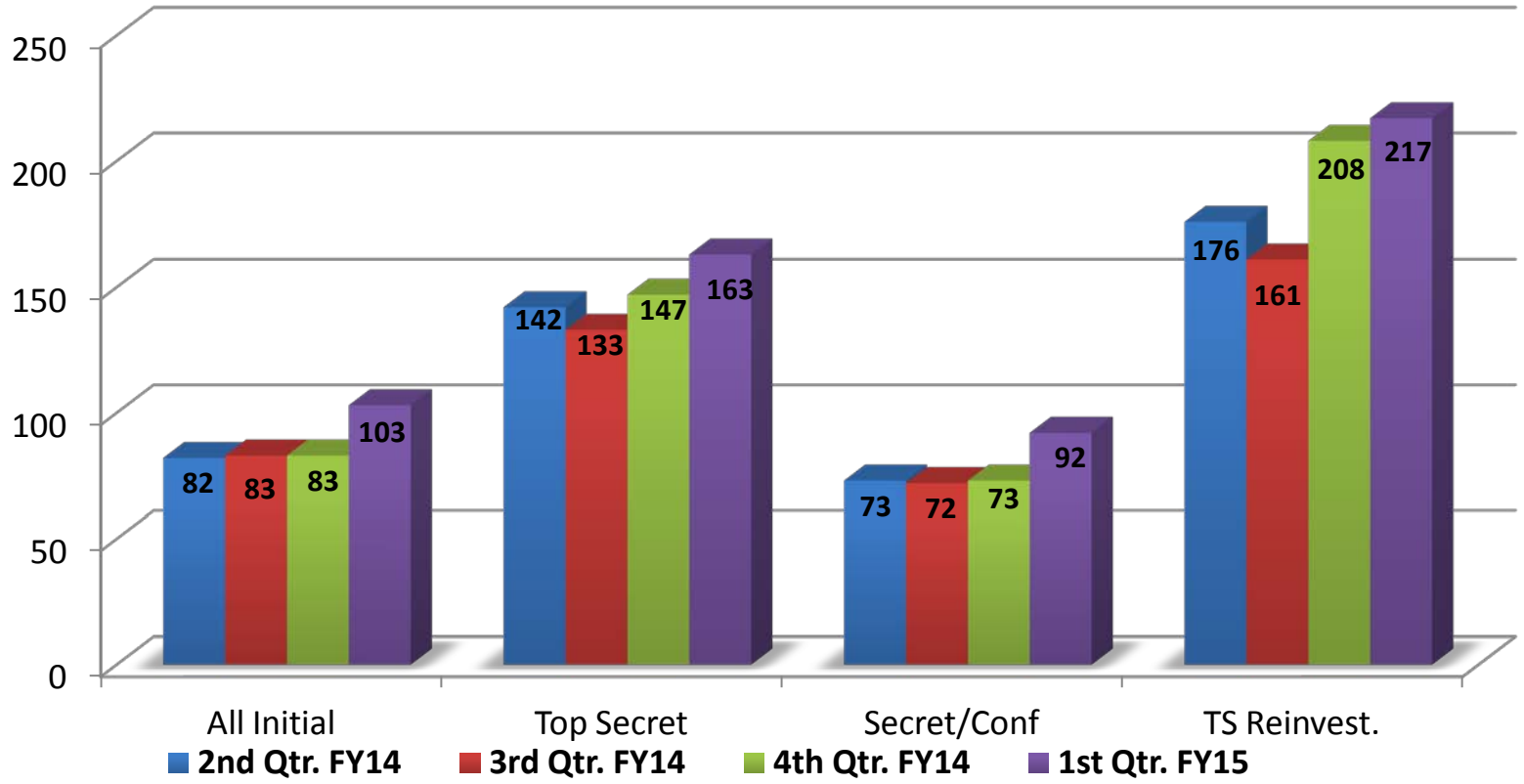


a New Day for Federal Service

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

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

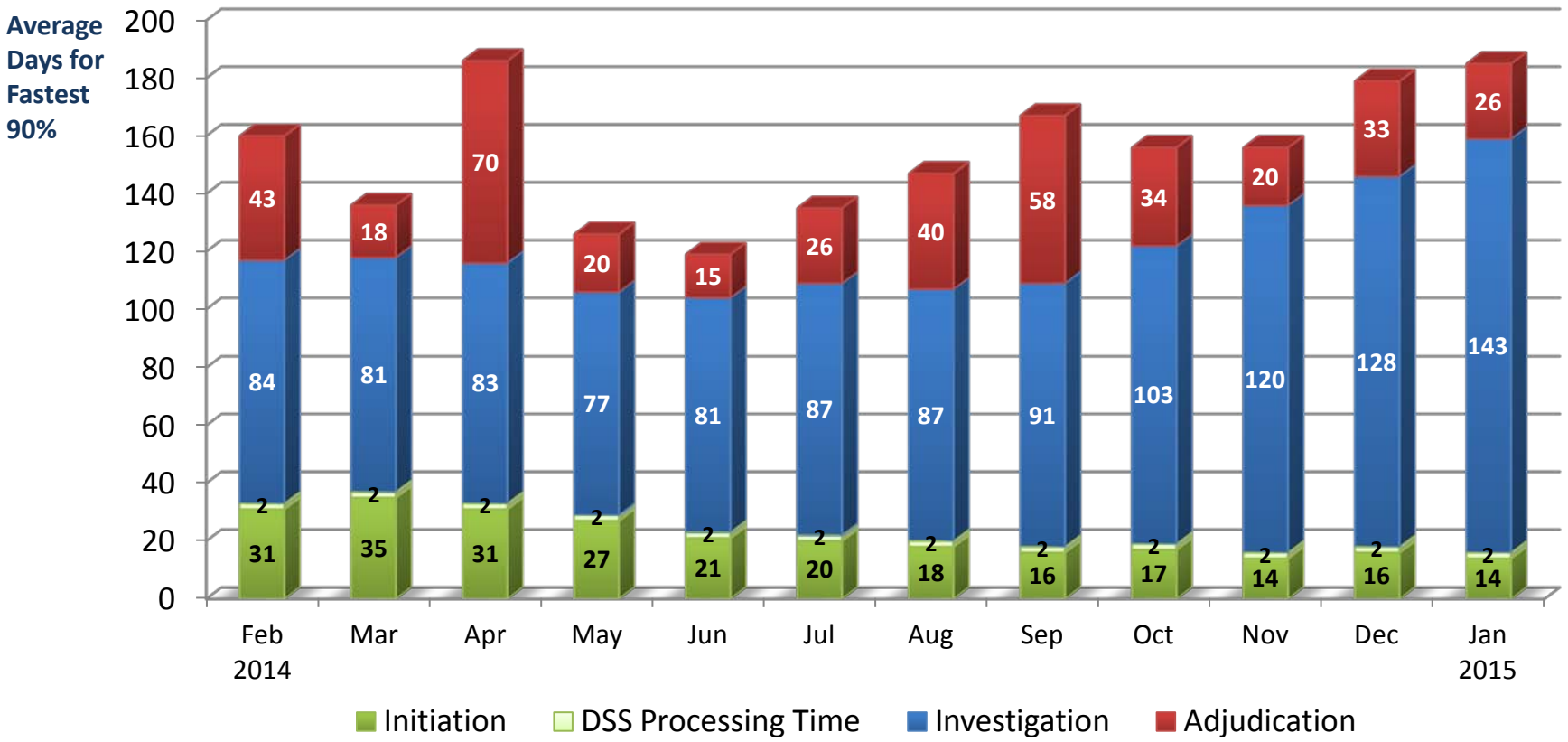
Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 2nd Q FY14	20,571	3,132	17,439	11,154
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

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

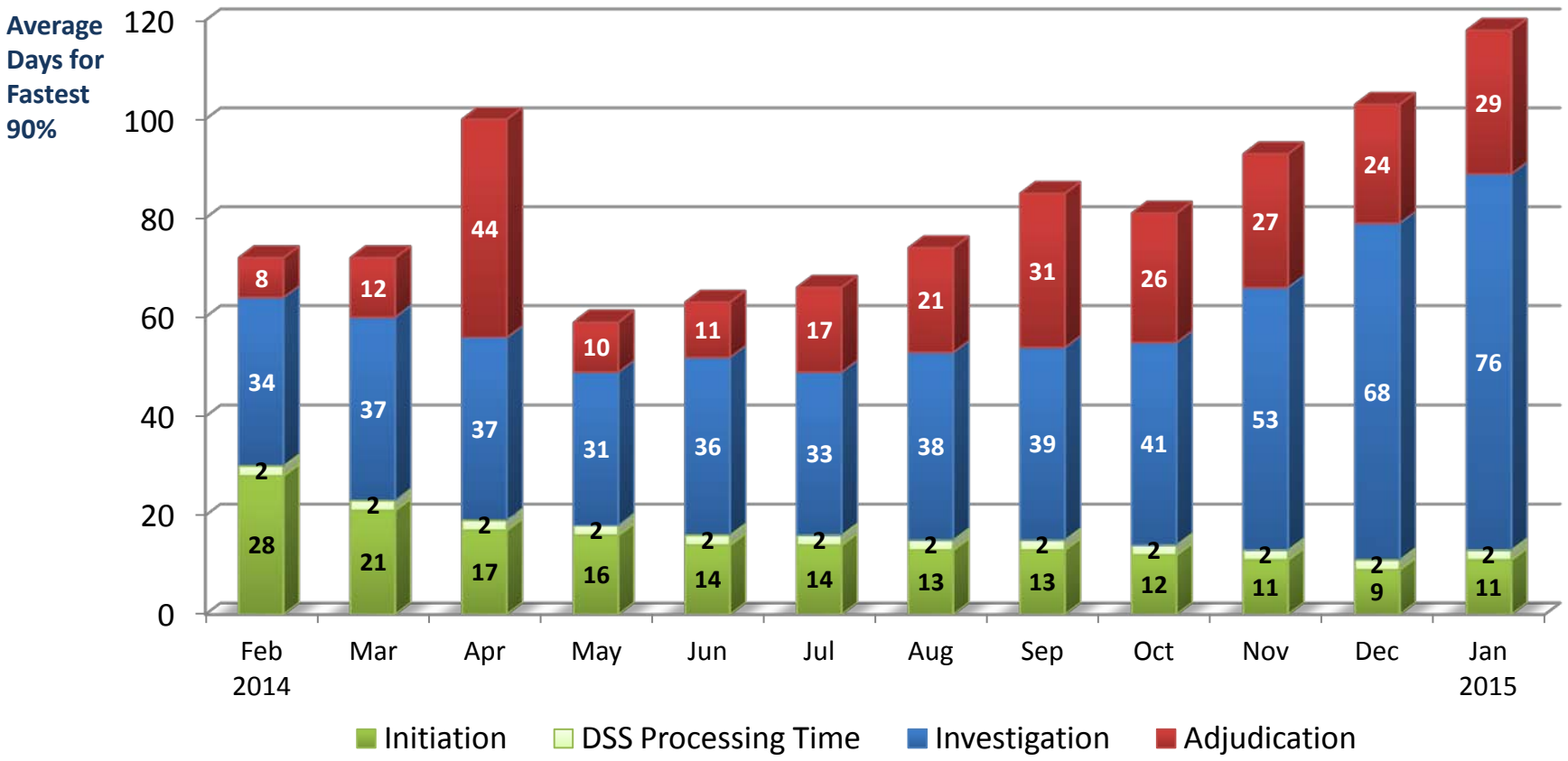
Industry's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



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

	Feb 2014	Mar 2014	Apr 2014	May 2014	Jun 2014	Jul 2014	Aug 2014	Sept 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015
100% of Reported Adjudications	777	1,603	961	1,581	1,481	1,103	932	800	1,206	933	983	1,045
Average Days for fastest 90%	160 days	136 days	186 days	126 days	119 days	135 days	147 days	167 days	156 days	156 days	179 days	185 days

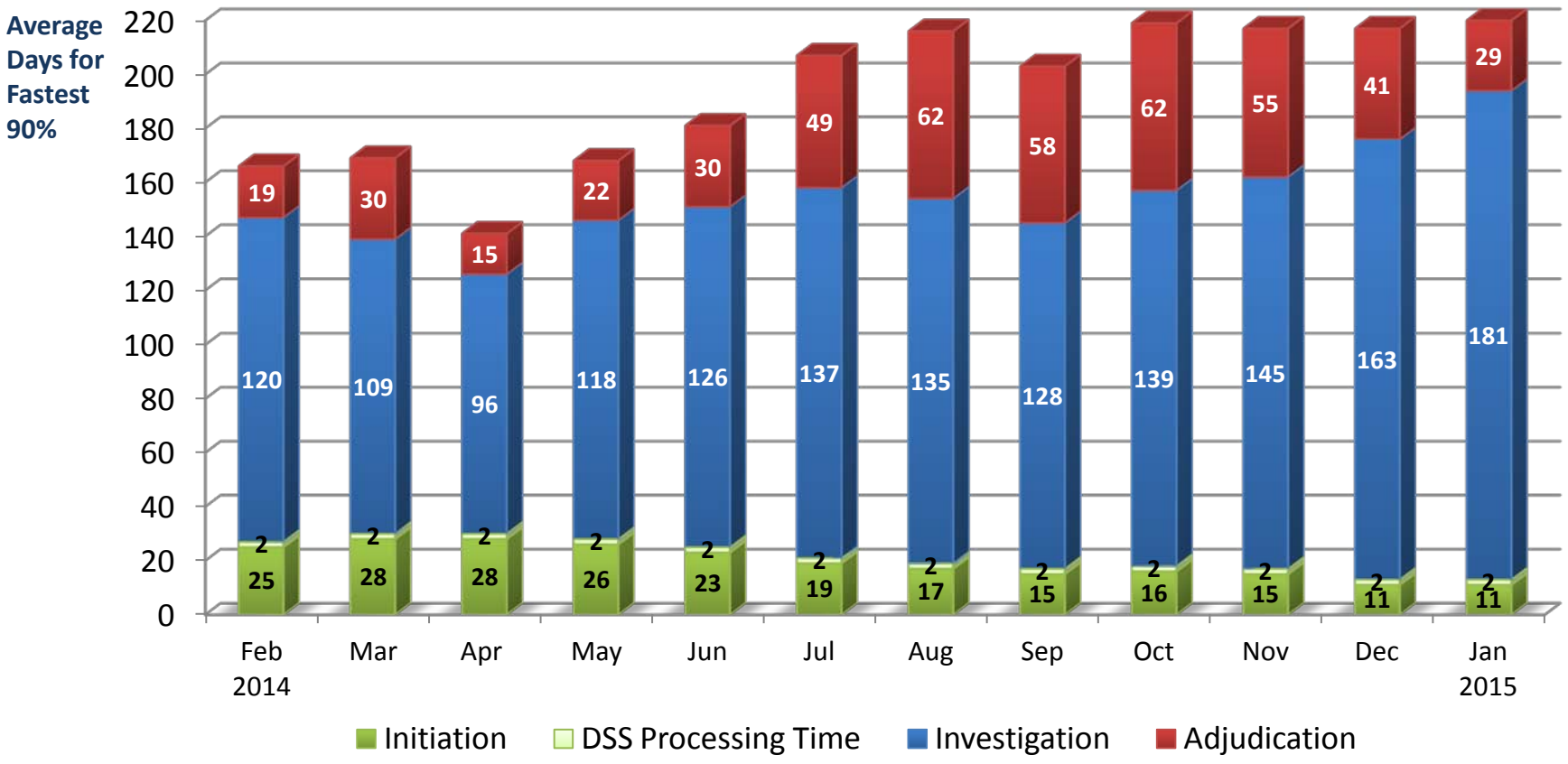
Industry's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



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

	Feb 2014	Mar 2014	Apr 2014	May 2014	Jun 2014	Jul 2014	Aug 2014	Sept 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015
100% of Reported Adjudications	6,644	5,485	6,996	5,187	5,463	5,993	5,621	4,510	5,293	4,978	5,579	5,358
Average Days for fastest 90%	72 days	72 days	100 days	59 days	63 days	66 days	74 days	85 days	81 days	93 days	103 days	118 days

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



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

	Feb 2014	Mar 2014	Apr 2014	May 2014	Jun 2014	Jul 2014	Aug 2014	Sept 2014	Oct 2014	Nov 2014	Dec 2014	Jan 2015
100% of Reported Adjudications	4,222	3,551	4,731	3,569	3,358	2,566	2,334	2,792	3,079	3,084	2,168	2,321
Average Days for fastest 90%	166 days	169 days	141 days	168 days	181 days	207 days	216 days	203 days	219 days	217 days	217 days	223 days