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 about 8% 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, 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, OUSD1 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. 13691 amendments 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
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
<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Igor Gardner</td>
<td>Department of Defense</td>
<td>Attendee</td>
</tr>
<tr>
<td>Priscilla Matos</td>
<td>Department of Defense</td>
<td>Attendee</td>
</tr>
<tr>
<td>Kenneth Campbell</td>
<td>Central intelligence Agency</td>
<td>Attendee</td>
</tr>
<tr>
<td>Charlie Rogers</td>
<td>Department of Homeland Security</td>
<td>Attendee</td>
</tr>
<tr>
<td>Lisa Loss</td>
<td>Office of Personnel Management</td>
<td>Attendee</td>
</tr>
<tr>
<td>Glen Clay</td>
<td>Department of Navy</td>
<td>Attendee</td>
</tr>
<tr>
<td>Mitch Lawrence</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Mark Ryan</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Mark Theby</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Jim Euton</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Richard Ray</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Michael Scheimer</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Dick Weaver</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Lloyd Gant</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Sarah Ballard</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Stacy Woodard</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Susan McCathern</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Rhonda Peyton</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Dennis Arriaga</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>John Dean</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Mary Albright</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Jim Martin</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Carla Whitehorn</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Ricky Velez</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Norman Pashoran</td>
<td>Industry</td>
<td>Attendee</td>
</tr>
<tr>
<td>Joe Marks</td>
<td>Reporter</td>
<td>Attendee</td>
</tr>
<tr>
<td>Alegra Woodard</td>
<td>Information Security Oversight Office</td>
<td>Attendee</td>
</tr>
<tr>
<td>David Best</td>
<td>Information Security Oversight Office</td>
<td>Staff</td>
</tr>
<tr>
<td>Robert Tringali</td>
<td>Information Security Oversight Office</td>
<td>Staff</td>
</tr>
<tr>
<td>Joseph Taylor</td>
<td>Information Security Oversight Office</td>
<td>Staff</td>
</tr>
<tr>
<td>Michael Manning</td>
<td>Information Security Oversight Office</td>
<td>Staff</td>
</tr>
</tbody>
</table>
NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

Industry
18 March 2015
Outline

- Current NISPPAC/MOU Membership
- Policy Changes
- Working Groups
<table>
<thead>
<tr>
<th>Members</th>
<th>Company</th>
<th>Term Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rick Graham</td>
<td>Huntington Ingalls Industries</td>
<td>2015</td>
</tr>
<tr>
<td>Steve Kipp</td>
<td>L3 Communications</td>
<td>2015</td>
</tr>
<tr>
<td>J.C. Dodson</td>
<td>BAE Systems</td>
<td>2016</td>
</tr>
<tr>
<td>Tony Ingenito</td>
<td>Northrop Grumman Corp.</td>
<td>2016</td>
</tr>
<tr>
<td>Bill Davidson</td>
<td>KeyPoint Government Solutions</td>
<td>2017</td>
</tr>
<tr>
<td>Phil Robinson</td>
<td>CGI Federal</td>
<td>2017</td>
</tr>
<tr>
<td>Michelle Sutphin</td>
<td>American Systems Corp.</td>
<td>2018</td>
</tr>
<tr>
<td>Martin Strones</td>
<td>Strones Enterprises</td>
<td>2018</td>
</tr>
</tbody>
</table>
# National Industrial Security Program

## Industry MOU Members

<table>
<thead>
<tr>
<th>Organization</th>
<th>Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIA *</td>
<td>Keith Waddell</td>
</tr>
<tr>
<td>ASIS *</td>
<td>Dan McGarvey</td>
</tr>
<tr>
<td>CSSWG</td>
<td>Mark Rush</td>
</tr>
<tr>
<td>ISWG</td>
<td>Karen Duprey</td>
</tr>
<tr>
<td>NCMS</td>
<td>Leonard Moss</td>
</tr>
<tr>
<td>NDIA</td>
<td>Mike Witt</td>
</tr>
<tr>
<td>Tech America</td>
<td>Kirk Poulson</td>
</tr>
</tbody>
</table>

* 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.
INSIDER THREAT

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


- 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.
    • 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
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”.
- 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

<table>
<thead>
<tr>
<th>Month</th>
<th>NISP Backlog</th>
<th>Annual NISP Receipt</th>
<th>Backlog % of Total NISP</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 13</td>
<td>13,515</td>
<td></td>
<td>8.1%</td>
</tr>
<tr>
<td>February 15</td>
<td>3,462</td>
<td>-10,053</td>
<td>1.9%</td>
</tr>
</tbody>
</table>
- Both NISP and non-NISP timeliness metrics increased as backlogs addressed
- Timeliness to fluctuate throughout FY15 until industry backlog is fully eliminated
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

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

Graph showing approval timeliness from February 2014 to January 2015 for IATO, Reg ATO, and SATO.
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
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

<table>
<thead>
<tr>
<th>Deficiencies</th>
<th>Feb-14</th>
<th>Mar-14</th>
<th>Apr-14</th>
<th>May-14</th>
<th>Jun-14</th>
<th>Jul-14</th>
<th>Aug-14</th>
<th>Sep-14</th>
<th>Oct-14</th>
<th>Nov-14</th>
<th>Dec-14</th>
<th>Jan-15</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td># Deficiencies</td>
<td>146</td>
<td>178</td>
<td>179</td>
<td>258</td>
<td>154</td>
<td>102</td>
<td>69</td>
<td>86</td>
<td>137</td>
<td>128</td>
<td>101</td>
<td>162</td>
<td>1026</td>
</tr>
<tr>
<td># Plans w/ Deficiencies</td>
<td>89</td>
<td>92</td>
<td>90</td>
<td>140</td>
<td>87</td>
<td>64</td>
<td>56</td>
<td>73</td>
<td>95</td>
<td>109</td>
<td>64</td>
<td>81</td>
<td>567</td>
</tr>
<tr>
<td># Plans Reviewed</td>
<td>357</td>
<td>396</td>
<td>363</td>
<td>431</td>
<td>275</td>
<td>228</td>
<td>247</td>
<td>317</td>
<td>357</td>
<td>322</td>
<td>279</td>
<td>286</td>
<td>2547</td>
</tr>
<tr>
<td>Avg Deficiency per Plan</td>
<td>0.41</td>
<td>0.45</td>
<td>0.49</td>
<td>0.60</td>
<td>0.56</td>
<td>0.45</td>
<td>0.28</td>
<td>0.27</td>
<td>0.38</td>
<td>0.40</td>
<td>0.36</td>
<td>0.57</td>
<td>0.43</td>
</tr>
<tr>
<td>Denials</td>
<td>22</td>
<td>31</td>
<td>28</td>
<td>30</td>
<td>26</td>
<td>14</td>
<td>10</td>
<td>10</td>
<td>18</td>
<td>12</td>
<td>17</td>
<td>14</td>
<td>145</td>
</tr>
<tr>
<td>Rejections</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>10</td>
<td>9</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>4</td>
<td>22</td>
</tr>
</tbody>
</table>

**Top 10 Deficiencies**

1. SSP Is incomplete or missing attachments
2. SSP Not Tailored to the System
3. Inaccurate or Incomplete Configuration diagram/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
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.

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

Session Controls: Failed to have proper user activity/inactivity, 15%

Configuration Management: Improper protection implemented and maintained, 11%

SSP Does Not Reflect How System is Configured, 5%

Bios not Protected, 4%

Topology not Correctly Reflected in (M)SSP, 4%

Inadequate Anti-virus Procedures, 3%

Identification & Authentication, 3%

Security Relevant Objects not Protected, 23%

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

Top 10 Vulnerabilities

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.
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
- Designates 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
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

<table>
<thead>
<tr>
<th></th>
<th>All Initial</th>
<th>Top Secret</th>
<th>Secret/Confidential</th>
<th>TS Reinvest.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2nd Qtr. FY14</td>
<td>67</td>
<td>90</td>
<td>94</td>
<td>67</td>
</tr>
<tr>
<td>3rd Qtr. FY14</td>
<td>63</td>
<td>84</td>
<td>99</td>
<td>126</td>
</tr>
<tr>
<td>4th Qtr. FY14</td>
<td>73</td>
<td>48</td>
<td>56</td>
<td>107</td>
</tr>
<tr>
<td>1st Qtr. FY15</td>
<td>94</td>
<td>47</td>
<td>74</td>
<td>104</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>All Initial</th>
<th>Top Secret</th>
<th>Secret/Confidential</th>
<th>Top Secret Reinvestigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjudication actions taken – 2nd Q FY14</td>
<td>1,547</td>
<td>724</td>
<td>823</td>
<td>2,578</td>
</tr>
<tr>
<td>Adjudication actions taken – 3rd Q FY14</td>
<td>1,515</td>
<td>695</td>
<td>820</td>
<td>2,619</td>
</tr>
<tr>
<td>Adjudication actions taken – 4th Q FY14</td>
<td>1,311</td>
<td>455</td>
<td>752</td>
<td>2,250</td>
</tr>
<tr>
<td>Adjudication actions taken – 1st Q FY15</td>
<td>1,431</td>
<td>552</td>
<td>879</td>
<td>1,338</td>
</tr>
</tbody>
</table>
DOE’s Average Timeliness Trends for 90%
Initial Top Secret Security Clearance Decisions

Average Days for Fastest 90%

---|---|---|---|---|---|---|---|---|---|---|---
Initiation | 15 | 14 | 13 | 14 | 14 | 18 | 23 | 21 | 20 | 14 | 17
Investigation | 72 | 67 | 58 | 63 | 68 | 72 | 73 | 76 | 90 | 99 | 125
Adjudication | 8 | 7 | 7 | 7 | 7 | 8 | 7 | 9 | 10 | 6 | 7

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

100% of Reported Adjudications

---|---|---|---|---|---|---|---|---|---|---|---
100% of Reported Adjudications | 221 | 239 | 219 | 261 | 204 | 219 | 204 | 118 | 171 | 191 | 184 | 152

Average Days for fastest 90%

---|---|---|---|---|---|---|---|---|---|---|---
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

Average Days for Fastest 90%

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>10</td>
<td>13</td>
<td>9</td>
<td>10</td>
<td>12</td>
<td>11</td>
<td>11</td>
<td>15</td>
<td>18</td>
<td>21</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>Investigation</td>
<td>24</td>
<td>27</td>
<td>25</td>
<td>26</td>
<td>29</td>
<td>31</td>
<td>32</td>
<td>33</td>
<td>44</td>
<td>50</td>
<td>48</td>
<td>59</td>
</tr>
<tr>
<td>Adjudication</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>11</td>
<td>10</td>
<td>10</td>
<td>11</td>
<td>10</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>10</td>
</tr>
</tbody>
</table>

100% of Reported Adjudications:
- Feb 2014: 280 days
- Mar 2014: 263 days
- Apr 2014: 289 days
- May 2014: 241 days
- Jun 2014: 251 days
- Jul 2014: 353 days
- Aug 2014: 166 days
- Sep 2014: 184 days
- Oct 2014: 238 days
- Nov 2014: 305 days
- Dec 2014: 326 days
- Jan 2015: 263 days

Average Days for fastest 90%:
- Feb 2014: 47 days
- Mar 2014: 46 days
- Apr 2014: 43 days
- May 2014: 47 days
- Jun 2014: 51 days
- Jul 2014: 52 days
- Aug 2014: 53 days
- Sep 2014: 59 days
- Oct 2014: 72 days
- Nov 2014: 83 days
- Dec 2014: 68 days
- Jan 2015: 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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>100% of Reported Adjudications</td>
<td>970</td>
<td>861</td>
<td>860</td>
<td>876</td>
<td>854</td>
<td>834</td>
<td>842</td>
<td>553</td>
<td>510</td>
<td>382</td>
<td>440</td>
<td>475</td>
</tr>
<tr>
<td>Average Days for fastest 90%</td>
<td>107 days</td>
<td>97 days</td>
<td>92 days</td>
<td>109 days</td>
<td>110 days</td>
<td>114 days</td>
<td>120 days</td>
<td>130 days</td>
<td>149 days</td>
<td>149 days</td>
<td>139 days</td>
<td>148 days</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th></th>
<th>All Initial</th>
<th>Top Secret</th>
<th>Secret/Conf</th>
<th>TS Reinvest.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2nd Qtr. FY14</td>
<td>3rd Qtr. FY14</td>
<td>4th Qtr. FY14</td>
<td>1st Qtr. FY15</td>
</tr>
<tr>
<td>Adjudication actions taken – 2nd Q FY14</td>
<td>208</td>
<td>53</td>
<td>155</td>
<td>52</td>
</tr>
<tr>
<td>Adjudication actions taken – 3rd Q FY14</td>
<td>219</td>
<td>36</td>
<td>183</td>
<td>61</td>
</tr>
<tr>
<td>Adjudication actions taken – 4th Q FY14</td>
<td>185</td>
<td>33</td>
<td>152</td>
<td>28</td>
</tr>
<tr>
<td>Adjudication actions taken – 1st Q FY15</td>
<td>138</td>
<td>16</td>
<td>122</td>
<td>18</td>
</tr>
</tbody>
</table>
NRC’s Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions

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

### Timeliness Trends by Month

<table>
<thead>
<tr>
<th>Month</th>
<th>Initiation</th>
<th>Investigation</th>
<th>Adjudication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 2014</td>
<td>17 days</td>
<td>90 days</td>
<td>28 days</td>
</tr>
<tr>
<td>Mar 2014</td>
<td>14 days</td>
<td>75 days</td>
<td>13 days</td>
</tr>
<tr>
<td>Apr 2014</td>
<td>19 days</td>
<td>66 days</td>
<td>15 days</td>
</tr>
<tr>
<td>May 2014</td>
<td>11 days</td>
<td>67 days</td>
<td>16 days</td>
</tr>
<tr>
<td>Jun 2014</td>
<td>16 days</td>
<td>72 days</td>
<td>22 days</td>
</tr>
<tr>
<td>Jul 2014</td>
<td>11 days</td>
<td>75 days</td>
<td>19 days</td>
</tr>
<tr>
<td>Aug 2014</td>
<td>10 days</td>
<td>82 days</td>
<td>25 days</td>
</tr>
<tr>
<td>Sep 2014</td>
<td>37 days</td>
<td>78 days</td>
<td>17 days</td>
</tr>
<tr>
<td>Oct 2014</td>
<td>146 days</td>
<td>126 days</td>
<td>31 days</td>
</tr>
<tr>
<td>Nov 2014</td>
<td>125 days</td>
<td>125 days</td>
<td>29 days</td>
</tr>
<tr>
<td>Dec 2014</td>
<td>104 days</td>
<td>104 days</td>
<td>29 days</td>
</tr>
<tr>
<td>Jan 2015</td>
<td>63 days</td>
<td>63 days</td>
<td>29 days</td>
</tr>
</tbody>
</table>

### Average Days for Fastest 90%

- **Initiation:**
  - Feb 2014: 17 days
  - Mar 2014: 14 days
  - Apr 2014: 19 days
  - May 2014: 11 days
  - Jun 2014: 16 days
  - Jul 2014: 11 days
  - Aug 2014: 10 days
  - Sep 2014: 37 days
  - Oct 2014: 146 days
  - Nov 2014: 125 days
  - Dec 2014: 104 days
  - Jan 2015: 63 days

- **Investigation:**
  - Feb 2014: 90 days
  - Mar 2014: 75 days
  - Apr 2014: 66 days
  - May 2014: 67 days
  - Jun 2014: 72 days
  - Jul 2014: 75 days
  - Aug 2014: 82 days
  - Sep 2014: 78 days
  - Oct 2014: 146 days
  - Nov 2014: 126 days
  - Dec 2014: 125 days
  - Jan 2015: 104 days

- **Adjudication:**
  - Feb 2014: 28 days
  - Mar 2014: 13 days
  - Apr 2014: 16 days
  - May 2014: 22 days
  - Jun 2014: 19 days
  - Jul 2014: 25 days
  - Aug 2014: 17 days
  - Sep 2014: 17 days
  - Oct 2014: 31 days
  - Nov 2014: 29 days
  - Dec 2014: 29 days
  - Jan 2015: 29 days

### Key Metrics

- **100% of Reported Adjudications:**
  - Feb 2014: 11
  - Mar 2014: 16
  - Apr 2014: 16
  - May 2014: 9
  - Jun 2014: 10
  - Jul 2014: 12
  - Aug 2014: 16
  - Sep 2014: 5
  - Oct 2014: 6
  - Nov 2014: 4
  - Dec 2014: 6
  - Jan 2015: 2

- **Average Days for fastest 90%:**
  - Feb 2014: 135 days
  - Mar 2014: 102 days
  - Apr 2014: 100 days
  - May 2014: 94 days
  - Jun 2014: 110 days
  - Jul 2014: 105 days
  - Aug 2014: 117 days
  - Sep 2014: 132 days
  - Oct 2014: 169 days
  - Nov 2014: 170 days
  - Dec 2014: 162 days
  - Jan 2015: 196 days
NRC’s Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions

**Goal:**
- **Initiation:** 14 days
- **Investigation:** 40 days
- **Adjudication:** 20 days

### Chart Description:
- The chart illustrates the average timeliness trends for 90% of reported adjudications from February 2014 to January 2015.
- Each column represents a month, with bars indicating the average days for three stages: Initiation, Investigation, and Adjudication.
- The bars are color-coded: green for Initiation, blue for Investigation, and red for Adjudication.

### Data Table:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>100% of Reported Adjudications</strong></td>
<td>55</td>
<td>60</td>
<td>52</td>
<td>54</td>
<td>75</td>
<td>77</td>
<td>41</td>
<td>34</td>
<td>30</td>
<td>40</td>
<td>52</td>
<td>29</td>
</tr>
<tr>
<td><strong>Average Days for fastest 90%</strong></td>
<td>81 days</td>
<td>98 days</td>
<td>79 days</td>
<td>79 days</td>
<td>73 days</td>
<td>79 days</td>
<td>84 days</td>
<td>90 days</td>
<td>91 days</td>
<td>99 days</td>
<td>113 days</td>
<td>115 days</td>
</tr>
</tbody>
</table>
NRC’s Average Timeliness Trends for 90%
Top Secret Reinvestigation Security Clearance Decisions

Average Days for Fastest 90%

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>100% of Reported Adjudications</td>
<td>26</td>
<td>9</td>
<td>24</td>
<td>18</td>
<td>18</td>
<td>14</td>
<td>9</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>Average Days for fastest 90%</td>
<td>143 days</td>
<td>188 days</td>
<td>169 days</td>
<td>165 days</td>
<td>186 days</td>
<td>204 days</td>
<td>138 days</td>
<td>158 days</td>
<td>165 days</td>
<td>207 days</td>
<td>186 days</td>
<td>219 days</td>
</tr>
</tbody>
</table>
Personnel Security Management
Office for Industry
(PSMO-I)

NISPPAC

March 2015
Overdue PRs

Industry Overdue PR Inventory

JPAS Notification sent to Industry
Downgrade DQI

Defense Security Service
e-QIP Rejection Reasons

PSMO-I FY15
as of Dec 31 2014

- Current Closed Investigation: 21%
- Financial Information: 23%
- Cohabitant/Spouse Information: 56%

OPM FY15
as of Dec 31 2014

- Release/Certification: 21%
- Gen Release: 10%
- Fingerprint: 69%
eFP Submissions

Electronic Fingerprint Submissions

<table>
<thead>
<tr>
<th>Month</th>
<th>Submission Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec-13</td>
<td>44%</td>
</tr>
<tr>
<td>Jan-14</td>
<td>75%</td>
</tr>
<tr>
<td>Feb-14</td>
<td>87%</td>
</tr>
<tr>
<td>Mar-14</td>
<td>90%</td>
</tr>
<tr>
<td>Apr-14</td>
<td>91%</td>
</tr>
<tr>
<td>May-14</td>
<td>94%</td>
</tr>
<tr>
<td>Jun-14</td>
<td>92%</td>
</tr>
<tr>
<td>Jul-14</td>
<td>94%</td>
</tr>
<tr>
<td>Aug-14</td>
<td>94%</td>
</tr>
<tr>
<td>Sep-14</td>
<td>94%</td>
</tr>
<tr>
<td>Oct-14</td>
<td>94%</td>
</tr>
<tr>
<td>Nov-14</td>
<td>95%</td>
</tr>
<tr>
<td>Dec-14</td>
<td>96%</td>
</tr>
<tr>
<td>Jan-15</td>
<td>96%</td>
</tr>
</tbody>
</table>
PSI-I Initiation = Shared Timeline

Initiation IRTPA Goal 90% <14 days

Day 0
- Subject releases e-QIP to FSO
- Subject provides eFP to FSO

FSO reviews and releases to PSM0-I
- FSO uploads to SWFT

PSM0-I reviews and releases to OPM
- SWFT sends eFP to OPM

OPM combines and schedules investigation

Day?
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

*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

**Average Days for Fastest 90%**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>31</td>
<td>35</td>
<td>31</td>
<td>27</td>
<td>21</td>
<td>20</td>
<td>15</td>
<td>18</td>
<td>16</td>
<td>14</td>
<td>16</td>
<td>14</td>
</tr>
<tr>
<td>DSS Processing Time</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Investigation</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
</tr>
<tr>
<td>Adjudication</td>
<td>43</td>
<td>70</td>
<td>26</td>
<td>40</td>
<td>58</td>
<td>34</td>
<td>20</td>
<td>33</td>
<td>26</td>
<td>22</td>
<td>22</td>
<td>22</td>
</tr>
</tbody>
</table>

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

100% of Reported Adjudications:
- Feb 2014: 777
- Mar 2014: 1,603
- Apr 2014: 961
- May 2014: 1,581
- Jun 2014: 1,481
- Jul 2014: 1,103
- Aug 2014: 932
- Sept 2014: 800
- Oct 2014: 1,206
- Nov 2014: 933
- Dec 2014: 983
- Jan 2015: 1,045

Average Days for fastest 90%:
- Feb 2014: 160 days
- Mar 2014: 136 days
- Apr 2014: 186 days
- May 2014: 126 days
- Jun 2014: 119 days
- Jul 2014: 135 days
- Aug 2014: 147 days
- Sept 2014: 167 days
- Oct 2014: 156 days
- Nov 2014: 156 days
- Dec 2014: 179 days
- Jan 2015: 185 days
Industry’s Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions

**Goal**:
- **Initiation**: 14 days
- **Investigation**: 40 days
- **Adjudication**: 20 days

### Timeliness Trends

#### Average Days for Fastest 90%

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>8</td>
<td>12</td>
<td>44</td>
<td>10</td>
<td>11</td>
<td>21</td>
<td>31</td>
<td>38</td>
<td>39</td>
<td>41</td>
<td>27</td>
<td>24</td>
</tr>
<tr>
<td>DSS Processing Time</td>
<td>28</td>
<td>21</td>
<td>17</td>
<td>16</td>
<td>14</td>
<td>13</td>
<td>2</td>
<td>44</td>
<td>37</td>
<td>37</td>
<td>31</td>
<td>36</td>
</tr>
<tr>
<td>Investigation</td>
<td>34</td>
<td>37</td>
<td>37</td>
<td>36</td>
<td>33</td>
<td>38</td>
<td>39</td>
<td>41</td>
<td>53</td>
<td>68</td>
<td>76</td>
<td></td>
</tr>
<tr>
<td>Adjudication</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

### Adjudications

- **100% of Reported Adjudications**
  - Feb 2014: 6,644
  - Mar 2014: 5,485
  - Apr 2014: 6,996
  - May 2014: 5,187
  - Jun 2014: 5,463
  - Jul 2014: 5,993
  - Aug 2014: 5,621
  - Sep 2014: 4,510
  - Oct 2014: 5,293
  - Nov 2014: 4,978
  - Dec 2014: 5,579
  - Jan 2015: 5,358

- **Average Days for fastest 90%**
  - Feb 2014: 72 days
  - Mar 2014: 72 days
  - Apr 2014: 100 days
  - May 2014: 59 days
  - Jun 2014: 63 days
  - Jul 2014: 66 days
  - Aug 2014: 74 days
  - Sep 2014: 85 days
  - Oct 2014: 81 days
  - Nov 2014: 93 days
  - Dec 2014: 103 days
  - Jan 2015: 118 days
Industry’s Average Timeliness Trends for 90% Top Secret Reinvestigation Security Clearance Decisions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>100% of Reported Adjudications</td>
<td>4,222</td>
<td>3,551</td>
<td>4,731</td>
<td>3,569</td>
<td>3,358</td>
<td>2,566</td>
<td>2,334</td>
<td>2,792</td>
<td>3,079</td>
<td>3,084</td>
<td>2,168</td>
<td>2,321</td>
</tr>
<tr>
<td>Average Days for fastest 90%</td>
<td>166 days</td>
<td>169 days</td>
<td>141 days</td>
<td>168 days</td>
<td>181 days</td>
<td>207 days</td>
<td>216 days</td>
<td>203 days</td>
<td>219 days</td>
<td>217 days</td>
<td>217 days</td>
<td>223 days</td>
</tr>
</tbody>
</table>

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