Minutes of the April 14, 2016 Meeting of the
National Industrial Security Program Policy Advisory Committee (NISPPAC)

The NISPPAC held its 53rd meeting on Thursday, April 14, 2016 at the National Archives and Records Administration (NARA) 700 Pennsylvania Avenue, NW, Washington, DC 20408. Bill Cira, Acting Director, Information Security Oversight Office (ISOO), served as Chair. The minutes of this meeting were certified on June 17, 2016.

I. Welcome and Administrative Matters:

The chair began the meeting by explaining that ISOO had cancelled the March 2016 NISPPAC meeting due to the unexpected shutdown of the Washington DC Metro system. He welcomed Ms. Beth Cobert, Acting Director of the Office of Personnel Management (OPM) and Mr. Richard Hale, DoD Deputy CIO for Cybersecurity, as special guests for today's meeting.

The chair advised that ISOO's previous director, John Fitzpatrick, has moved to a new position at the National Security Council (NSC), where he is the Director for Records, Access, and Information Security. In that capacity he functions as ISOO's NSC conduit and point of contact for policy and operational matters. Mr. Fitzpatrick remains very much involved with ISOO and the work of the NISPPAC. The selection process for a new ISOO director is underway.

The chair reminded everyone that this is a public meeting and is being recorded. Microphones are placed around the table for any committee member who wishes to speak, and a floor microphone is available for audience members. Anyone making a presentation can use the podium. Teleconferencing capability is set up for members who were unable to travel to the meeting.

The chair welcomed attendees, and after introductions, turned the meeting over to Greg Pannoni, the NISPPAC Designated Federal Official (DFO).

(See attachment 1 for a list of attendees.)

II. Old Business

Mr. Pannoni introduced Kathy Branch as the newest Senior Program Analyst at ISOO and the responsible officer for the NISP. He advised that there were no action items from the last meeting. The minutes of the November 2015 meeting and handouts for this session are in the folders handed out for the meeting. Mr. Pannoni then returned the meeting to the Chair.

(See attachment 2 for a list of this meeting's action items.)

III. New Business. Security, Suitability, and Credentialing Reform and Stand-up of the National Background Investigation Bureau (NBIB)

The Chair reminded the committee of the discussion at the November meeting regarding the breach of the OPM systems and the resulting impacts on industrial security. Much has occurred

in the meantime in terms of security, suitability, and credentialing reform. The chair asked Ms. Cobert and Mr. Hale to provide the committee with updates in those areas.

Ms. Cobert thanked the committee for giving her and Mr. Hale the opportunity to provide an update on the efforts to improve the background investigation process for the federal government. Ms. Cobert reminded the committee that OPM's Federal Investigative Services (FIS) conducts investigations for more than a hundred federal agencies, or about 95% of the total investigations government-wide. Following the increasing number of cyber security threats and the breaches of the OPM system last year, and building on the recommendation of the 120-day review that resulted from the Navy Yard incident, OPM began a comprehensive review of the background investigation process. OPM's aim was twofold: to find the best ways to secure the sensitive data collected as part of the background investigation process, and seek ways to modernize the function so that its governance, workforce, and business processes meet the ever higher performance standards required under the current operating environment. In addition, in January 2016 the Administration announced a framework for strategic and structural changes to modernize and fundamentally strengthen how the federal government performs background investigations.

As part of the reform effort OPM will stand up a new government-wide service provider for background investigations, the National Background Investigations Bureau (NBIB). DoD, with its unique national security perspective and capabilities, will design, build, secure, and operate in coordination with NBIB, new investigative information technology (IT) systems. Ms. Cobert described this as a true partnership, as DoD will be both the core IT supplier, as well as the largest customer in terms of the outputs of the background investigation process. She described NBIB's focus to produce effective, efficient, and secure background investigations for the federal government. This process will represent significant change in a number of ways. First, the head of the NBIB will be a presidential appointee and a full member of the Performance Accountability Council (PAC), to ensure the alignment of the operational and policy components of background investigations with all force components. Second, the NBIB will have the necessary operational flexibility and dedicated support structures for these specialized skills while still using OPM's existing general administrative support structure. Finally, NBIB will be able to operate and leverage DoD's considerable IT, national security, and cybersecurity expertise. Ms. Cobert explained that OPM has already begun the NBIB implementation and stand-up efforts by establishing a transition team. The NBIB transition team is made up of personnel with expertise in background investigations, suitability, and security policy, as well as those with significant organizational and change management experience. They had specifically embarked upon and succeeded in capturing a true interagency group. She described this initiative as a desire to utilize these different perspectives to maintain momentum where we have it, and accelerate improvements where we need them. Their work will focus on business process analysis and reengineering, resource management, IT and cybersecurity, the transition of systems to DoD, how to structure appropriate mission support services for NBIB, and overall, the change management process. They will continue to work closely with OPM's existing FIS leadership as well as with others across the government involved in the security and background investigation process in order to make the transition with minimal disruption to ongoing operations.

Ms. Cobert reminded the committee that there has been and continues to be an ongoing effort at OPM to strengthen systems in a focused, multilayered way. Over the past year OPM has made significant improvements in building the required defenses and responsiveness; citing as examples, the implementation and enforcement of the personal identity validation (PIV) cards for two-factor authentication for network access, and increased numbers of scans performed on a regular basis to review the network for signs of compromise. She recognized interagency partners, many of whom are in attendance at this meeting, to include: DoD, the Department of Homeland Security (DHS), the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the Office of Management and Budget (OMB), and others. OPM tightened policies and practices for privileged users, and initiated an ongoing review process for high value assets. OPM appointed a new acting Chief of Information Security (CIO), as well as four new Senior Executive Service IT leaders, and four new senior program managers. Ms. Cobert advised that she has a new senior advisor on cybersecurity and information technology from the private sector who has deep experience in running large IT organizations. Finally, OPM has the services of Ms. Lisa Schlosser, a former deputy federal CIO, as their acting CIO. OPM continues to strengthen their systems, even as they operate today, and to work closely with colleagues from DoD in this transition process.

Ms. Cobert advised that OPM is well aware of the need to address efforts to reduce the backlog of investigation, and is taking more steps towards this objective. OPM is continuing to put in place a number of efforts designed to run their processes more efficiently in coordination with stakeholders. OPM increased hiring capacity for federal staff field investigators with the target of acquiring 400 this year, and are well along the path to accomplishing that goal. OPM is also working closely with their existing contractors to help them increase their own capacity.

The PAC meets frequently, holds frank and open conversations, and is focused on the shared goal of achievement of a positive, effective, high quality process, which is ever responsive to the needs of its stakeholders. OPM is pleased with the team's approach of a whole government perspective.

Ms. Cobert then turned the presentation over to Mr. Richard Hale, DoD.

Mr. Hale introduced himself as the cybersecurity lead for DoD, as well as the responsible agent for putting the new investigations system on the ground. DoD is putting together a handpicked team to work closely with the NBIB, particularly on the business process reengineering effort. A new system must be sensitive to process change, moving from episodic, investigative-driven data about people to a more continuous big data approach. The requirements gathering phase is already underway. Much work was done prior to DoD's entrance, so DoD taking that previous work as the primary input starting point. DoD is going to create a model-based requirements process; i.e., an iterative build-and-try process that is primarily focused on better defining requirements. DoD is in the process of trying to design visible, customer-driven pieces that will be available early on so it can sort out what problems really need to be solved as opposed to the ones that someone thinks need to be solved. Some of that capability may turn into pieces of the operational system, depending upon how this end-to-end business process ultimately works out, and on the ultimate shape of the end-to-end architectural structure. One thing DoD has concluded already is that there are a lot of pieces to the puzzle. When the government decides to

look into someone's trustworthiness, it needs to begin by deciding precisely what it needs to know about the individual. The government has to have sound mechanisms in place to find out exactly what decisions to make about the individual, and how to publish those decisions so the right people can get the information they require in order to put the decisions to proper use. DoD is presently working the middle piece of the end-to-end process; but the cybersecurity, performance, and dependability pieces all have to be worked end-to-end, so DoD will need to work with all the players as it puzzles out the interfaces and the boundaries, which are not yet completely clear as it negotiates towards building the business process changes. As the government moves to a more continuous evaluation (CE) model, it will be accumulating far more data about people than it's ever had before, providing yet another incentive to make certain that the final structure will be an end-to-end process. DoD has many challenges regarding what legacy inputs are allowed to connect to whatever new processes are built: i.e., legacy material related to deciding to investigate a particular individual, making decisions about that individual, the resulting adjudication systems, and systems that hold the results of adjudications. Ultimately DoD understands that it must put processes in place that are as transparent as possible, and set standards that govern all forms of inputs and outputs. In the interim, the government will continue to use OPM's existing investigative infrastructure, as the DoD funding for this project begins in Fiscal Year 2017. However, DoD is permitted to design pre-acquisition activities. OPM is funding some of this early architecture and business process engineering work. The current system is going to remain operational for some years as the government transitions incrementally onto the new system. Even so, DoD is already committed to immediately putting more people on the ground at OPM to assist with better security and operability of the existing system and help manage the transition. Finally, it's not difficult to see that there will continue to be serious security, privacy, and civil liberties issues in the design of this new structure. The government will quickly come to know a lot about a lot of people, and will need much help from everybody in order to design the best way ahead.

Ms. Cobert introduced Mr. Jim Onusko, who in turn introduced Ms. Christy Wilder. Mr. Onusko introduced himself as leader of the NBIB transition team and Ms. Wilder as a key team member. He advised that the NBIB brings together a wealth of knowledge and experience in both change management and personnel security expertise. He described the team's five work streams:

- The first is change management, led by Ms. Victoria Gold of the Bureau of Alcohol, Tobacco, Firearms and Explosives, to drive the cultural change needed to meet the October 1, 2016 mandate to transform all aspects of the new organization into its required future state.
- Secondly, there is the business reengineering process work stream, which has already kicked off a process reengineering study. The study includes representatives from throughout the federal community to ensure the best opportunity to develop an integrated analysis of what needs to change, and develop the close working relationships necessary to build the requirements and to achieve the goals. Mr. Onusko noted that, the Defense Security Service (DSS) is already firmly embedded within that study group to work on behalf of industry.
- The resource management work stream, headed by Ms. Laura Duke, OMB.

- The IT work stream is led by led by Mr. Curtis Meyer to work closely with DoD and Defense Information Systems Agency to build the requirements for security and a new innovative, end-to-end IT system that can perform the mission.
- Mission support will be led by Jamal Harley, Office of the Director of National Security, ODNI, who will bring resource capabilities in both people and other resources to provide the dedicated support and operational flexibility necessary to make NBIB successful.
- Finally, for business process analysis and reengineering, Mr. Mark Sherwin, Deputy Associate Director, FIS, thoroughly understands the operations of the current FIS process.

Mr. Onusko advised that he has a very robust team to work collaboratively and aggressively with everyone in the development and deployment of an effective outreach process: to successfully identify stakeholder requirements, encapsulate them into complete working models, and subsequently align seamlessly with the DoD team to bring everything together.

J. C. Dodson, industry member, asked Ms. Cobert what industry could do to enable this initiative to move forward. Ms. Cobert responded that industry will be indispensable in providing input for stakeholder requirements from an end-to-end perspective. OPM will be able to leverage industry experiences and creativity to solve some of the knotty problems. Secondly, Ms. Cobert advised that OPM needs industry's patience through this transition. OPM will try to keep moving quickly, and will accept a little pressure from industry in the bargain. Industry is OPM's partner in this on many different dimensions. Industry needs individuals to be cleared, and industry will provide some of the data. There's a whole new and different way to interact as OPM works to set up a structured way to get the right inputs.

Tony Ingenito, industry spokesperson, stated that he appreciates the large influx in manpower authorizations necessary to achieve these bold objectives. In view of the process for training and implementation, he asked about the PAC's projected timetable to get everyone trained and in place. Mr. Ingenito advised that industry sees a continual growth of the backlog as well as the potential requirement for a drastic increase in cleared individuals to support some of these program initiatives. Ms. Cobert responded that OPM is aggressively bringing personnel on board and working to get them trained as quickly as possible. The initial commitment was to have 400 on board by year-end. OPM feels the same pressure as industry does, and knows the operational difficulties and challenges that having the backlog creates. OPM is continuing to work with their contractors to help them increase capacity. Ms. Cobert said that she realizes it is all going to take some time, but OPM has accelerated to where it is now. OPM is studying other initiatives to build up capacity faster and in a way that ensures people have the training they need to do their jobs right. The longer-term solution involves the re-compete of the field investigation contract, just recently out to the market, and thinking about ways OPM can create a more systemic solution for the long haul. OPM is working and tracking these things.

Greg Torres, DoD member, added that even now there is a team of government personnel looking at what can be done to mitigate the current requirements. Notwithstanding the rules and policies on what needs to be done, when it needs to be done, and how it needs to be done, this group is working right now in another meeting to understand where some impactful changes might be made to help buy down the current challenges. These challenges are being tackled on

several fronts simultaneously, and are being felt by industry as well as by DoD. Mr. Torres advised that he just received a request for a meeting with the DoD components to talk about the impacts to hiring, periodic reinvestigations (PRs), etc.; so he anticipates that the DoD group will come up with some innovative solutions to enhance the larger effort.

Dennis Keith, industry member, asked Mr. Hale if he could elaborate further on the model-based requirements process he had mentioned, and whether it's addressing the work processes in existence today or some yet to be articulated process. Mr. Hale responded that he was referring to both, and that the yet to be articulated process has already been partially addressed. Mr. Hale stated that the business process reengineering effort is in progress, but that there was much business process reengineering work done prior to now. He stated the desire to prototype some of the things that represent stable requirements, such as how people enter the system for the first time. Beyond that, DoD is planning to develop a new prototype in the cybersecurity arena that will be invisible to customers, to complete the application portion of the process. He also mentioned prototyping some of the interfaces to adjudication systems. He advised that at some point they will have contracts in place that will allow them to try many different things.

Kirk Poulsen, industry MOU attendee, asked Ms. Cobert if there was a timeline for when she expects to reach full operating capacity. Ms. Cobert responded that there is no complete timeline developed, as all the milestones have not yet been identified. Getting the initial standup of NBIB completed by the end of the current fiscal year is a top priority. OPM is concentrating on accelerating the progress, but in a way that keeps current operations running at the pace they need to be, while maintaining proper quality and security. A high priority of the transition team will be keeping all these things in balance. As OPM establishes priorities they will be made available. OPM needs to be held accountable for meeting the deadlines to which all have agreed.

Mr. Pannoni, ISOO, commented that throughout his years of experience one of the themes he has seen many times over is that we often see good, conceptual policies, but fail to follow through on implementation and consistency. Reciprocity is just one example. This reality transcends not just the clearance environment, but also the suitability environment; such as, getting access to a base, or being able to adapt to different command requirements. While the idea of a champion of consistency and implementation is something that would be very helpful, we're not sure who that champion would be. Ms. Cobert responded that her varied experiences have shown her that we do indeed have responsibilities that cut across the federal government, and that balancing these is a hard thing to do. She said that one of the themes she has stressed with her teams in a number of different areas is that once the policy is in place, getting clarity and consistency into its implementation is important. She agreed that we need to spend as much, if not more time, thinking about how we communicate, how we make things clear, and how we make things happen in the many disparate places it has to happen. She advised that was a factor for the transition team; i.e., broad interagency representation, bringing together broad experiences on how things happen differently in different places, such as Department of Veterans Affairs versus the Department of State, or the multiple layers of DoD. OPM gathered people who bring different perspectives to policy and how to implement it. She agreed that it does have the critical importance Mr. Pannoni suggests. Ms. Cobert challenged the NISPPAC to continue to raise the issue, as ideas of this kind, as much as policy and model design, will be welcome in terms of what will make the network perform effectively.

Tony Ingenito continued this idea by pointing out that the direction industry is trying to take is development of policy at the top while minimizing the necessity for each entity below to come behind with their own policy; which negatively effects timeliness issues and promotes inconsistent guidance. He stated that it would be nice to see an approach to design from the top of government that doesn't automatically require numerous changes in order to personalize it for each particular agency or branch. Mr. Hale responded that many here agree with that wholeheartedly, but that the challenge is in finding a balance. For example, it is easy to write policy in such a way that is so generic that nobody can object to it. However, inconsistency soon creeps into the equation. He advised that once you attempt to establish specificity you begin to get a lot of objections, as everyone feels the need for the policy to meet all of their needs. He continued that experience has taught us that the challenge is in trying to find that sweet spot where you have enough specificity that everybody's not doing it differently but enough leeway that you're not trying to solve every individual organization's challenges, and that returns us to the need to find balance.

Dennis Keith expressed interest in the concepts of change management and cultural work stream. He asked for a description of the inherent challenges. Ms. Cobert responded that this involves a set of issues that cut across multiple dimensions. An example is the NBIB continuing some of the transformation that started with strategy and policy recommendations from the 120-day review; that is, how to move a periodic, paper-based, or person-based investigatory model to a CE model more driven by data analytics. There are cultural and change management issues to create the operational flexibility and dedicated resources within NBIB. There are also implications for the rest of OPM to ensure it maintains a dependable and dynamic workforce inside the federal government. Background investigations are an important component but are not the only thing OPM does. In order to make the changes necessary to have NBIB operate as intended, there are implications for the rest of OPM. OPM is building a tighter working relationship with DoD within the IT community. That alone is profoundly different from how OPM has operated before. Ms. Cobert continued that OPM and DoD has worked together on so many different things over time, particularly following the breach of OPM's data, on a whole range of operational contingencies, including the contract for identity theft protection. We worked with Naval Sea Systems Command as our contract support. We worked with the Defense Logistics Agency and the Defense Finance and Accounting Service to get the letters out. This was a whole new set of things that we hadn't done before. Ms. Cobert shared that she spoke daily with Mr. Hale as they were working on these things. She concluded that there have been real opportunities to build on successes, and to develop the mindset that we are truly creating something that serves not just DoD and OPM but the entire federal government and our industry partners. This will ultimately require changes in people's jobs and how they do their every-day work.

Mary Edington, industry attendee, asked how Ms. Cobert perceives using social media in future investigations. Ms. Cobert responded that they are continuing to work through a social media policy, and are working with a pilot model at OPM. Ms. Cobert pointed out that DoD is also working on this issue through their own pilot model. In as much as this is a totally new field, Ms. Cobert recognized the need to do it right, with both policy and an appropriate attitude that respects people's privacy, but leverages the relevant information that is available.

Ms. Cobert thanked the NISPPAC for allowing her to speak, and reiterated her request for their continued inputs, noting that the PAC needs to continue to gather feedback from its industry and government partners. She challenged the group to remember that this a task that falls to all of us. We must all play a role as we will all live with the consequences of success or failure.

IV. Reports and Updates

The Chair thanked Ms. Cobert, Mr. Hale, and the NBIB leadership team for taking their time to come and speak with the committee. He then turned to the Reports and Updates portion of the meeting, and called for Patrick Viscuso, Associate Director of ISOO for the Controlled Unclassified Information (CUI) program, to provide an update.

(A) CUI Updates

Mr. Viscuso began by outlining a brief history of the CUI program, established in 2010 by Executive Order 13556 (the Order). NARA is the program's executive agent. He described three principle CUI program elements.

The first element is the program's scope. The CUI program encompasses all information that law, federal regulation, or government-wide policy requires to be protected (outside of classified information). The scope has widened to include a CUI registry, which is now available online. This registry contains 23 categories and 83 subcategories of unclassified information that require protection throughout the executive branch. Each one of these categories contains links to the authority, law, regulation, and/or government-wide policy that requires the protection.

The second program element involves guidance. The Order speaks to consistency in government practice in four main areas: safeguarding, dissemination, marking, and de-control of the information. For that reason the Order directed that the CUI Executive Agent issue directives. 32 Code of Federal Regulations (CFR), Part 2002 has been in development, through the efforts of a CUI Advisory Council, for five years. The Order also required consultation with affected agencies. The Advisory Council is primarily based on the membership of the Chief Financial Officers Council (CFOC), which controls most of the federal budget. In total there are 28 agencies represented in the CFOC, to include the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI). This is the team that informally developed the federal regulation, and embarked on the formal OMB-managed public rule-making process. Upon completion of numerous interagency comment periods and a public comment period, ISOO is now at end stages of finalization of the federal rule. ISOO expects a May 2016 issuance of the federal rule, with an effective date of 60 days subsequent to its issue.

The third part to the program is phased program implementation. ISOO has established the milestones, phases, and deadlines in a national implementation issuance that will accompany the federal rule. Some of the milestones include the requirement for a 180-day period in which the parent agencies and their components are to complete the internal development of policies that implement the federal regulation. Upon completion of the initial 180-day policy development period, the federal rule will provide for an additional 180-day period for agencies to complete the

development of training for the parent and its components, followed by a final 180-day period for completion of the training of the federal workforce. The CFR will also call for a transition assessment and development of transition plans within the first year for IT systems, centered on requirements consistent with OMB policies and guidelines and standards of the National Institute of Standards and Technology (NIST) for moderate-level information protection confidentiality. Executive branch agencies will be required to develop a self-inspection program. ISOO, as the CUI Executive Agent will be required to submit an annual report to the president on the status of the program and its implementation.

With regard to industry, ISOO intends to develop a Federal Acquisition Regulation (FAR) clause to ensure consistency in the implementation of the requirements of the program within industry. This FAR clause will reference a document developed in partnership with the NIST, Special Publication 800-171, which addresses how moderate confidentiality should be implemented within the non-federal environment exclusive of any purely federal requirements (such as those developed for a Continuity of Operations Plan (COOP)). These were some of the factors that guided ISOO in the development of the NIST document, and anticipate in developing the FAR clause using the usual processes of the FAR Council and its public rule-making process. This will involve considerable comment from industry. ISOO has an interest in hearing from industry on these points. To that end ISOO is meeting with industry associations to learn of their concerns and needs. ISOO is also very concerned about the university and the academic communities. ISOO has had very good discussions with associations involved in the life of these communities, focusing discussions primarily on the concepts inherent in fundamental research and the need for research protection in order to maintain our nation's technological edge.

Dorothy Rader, industry attendee, asked about the expected timeframe for the FAR clause. Mr. Viscuso responded that the FAR clause should require about one year to complete, as it will be subject to public comment. He stressed the CUI community's desire to hear any concerns or needs that the industrial community has.

The Chair then asked Mr. Pannoni for an overview of the revisions to the NISP implementing directive.

(B) NISP Implementing Directive Updates

Mr. Pannoni prefaced his remarks with a public acknowledgement of the efforts of Mr. Viscuso and his CUI team. He noted that this CUI process has been a complex and challenging one, especially in view of the fact that the team has worked tirelessly to stand up a completely new and ground-breaking program.

Mr. Pannoni then provided an update on the effort to revise the NISP implementing directive. He reported that ISOO has been meeting with the NISP cognizant security agencies (CSAs), along with DSS, and the CIA as the government's primary program implementers, and the group is near completion of an initial draft revision. He pointed out that this revision began as a result of the insider threat program that required that provisions be put in place for industry. He noted that as the group started to study the directive, it recognized gaps in the policy for the agencies. Agencies were relying on the National Industrial Security Program Operating Manual

(NISPOM), which is industry's operating manual. It is not the document from which the government is supposed to take its direction. The group focused on the areas of the facility security clearance process, foreign ownership control and influence standards, and national interest determination standards. The group recognized the need to get these programs documented as a single, integrated, cohesive program into the federal regulation. For example, facility security clearance is not a term that every CSA uses. The intent is to establish a clear, identical, operating baseline, so that regardless of whether we use a term like "facility security clearance" or "an eligibility determination for an entity," we all mean the same thing, expect the same results, and do so in a way that we will account for essential conditions and terminology. The team is to meet again this afternoon, and hopefully, in a couple of more meetings, will be able to provide the revised document to all impacted NISP government agencies, consult with each other as required by the executive order, and ultimately submit to the NSC for approval. Subsequent to approval, we will place a notice in the *Federal Register* in order to offer the suitable public comment period.

Michelle Sutphin, industry member, asked if there was any anticipation that this process would result in impact to the NISPPAC charter or bylaws. Mr. Pannoni responded that he thought not; nor is any impact expected to the NISPOM itself because the group is proceeding very carefully to avoid violating any existing requirements.

The Chair then called for the update from the Office of the Undersecretary of Defense for Intelligence (OUSD(I)) and invited Greg Torres, Director of Security, to address the committee.

(C) DoD Updates

Mr. Torres, OUSD(I), expressed his appreciation for the opportunity to return to the NISPPAC. He stated that he had a few items to speak to relative to the NISP and the NISPOM. First, he advised that change two to the NISPOM has cleared DoD legal sufficiency review. Valerie Heil, of his office, is preparing it for publication. He stated that the Industrial Security Letter (ISL) pertaining to insider threat is in legal sufficiency review. He acknowledged that the ISL needs to come on the heels of the NISPOM change very quickly. To that end, DoD is having regular meetings to prioritize items to move the process along.

Mr. Torres announced that Mr. Ben Richardson, from the Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics (OUSD(AT&L)), has been selected as OUSD(I)'s Deputy Director of Security. Mr. Richardson brings a history and wealth of knowledge in everything from the Committee on Foreign Investment in the United States (CFIUS) to previous DSS service.

Mr. Torres noted that there had recently been a number of government agencies expressing an interest in obtaining access to the Joint Personnel Adjudication System (JPAS). He advised that the idea deserves some dialogue, so should any of those agencies be represented here today, he would remain after the meeting to discuss their concerns and needs.

The Chair then reminded everyone that Mr. Stan Sims has recently retired and that DSS has a new director, Mr. Dan Payne, from the National Counterintelligence and Security Center. Here

today, on behalf of Mr. Payne, is Mr. Fred Gortler, the Director of Industrial Policy and Programs, who will give the DSS update.

(D). DSS Update

Mr. Gortler began by explaining that Director Payne had returned from temporary duty only late last evening and could not attend today's meeting, but that he feels certain that they will be able to introduce him to the NISPPAC at its next meeting in Nashville, TN. He then described the new director's four main agenda items: improving integration of counterintelligence and security; improving integration and collaboration at the federal level; building upon an already solid foundational partnership between government and industry; and strengthening relationships with our foreign allies.

Mr. Gortler expressed the desire to add to Mr. Torres remarks regarding the ISL on insider threat. He pointed out that it was in the November/December timeframe that representatives from the NISPPAC came together for the first time to help DSS develop the ISL. He acknowledged how important these efforts were in development of refinements to implementing NISPOM change two, and the significant contributions made by OUSD(I) and Mr. Torres.

He explained that he was joined today by DSS subject matter experts to address Personnel Security Investigations (PSI or any other topic related to industrial security initiatives. Mr. Gortler then turned the floor over to Mr. Keith Minard.

Keith Minard, DSS, provided an update and presented the committee a snapshot of DSS's annual security cost collection survey. (See attachment 3.) Mr. Minard pointed out that 32 CFR, Part 2004, *National Industrial Security Program Directive No. 1*, requires the Secretary of Defense, acting as the Executive Agent for the NISP, to collect cost estimates for NISP-related activities of contractors, licensees, certificate holders, and grantees, and report them to ISOO. He explained that this year's collection was conducted in January and February, and represented a sampling of about 1700 companies. The sample was analyzed to determine the total cost for the approximately 13,000 facilities under DSS cognizance. These costs, approximately $1.27 billion, have been pretty consistent since about FY 2009.

Mr. Minard then presented an update pertaining to the Electronic Questionnaires for Investigations Processing (e-QIP) system submissions. He explained that they were still dealing with funding constraints, and had been forced to limit the number of investigation requests submitted to OPM in order to remain within their budgetary authority. DSS continues to prioritize initial investigations and PRs. He challenged the committee to contact DSS with any special concerns.

He advised that DSS has restructured the call center, (now the knowledge center), providing callers with decentralized capabilities for help with account lockouts, to contact with the Personnel Security Management & Oversight for Industry (PSMO-I) office, obtain facility clearance information, and access to the Office of Designated Approval Authority (ODAA) Business Management System (OBMS), as well as access to the international office and the ability to reach the DSS policy office for NISP policy concerns. Mr. Minard recommended that

everyone visit the DSS website to search for the knowledge center and locate important contact numbers.

Mr. Minard described the current status of the present PSI survey, stating that the March 2016 suspense had been extended for a few days in hopes that response would exceed last year's 89% capture. He reminded everyone that it's critical for DoD to obtain information to properly budget for the upcoming years' investigations requirements.

Finally, Mr. Minard reported that United States Postal Service (USPS) has signed an agreement with DoD to provide industrial security services, becoming the 31st agency for DSS to provide oversight of cleared contractor operations related to the NISP. He welcomed USPS as the newest agency to enter the program and contribute to its recent, rapid growth.

Quinton Wilkes, industry member, asked if DSS plans to communicate with industry with regards the backlog of cases pending at PSMO-I, so that we can get a clearer picture of the current status of the clearance process. Ms. Heather Green, DSS, responded that they were continuing to process all requests, but that it was simply requiring a longer time, primarily as a result of the number of quarterly applications. Ms. Green stated that she would ensure that the latest figures were placed on the website as soon as possible so as to bring it up to date.

Kim Baugher, member from Department of State (State), asked if DSS is requesting additional funds to address the backlog to help relieve some of the pressure. Mr. Minard responded that throughout the year these issues are addressed to DoD, up to and including asking for the possible redeployment of budget resources, in an attempt to better meet budget requirements. He reminded the committee that it is of paramount importance that DSS capture, though the PSI survey, the actual industrial costs. Therefore, it is critical for industry to submit their cost estimates right away, as this becomes the baseline for the enunciation of continued budgetary requirements. Mr. Minard also pointed out that DSS, like many service-providing agencies, isn't always able to capture exactly how many classified contracts will be required during a year, so they often have to guestimate some future budget requirements.

Steve Kipp, industry attendee, asked if DSS takes the growing backlog into consideration when requesting future requirements. Mr. Preston Harper, DSS, explained that all deferred cases would be captured in future requests. Mr. Torres, DoD, added that quite often within DoD funding doesn't come all at once, but is received in increments, which might appear as a straight line increment, but may actually be either above or below that particular line. Therefore, while you exceed that line, you only receive funding at the line, and a new challenge is created. DoD is constantly looking at the underlying question of how to do a better job of projecting requirements. Further, Mr. Torres pointed out that there is a study in progress at the Defense Personnel and Security Research Center that is attempting to understand how to improve the budget estimation process. He suggested that this will be considered for inclusion in the new end-to-end system to better capture requirements.

Mr. Minard added that the investigations that DSS processes are only for access to classified information. When contractors are required to submit investigations for base access, they are a government agency responsibility that affects funding and managing. Mr. Minard advised

industry to notify DSS of any deviations to the government policy. While the numbers may seem small, they impact DSS ability to process the investigations needed to support classified contract work. Mr. Gortler added that DSS does account for the backlog, and in support of Mr. Torres point, DSS is spending even faster in an attempt to maximize the flow, and is working with higher headquarters to get additional funding for next quarter. DSS will ensure maintenance of a clear line of communication to industry relative to our progress in this process.

J. C. Dodson asked about this year's participation rate in the cost collection sampling? Mr. Minard responded that this year 1700 companies made up the survey sample for the cost analysis.

Dennis Keith asked how the data from the cost collection is used. Mr. Minard responded that the cost collection data is presented to ISOO for inclusion in its annual report to the president. Mr. Pannoni clarified by stating that ISOO has an obligation to report to the President on the cost of implementing the NISP on the executive branch side, as well as for industry. Mr. Keith then asked if the data is subsequently used to affect any adjustments to policy. The Chair responded that the data is not used in that way, but rather the concept goes back to the late 1970s when it was determined that ISOO should include in its report the levels of classification activity every year and the amount of money that is spent on the security of classified information, as a way for the government to ensure public accountability and openness.

Mr. Dodson then suggested that, on behalf of industry, he would be interested in seeing whether the current methodology, established in 2008, really reflects industry costs and takes into account how the defense industrial base has expanded in non-traditional ways. Mr. Dodson also expressed a desire to acquire more detailed information to determine if this methodology is still reasonable and meeting the intent of the NISPPAC and ISOO. Mr. Dodson proposed meeting with DSS.

The Chair then called for the combined industry update.

(E) Industry Update

Tony Ingenito, industry spokesperson, began by thanking Ms. Cobert and her staff for providing an updates regarding the OPM breach, and expressed industry's desire to learn more of the upcoming transition plan. (See attachment 4.)

Mr. Ingenito offered appreciation for the CUI update. He added that industry is continuing to get requirements through contract clauses, based on the NIST publication 800-171, even though CUI is not yet promulgated by the FAR rule. He advised that industry tries try to educate their contracts personnel to look for and identify these contract clauses, so that they can challenge the agencies that are prematurely implementing.

Mr. Ingenito expressed industry's appreciation for conclusion of the legal sufficiency review process for the NISPOM change two, and looks forward to implementation. He noted that industry's primary concern is a desire for a NISPPAC-sponsored insider threat working group that would meet on a regular basis. It would be the key to making the NISPOM change work

effectively. Mr. Pannoni offered to place that under the NISPPAC's jurisdiction, and to create this ad hoc working group. Mr. Ingenito welcomed such an initiative.

Mr. Ingenito expressed that industry is anxious to see what DHS develops as they begin their role as a CSA. Mr. Ingenito reported that he had just now received an e-mail that referenced some of the non-NISP entities that would fall under DHS cognizance who are inquiring about how they can participate and provide input. Therefore, he plans for industry representatives to sit down with DHS officials in an attempt to learn more and to determine what role(s) industry might need to play.

Mr. Ingenito updated the committee on the government-industry work on the NISPOM rewrite. He stated that much positive work has been completed, and that they have provided the substance of these efforts to the CSAs. Industry is waiting for final CSA review of the proposed changes. He applauded the efforts of OUSD(I) in working with the both government representatives and with government and industry representatives as a coordinated working group effort. It gave industry an opportunity to provide their view of upcoming challenges.

With regard to the NISPPAC Special Access Programs (SAP) working group, Mr. Ingenito recognized that all of the SAP manuals have been published, and that industry has received notice that the Department of the Air Force's SAP Coordination Office (SAPCO) has rescinded the Joint Air Force, Army, and Navy guidance; however, industry has not yet received notice from the other service SAPCOs. Industry is concerned that the SAP working group is not meeting on a regular basis at the same time that industry is required to implement the Joint SAP Implementation Guide (JSIG) and the Risk Management Framework (RMF). Mr. Hale asked if there was inconsistent guidance from agencies with regards to JSIG and RMF. Mr. Ingenito responded that it's not inconsistent guidance, but that each information assurance specialist has his or her own unique process interpretation that requires much dialogue in getting plans in place. When there are frequent changes in both government and industry personnel, the result is redoing each process, which requires more time and effort.

In the area of policy integration, Mr. Ingenito advised that industry is tracking more than 80 different government initiatives that impact industry. He reported that industry has its own working group, and that there is significant progress towards establishing some working guidance in this area, so that industry will be ready to identify probable costs and impacts.

Mr. Ingenito spoke briefly about some of the issues being addressed by the NISPPAC working groups. He pointed out the concern with the Tier 3 investigative requirements, pointing out that the process is slowing dramatically. He encouraged industry members to provide the most accurate projections possible and to take into account the fact that they are obviously forecasting significant growth rates due in part to substantial acquisitions recently awarded and projected out perhaps as far as 2019. He advised that clearance requirements are on the rise even as investigative times are slowing.

Charlie Sowell, industry attendee, interjected that both defense industry and DHS are considering moving towards full-scope polygraphs, and that this would add yet another pressure on an already over-stressed clearance system process. Mr. Ingenito agreed, and pointed out that some

within the intelligence community (IC) are moving to an even more restrictive polygraph program, so that there could be increases in the number of people being disqualified from serving in the jobs they currently hold. In addition, he reminded the committee that recent discussions, including in the DSS stakeholders' meeting, have indicated that the FBI has a significantly reduced capability to conduct the checks required for interim clearances and those necessary for common access card acquisition, notwithstanding the recently completed automation of the fingerprint program, and industry is beginning to feel the impact.

With regard to the NISP Contractor Classification System and automating the DD Form 254 process, Mr. Ingenito advised that industry continues to be involved. Participation in the beta test is a very welcome prospect for industry.

Mr. Ingenito reported that industry enjoys continued participation in the development of National Industrial Security System, and looks forward to the next meeting. He recognized concern with the Joint Verification System, to replace JPAS, which is scheduled to be rolled out to industry in November 2016, as industry has not yet seen a training plan for users. He pointed out that experience has shown that the new system will suffer without an effective, government-designed training plan in place at the time of rollout.

The Chair moved to the working group updates, and called for Tracy Brown, DSS, to provide the Certification and Accreditation Working Group's. (C&AWG) report.

(F) Working Group Updates

C&AWG Updates

Tracy Brown, DSS, provided the C&AWG update. (See attachment 5.) She stated that she would provide the RMF update for DSS, on behalf of DoD as the CSA. She reported that RMF is replacing the certification and accreditation process. It was established by the NIST in partnership with DoD, the intelligence community, and the Committee on National Security Systems (CNSS). It provides an effective and efficient approach to risk management while creating a common foundation for information security systems supporting reciprocity. She cited the key reference documents, including the NISP's SP 800-37, SP 800-53, and SP 800-53A, the CNSS's CNSSP 22, CNSSD 504, CNSSI 1253, and CNSSI 4009, as well as the NISPOM change 2, DoD 5220.22-M, which will require that all CSA's develop a process manual. She defined the RMF as a six-step process, encompassing system categorization, the selection of security controls, implementation of security controls, controls access, system authorization, and continued monitoring of the controls throughout their life cycle. To that end, DSS is scheduled to release its assessment and authorization process manual in July, 2016, that will include a phased approach to implementation to be completed by March of 2017. She stated that DSS has begun a joint government-industry pilot program to help understand the basic challenges inherent in RMF. She pointed out that for the pilot, which uses the draft assessment and authorization manual, DSS has already developed all the required supporting artifacts. At the conclusion of the pilot, DSS will update the manual prior to its July release. In support of this process development, and in order to prepare industry for RMF conversion, the DSS's Center for Development of Security Excellence (CDSE) already has eight online classes that

familiarize participants with the various steps in the environment. To supplement this training DSS will be presenting webinars for assessing the controls. The initial webinar is tentatively scheduled for June 15, 2016, with others to follow in July. Finally, Ms. Brown reviewed the Interim Authorization to Operate and the Straight to Authorization to Operate timeliness statistics, advising that DSS is still authorizing systems to operate within the 30-day objective. With maturation of the RMF process, DSS expects those figures to require some upward adjustment, and that DSS believes the pilot program will prove to have been a helpful instructor.

Mr. Pannoni asked if all systems must convert to RMF by 18 months from August 2016. Ms. Brown responded that that was accurate, and that as of August 1, 2016 no new authorizations would exceed 18 months. Further, she stated that systems that are not stand-alone would follow the existing process until next year.

The Chair then called for the report from the Personal Security Clearance Working Group (PCLWG), and explained that the updates would be presented by the group's new Chair Ms. Kathy Branch.

PCL WG Update:

Ms. Branch, ISOO, thanked the Chair, expressing appreciation for the opportunity to serve as the PCLWG Chair. She explained that the working group would continue to examine the statistics provided by the agencies that perform background investigations and make adjudicative determinations. However, she described a change in the group's focus to a greater emphasis on personnel security issues that impact industry's ability to perform on classified contracts. This includes the investigative reform efforts and the standup of the NBIB. She noted that a representative of the PAC has agreed to become a group member. Ms. Branch then called for Ms. Donna McLeod to provide the OPM update.

Ms. McLeod, OPM, explained that the focus of her presentation would be the FIS (see attachment 6), and specifically the efforts to reduce the investigative backlog. She described these efforts as both streamlining for the future and improving the current process for background investigations. Even as timeliness continues to increase, OPM's focus is on what can done to decrease the numbers and reduce the backlog. She described improvements in our report writing; i.e., streamlining content so that investigators can complete their reports in less time. This would reduce the time required for adjudications, and subsequently, the time required for the review process. OPM's FIS welcomes Director Cobert's goal to hire 400 additional investigators. Ms. McLeod advised that new investigators attend a four-week training class, followed by a mentoring period, and then a one-year, on-the-job probationary period. That means that there is considerable time before a new hire can perform on his or her own. Ms. McLeod referenced the efforts mentioned by Director Cobert to also increase the contractor workforce, which would provide greater resource availability, and help to reduce the backlog. Finally, she pointed out that the current FIS backlog is not unique. Other investigative agencies are experiencing the same backlog, such as FBI. OPM has pledged to continue to identify any methodologies that might improve the process.

Ms. Sutphin asked what FBI is doing to address the problem they are experiencing. Ms. McLeod responded that OPM had recommended to FBI that they consider having resources from FIS perform the FBI tasks. However, specialized training is required to perform FBI work, and the resources would have to be physically located with FBI. OPM is aware that FBI is also looking at bringing on additional resources, and that they are working the same internal processes OPM is working.

Ms. Sutphin then asked if FBI was considering contracting work out to industry. Ms. McLeod responded that she was unaware of such a plan. Mr. David Morrison, ODNI, offered that he was aware that the FBI was trying to hire additional contractors. He was also aware of FBI considering reaching out to retired special agents who would not require the same learning curve as that of a new hire. However, the idea has not yet reached maturity. Mr. Morrison also offered that FBI is willing to prioritize the requests submitted to them. Ms. McLeod added that OPM's FIS has asked agencies to prioritize the work being sent to them. Ms. McLeod advised that OPM should be notified of a cancellation as soon as possible, so that resources are not spent on investigations that are no longer required.

Mr. Wilkes asked if this was an automated process, one that could be automated, or something that requires human intervention. Ms. McLeod responded that they are working to improve the process, which is now a paper one. Until this is accomplished there is a manual search that has to be done with every record check.

Mr. Sowell noted that there are a number of initiatives under way to address the backlog. He asked if there were any projections as to when it will be eliminated. Ms. McLeod responded it will take several years before we can hope to get well, based on the ability to hire and get investigators onboard.

Ms. Cobert pointed out that it's a dynamic process, and with unexpected increases in demand this year. OPM would have had a backlog regardless, but it wouldn't have been as severe. OPM is looking at the mix and the different levers to pull on the demand side, understand the prioritization on the supply side with contractors, and the efficiency side with process changes. The forecast is dependent on many diverse variables. As it has taken us a while to get to the situation today, it's going to take us a while longer to work out of it. The rebuild of the NBIB systems with DoD will help, but some aspects will cause improvements while some will not. Perhaps this is not a very satisfactory answer, but OPM continues to focus on the things that seem to offer the best chance to actually accomplish something that will result in real improvements.

Mr. Pannoni pointed out that over the years assistance of non-federal partners in the investigative process has been spotty and uneven, especially in terms of cooperation in providing investigative information at the state and local levels. Mr. Pannoni asked if a strategy has been developed to get better cooperation. Ms. McLeod responded that OPM is trying to work through these partnerships. A dedicated group within FIS reaches out to the providers to make sure they understand the importance of getting the information to the investigation. Ms. Cobert further explained that through some excellent bipartisan help in Congress, OPM secured some provisions in the last National Defense Authorization Act (NDAA) related to the law

enforcement status of investigators. Therefore, there have been improvements in different pockets. The capability to work with law enforcement was one of the recommendations emerging from the 120-day review and the records access taskforce.

Ms. Sutphin stated that she wanted to emphasize the FBI's position in this equation, as right now fingerprint checks are not required to get an interim clearance, but they soon they will be. She pointed out that if there are delays with the fingerprint checks, industry can't get interim clearances, and can't put people to work. This will become a very serious issue very quickly. Ms. McLeod responded that the backlog is not caused by the fingerprint checks, but rather the name-based search done through the FBI that causes the delay. After some further discussion, Ms. McLeod clarified that there will continue to be delays, as the name-based searches are a part of the process, and that at this time, we cannot change that fact. Mr. Wilkes also pointed out that the interim clearance rate is the result of a waiver. Once that waiver expires, there will be impacts that cause the backlog to get even worse.

The Chair then called for Intelligence Community's (IC) personnel security metrics.

Gary Novotny, ODNI, pointed out to the committee that his presentation uses the PAC's security clearance methodology (see attachment 7), looking at end-to-end timeliness beginning at the initiate phase through adjudication. No pre- or post-coordination metrics are included. He described the end-to-end timelines, for both the secret and the top secret submissions, investigations, and adjudications are continuing to rise. He noted that PR's present a somewhat better picture, as their timelines have now lowered. He reminded the committee that one of the initiatives in the NDAA was for the ODNI to reduce the PR backlog and timelines, and the metrics for the first quarter support that effort. ODNI will begin to analyze the second quarter data and reach out to affected agencies to see if the first was simply an anomaly or if there is something that that can help further reduce the backlog.

Mr. Novotny presented the components of secret investigations, top secret investigations, and PRs into initiate, investigation, and adjudication phases. The metrics indicate that both the secret and top secret investigations fail to meet the 40-day mark. The majority of the failure to meet the end-to-end timeliness goal is in the background investigation phase. There is overall improvement with the PRs, except in the investigation phase, expected to continue to rise. The ongoing efforts of ODNI, OPM, and OMB will begin to impact the backlog and, in time, the timelines will show improvements.

Mr. Novotny reminded the committee that ODNI is not only focused on the timeliness, but also on the quality of the background investigations. OPM and ODNI issued the quality assessment standards and implementation plan some time ago. ODNI recently provided the implementation plan to the heads of the Executive branch agencies. ODNI is creating a tool to collect quality metrics to ensure that adjudicators receive a quality product.

Mr. Novotny advised that ODNI has a directive that is nearing completion regarding the minimum mandatory reporting requirements for the secret-, top secret- and top secret/SCI-level population, which contains criteria for what needs to be reported to the security office.

ODNI expects to complete and publish a social media policy in the near future that will explain what can and cannot be done when using the various social media formats.

The Chair then called for Daniel Purtill to present the DoD Consolidated Adjudication Facility (DoD CAF) updates.

Daniel Purtill, DoD CAF, began by briefly reviewing workload trends and advising that the CAF is presently in reasonably good health. It continues to trend in a positive direction, and their backlog is reduced to the point that it should be completely gone by the end of calendar year 2016 (see attachment 8). Mr. Purtill expressed confidence that the CAF will be in a position to absorb the impacts resulting from the new FIS standards and the CE implementation process. In addition, the CAF has excellent relationships with its partners throughout the enterprise that can help ensure continued success.

Mr. Wilkes asked Mr. Purtill to update the committee on current e-adjudication trends and how these are affected by Tier 3 investigations. Mr. Purtill responded that the CAF was within a few weeks of achieving final approval on Tier 3 e-adjudication implementation. Through Tier 3 implementation the CAF is expecting a lower secret-level pass rate. At the same time the CAF is going to be looking at a broader range of cases which will include both National Agency Check, Local Agency Check (NACLAC) and Access National Area Check and Inquiries (ANACI), so the CAF expects little to no negative impacts. Mr. Wilkes asked if as a result of the implementation of Tier 3 investigations the CAF was still trending upwards even though being forced to go to an adjudicator, and thus incurring a longer processing time. Mr. Purtill responded that the CAF has seen a dramatic shift, but that with next to no NACLACs at this point, combined with almost all Tier 3s coming in at the secret level, the system is quite capable of adapting, especially in view of the fact that all Tier 3 adjudications are manual at this point.

Mr. Purtill reported the CAF's Intelligence Reform and Terrorism Prevention Act (IRTPA) compliance as having returned to a much more normal level, and continuing to work through that backlog. Because the CAF doesn't count a case until it is finished, the IRPTA numbers tend to spike only whenever there are old cases still in the system. Finally, Mr. Purtill was able to report that with PRs finally back under the 30-day mandate, which provides some leeway.

V. General Open Forum/Discussion:

The Chair opened the meeting to comments from the attendees, or any issues of interest, or any concerns. Kim Baugher, State Department, took the opportunity to address the committee on the subject of JPAS access as it pertains to non-DoD, Executive branch agencies. She began by acknowledging that all Executive branch agencies take very seriously the security of our nation's secrets as well as the trust placed in private industry to work with classified material to fulfill the contractual requirements necessary to meet the government's business needs. Indeed, the scope and complexity of just such needs reflect the fundamental reasons why both DoD and non-DoD agencies have worked so hard to establish effective industrial security programs and why the companies represented here today and others across this nation have done the same. She expressed a personal pride in the fact that the Department of State has provided her with the resources necessary to develop a robust industrial security program, and pointed out that they

could not hope to accomplish its varied, world-wide missions without its contractor partnerships, which are without question critical to the protection of our classified information, the security of our domestic buildings, the secure design and construction of our embassies overseas, and the security of the lives of our personnel and other agency personnel, to include scores of DoD, civilian, and military personnel, visiting or assigned to our missions abroad. Further, she declared that, particularly in these difficult times, it's even more critical that we all have the tools we need to expeditiously ensure the security of all of our facilities, personnel, and information, and concluded that a huge part of all our jobs is to ensure that contractor personnel have the requisite security clearances before they are afforded access to classified information and facilities. This fact she described as leading to extreme confusion and frustration when one tries to explain why an agency like State, as well as the 30 other non-DoD agencies in the NISP, should find themselves restricted from direct access to JPAS, the system of record for verifying security clearances in the NISP. She further pointed out that, notwithstanding the occasional exception, all DoD components, as well as the over 13,000 contractors in the NISP, have JPAS access, whereas the 30 non-DoD user agencies do not. She acknowledged that the Defense Manpower Data Center's (DMDC) regulations state that JPAS accounts for non-DoD agencies "are issued by exception, due to the lack of insight into non-DoD subjects, employment, security clearances, or oversight," but she categorically fails to understand this premise, especially as the non-DoD agencies follow the same national standards as DoD components for processing clearances and hiring personnel. She pointed out that she and many others have offered time and time again to provide whatever information is needed to facilitate access to JPAS. In fact, she confirmed that two years ago she required all of her personnel complete all the training and follow all of the steps required in DMDC's JPAS account requests procedures manual, even including the required full explanation as to why OPM's CVS system does not meet operational needs. Nevertheless, DMDC, at the urging of OUSD(I) officials, refused to process the State Department request, although subsequently issued an interim waiver allowing State to continue to request JPAS person summaries from our contractors. We as a user agency, and one that has always taken as deeply seriously its role as a member of the NISPPAC and the Government Industrial Security Working Group, do not understand this restriction and have a difficult time in explaining to our senior officials why we are treated differently with regard to JPAS access and, by extension, how this could have direct and negative impacts on the security of our missions around the world. Given the issues that we have seen and worked time and time again, and as my staff has continued to review visit letters and JPAS person summaries from our contractors, we cannot continue to arbitrarily accept the limited information contained on visit letters submitted by our companies. Somehow we have to continue to verify that the information provided by our companies is accurate, as my office is ultimately responsible for ensuring that each and every contractor who comes to our facilities, and especially those at our embassies and consuls abroad, has the requisite personnel security clearance. Here she restated her concern that CVS could be useful as a tool for personnel security professionals, such as when verifying security clearances on an intermittent basis, but that it cannot serve as the ultimate tool for State's industrial security professionals, as they work diligently to verify the clearance and investigations status of over 25,000 contractor personnel on a yearly basis. Though there have been some improvements to CVS over the past few years, such as with the addition of cage codes, she challenges OPM, when examining the long term, to describe how its system could be made more user friendly and less onerous to non-DoD agencies, especially as continued denial of access to JPAS severely inhibits all attempts to complete security-related tasks effectively and

efficiently. Also, continuing to rely on CVS versus JPAS for verification of the current status of contractor clearances triples processing times required for the review and approval of over 2,000 visit letters per month, which in turn results in significant delays to both domestic and overseas contract performance and equates to thousands of additional man-hour expenditures. Therefore, her request at this forum, is to ask DoD if there is any possible way that an exception might be granted for access to JPAS, so that State's industrial and personnel security professionals can be brought more in line with DoD and contractor security professionals. To that end, she would welcome a dialogue, as would perhaps many non-DoD agency personnel, with DoD officials, so that this issue might be resolved rather than alternatively raising it directly to senior State officials.

At the conclusion of Ms. Baugher's comments, no additional items were raised.

VI. Closing Remarks and Adjournment:

The Chair thanked everyone for their attendance at today's meeting, and confirmed that the next meeting of the NISPPAC is scheduled for Monday, June 6th, 2016, from 2:00 to 4:30 p.m. at the Gaylord Hotel in Nashville, TN, and is to be held in conjunction with the National Classification Management Society's annual conference. The Chair adjourned the meeting at 12:12 p.m.

Attachments:

(1) NISPPAC Attendance List, April 14, 2016
(2) NISPPAC Action Items, April 14, 2016
(3) DSS Cost Collection Survey
(4) Industry Update
(5) C&A Working Group Update
(6) OPM Update
(7) ODNI Update
(8) DoD CAF Update
(9) DOE Personnel Security Performance Metrics
(10)NRC Personnel Security Performance Metrics

Attachment #1

NISPPAC MEETING ATTENDEES

The following individuals attended the April 14, 2014, NISPPAC meeting:

• William Cira	Information Security Oversight Office	Acting Chair
• Greg Pannoni	Information Security Oversight Office	Designated Federal Official
• Beth Cobert	Office of Personnel Management	Attendee/Presenter
• Richard Hale	Department of Defense	Attendee/Presenter
• James Onusko	Office of Personnel Management	Attendee/Presenter
• Christy Wilder	Office of Personnel Management	Attendee/Presenter
• Patrick Viscuso	Information Security Oversight Office	Attendee/Presenter
• Greg Torres	Department of Defense	Alternate/Presenter
• Tony Ingenito	Industry	Member/Presenter
• Tracy Brown	Defense Security Service	Attendee/Presenter
• Donna McLeod	Office of Personnel Management	Observer/Presenter
• Gary Novotny	Office of the Director of National Intelligence	Attendee/Presenter
• Daniel Purtill	Department of Defense	Attendee/Presenter
• Steve Lanz	Department of the Air Force	Attendee
• Lisa Desmond	Department of the Army	Attendee
• George Ladner	Central Intelligence Agency	Alternate
• Kisha Braxton	Department of Commerce	Attendee
• Ben Richardson	Department of Defense	Attendee
• Fred Gortler	Defense Security Service	Member
• Keith Minard	Defense Security Service	Alternate
• Carl Piechowski	Department of Energy	Attendee
• Michael Bodin	Department of Energy	Attendee
• Scott Ackiss	Department of Homeland Security	Member
• Anthony Smith	Department of Homeland Security	Alternate
• Anna Harrison	Department of Justice	Member
• Dennis Hanratty	National Security Agency	Member
• Jeffrey Bearor	Department of the Navy	Member
• Denis Brady	Nuclear Regulatory Commission	Member
• Kimberly Baugher	Department of State	Member
• David Morrison	Office of the Director of National Intelligence	Attendee
• Shirley Brown	National Security Agency	Attendee
• J. C. Dodson	Industry	Member
• Dennis Keith	Industry	Member
• Phillip Robinson	Industry	Member
• Michelle Sutphin	Industry	Member
• Quinton Wilkes	Industry	Member
• Daniel McGarvey	MOU Representative	Attendee
• Mitch Lawrence	MOU Representative	Attendee
• Kirk Poulsen	MOU Representative	Attendee
• Heather Green	Defense Security Service	Attendee
• Doug Pulzone	Defense Security Service	Attendee

•	Justin Walsh	Defense Security Service	Attendee
•	Preston Harper	Defense Security Service	Attendee
•	Elizabeth Farr	Department of Defense	Attendee
•	Stephen Lewis	Industry	Attendee
•	Charlie Sowell	Industry	Attendee
•	Steven Kipp	Industry	Attendee
•	Nissa Kunkel	Industry	Attendee
•	Vincent Jarvie	Industry	Attendee
•	David Wennergren	Industry	Attendee
•	Noel Matchett	Industry	Attendee
•	Erin Bruce	Industry	Attendee
•	Dorothy Rader	Industry	Attendee
•	Rick Ohlemacher	Industry	Attendee
•	Norm Pashoian	Industry	Attendee
•	Leonard Moss	Industry	Attendee
•	Mary Edington	Industry	Attendee
•	Kathy Branch	Information Security Oversight Office	Staff
•	Robert Tringali	Information Security Oversight Office	Staff

Attachment #2

Action Items from NISPPAC Meeting, 20160417

1) DSS will post current information on their website pertaining to the backlog of cases pending at PSMO-I.

2) Industry and DSS will meet to review the current DSS cost collection methodology in order to determine if the methodology is still reasonable for its intended use.

3) ISOO will establish an ad hoc NISPPAC Insider Threat Working Group.

Attachment #3

Annual Security Cost Collection Survey

Purpose

Capture security costs incurred by contractor facilities in connection with implementation of the NISP

Regulation / Requirement

32 CFR, Subpart F, section 2001.61 (b); Classified National Security Information; Final Rule, requires the Secretary of Defense, acting as executive agent for the NISP, to collect cost estimates for classification-related activities of contractors, licensees, certificate holders, and grantees and report them to the Information Security Oversight Office (ISOO)

Survey process in place since 1996; transferred to DSS in 2008

Survey methodology approved by ISOO; DSS received OMB approval for Collection of Data in December 2008

	FY15	FY14	FY13	FY12	FY11	FY10	FY09
NISP Cost Estimate	$1.27B	$1.13B	$1.07B	$1.19B	$1.26B	$1.25B	$1.12B

Attachment #4

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

Industry

16 March 2016

Outline

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

National Industrial Security Program

Policy Advisory Committee Industry Members

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

National Industrial Security Program

Industry MOU Members

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

National Industrial Security Program

Policy Advisory Committee

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

OPM Data Breach

- IMPACT
  - Significant delays in BI process directly impacting contract performance (SCI/SAP efforts)
  - Increase to existing clearance backlog due to the shutdown
- National Background Investigations Bureau (NBIB)
  - Federal Investigative Services (FIS) transition to NBIB.
    - What will be the transition plan?
    - Impact to the current lagging investigative process?
- Next Step
  - Working thru the backlog. What is the "Get Well Plan"?
  - Planned hire of 200 Investigators in 2016. Slow pace of hiring and training not expected to have impact on growing backlog.
  - NISPPAC involvement to ensure consistent agency actions.
  - Interim policy guidance to address:
    - Interim Clearances and Out of Scope BIs. ODNI Memo to Components (similar to 2006 letter)
    - CAC Suitability (NACI) .

Security Policy Update

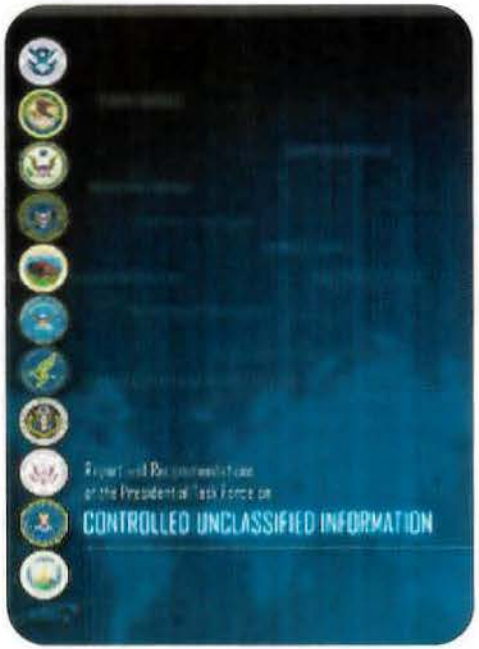
Executive Order #13556

EO # 13556

Controlled Unclassified Information (CUI)

4 NOV 2010

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



- Next Steps
  - (NIST Special Publication 800-171) Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations published June 2015.
    - Currently included in contract clause from some user agencies.
    - Does not allow for risk based tailoring
    - Fails to address non applicability of requirements due to the use of compensating controls
    - No mechanism to address inefficiencies due to conflicting guidance.
    - Challenges for small contractors to implement (cost and lack of staff).
  - Status of CUI Proposed Rule (32 CFR 2002)?
  - ISSO working with FAR Council on specific CUI clause.
    - Awaiting opportunity to review draft clause.

Security Policy Update

Executive Order #13587

EO # 13587

Structural Reforms to improve security of classified networks

7 OCT 2011

Office of Management and Budget and National Security Staff - Co-Chairs

- Steering Committee comprised of Dept. of State, Defense, Justice, Energy, Homeland Security, Office of the Director of National Intelligence, Central Intelligence Agency, and the Information Security Oversight Office

INSIDER THREAT

- Directing structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks
  - Integrating InfoSec, Personnel Security and System Security
- Need consistent requirement across all the User Agencies relating to implementation SOPs.
- Monitoring separate policy/directive actions across the USG and providing input where possible.
  - Fractured implementation guidance being received via agency/command levels.
  - Awaiting release of NISPOM Conforming Change # 2 and DSS ISL. Continues to be of high interest; particularly as it affects timeline expectations for implementation, assessments and scaling of programs across entirety of DIB.
  - Healthy interchange between USG and industry to get this right while we wait for OSD/GC action.
  - Customers already asking industry to describe their Insider Threat programs

Security Policy Update

Executive Order #13691

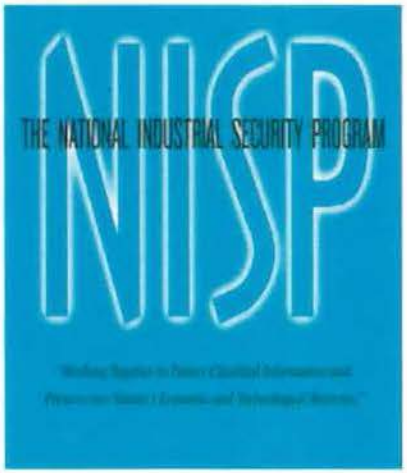
EO # 13691

Promoting Private Sector Cybersecurity Information Sharing

13 February 2015

Department of Homeland Security

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

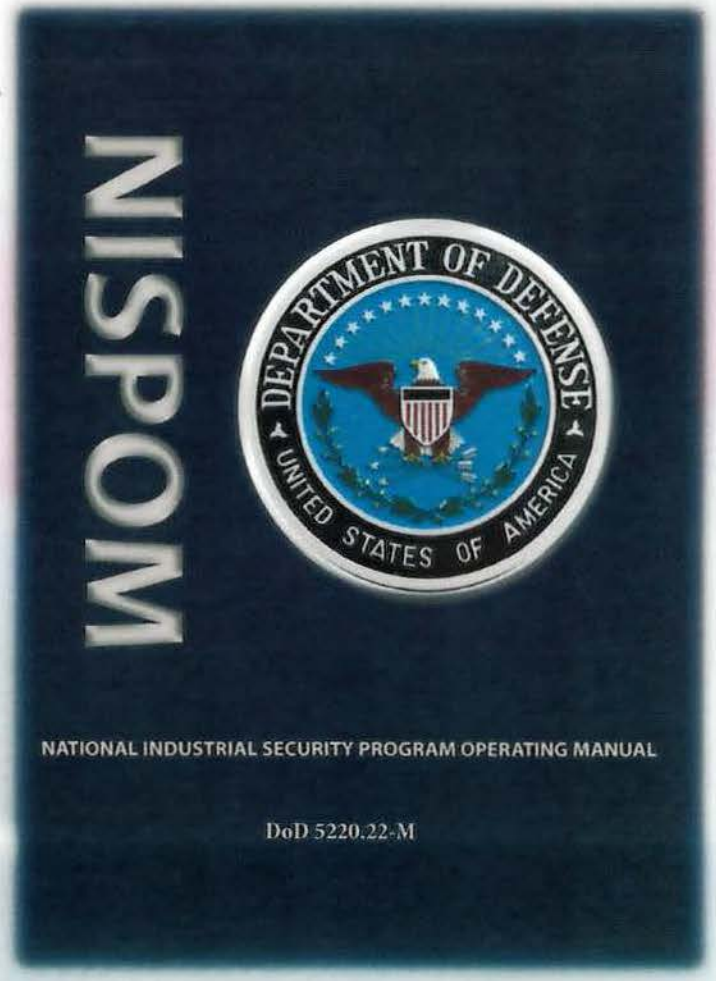


- Amends the National Industrial Security Program (EO 12829)
  - Inserts the Intelligence Reform and Terrorism Prevention Act of 2004.
  - Adds the Secretary of Homeland Security as a cognizant security agency.
    - Drafting NISPOM enclosure addressing Critical Infrastructure Program
- Meeting with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

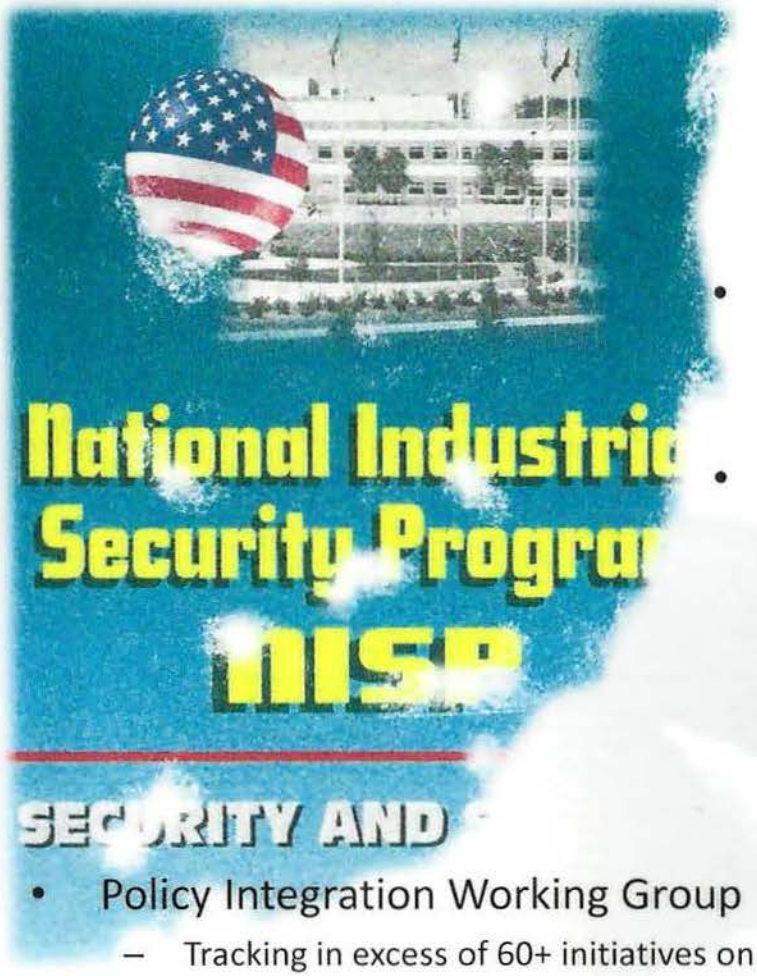
Security Policy Update

Industrial Security Policy Modernization

- National Industrial Security Program Operating Manual revision and update
  - Industry provided comments on draft Jun/July 2010
  - NISPOM Re-Write WG : Gov/Industry team completed review of all buckets. Draft converted to new USG policy format. Next step for CSA's to review updated draft.
  - Awaiting conforming change #2 release.
  - OUSDI, DSS & Industry collaborating on Insider Threat ISL. Concern that ISL could take near 180 days to publish after CC # 2 hits the street.
- Department of Defense Special Access Program Manual development
  - Vol 1 (General procedures) Published
  - Vol 2 (Personnel Security) Published
  - Vol 3 (Physical Sec) Published
  - Vol 4 (Classified Info Marking) Published
  - Eliminates JFAN and NISPPOM SAP Supplement upon publication of all the above.
  - AF SAPCO officially rescinds JFAN 6/9 and citing in DD254's
- IMPACT
  - Industry working under a series of interim directions
  - Strong industry coordination for this interim direction is inconsistent
  - Delay of single, integrated policy is leading to differing interpretation of interim direction by user agencies



Policy Integration Issues



- National & world events have stimulated reactions for policy changes and enhanced directives to counter potential vulnerabilities
  - Key areas include Cyber Security, Insider Threat and PERSEC
- 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. Not flowing changes thru contract channels.
  - Need to process tactically 1st before becoming procedural.

- Policy Integration Working Group
  - Tracking in excess of 60+ initiatives on the policy tracking matrix. Intend to review interdependencies between the policy initiatives.
  - Process update for vetted & validation thru MOU to NISPPAC to USG counterparts. Identifying cost and impacts.
  - Intent that during the formulation stage, the impact and assumptions within Industry are considered.

National Industrial Security Program

Policy Advisory Committee Working Groups

- Personnel Security
  - Working group moving out to address areas of concern.
    - E-adjudication business rules being aligned with new Federal Investigative Standards. New FIS expected to produce an decreased in e-adjudication across the board.
    - DOHA SOR Process. Definitively ID true caseload and aging of those cases. Consider adding WHS representation since DOHA & CAF align under them.
    - Interim Clearance impacts due to FBI Fingerprint backlog (2 days to 6 wks)
    - Fingerprint backlog also impacting CAC issuance due to FP credentialing requirement.
    - Expecting backlog to continue growing based on OPM Breach, new FIS and DSS change to 90 day PR clearance initiation process.
- Automated Information System Certification and Accreditation
  - Working group focus is on incorporating the Risk Management Framework (RMF) into future process manual updates. Early collaboration on this initiative will be key to successful transition. Positive interactions in the multiple meetings.
  - Industry has identified 7 participants (large and small companies) to participate in DSS RMF beta test.

National Industrial Security Program

Policy Advisory Committee Working Groups (cont.)

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

Attachment #5

Defense Security Service

RISK MANAGEMENT FRAMEWORK (RMF) FOR NISP CONTRACTORS

April 2016

What Is Risk Management Framework (RMF)

- RMF is a key component of an information security program used in the overall management of organizational risk to individuals, assets and information

- It is a unified information security framework for the entire federal government that replaces legacy Certification and Accreditation (C&A) Processes applied to information systems

Benefits of RMF

- Utilizes common terms & security principles throughout the system development lifecycle
- Reciprocal approach allows for greater interconnectivity between systems & agencies
- Promotes structured yet flexible approach for managing organizational risk associated with the operation of information systems
- Facilitates prioritization of security requirements and allocation of IS security resources

Key RMF Policy References

NIST

- SP 800-37
- SP 800-53
- SP 800-53A

CNSS

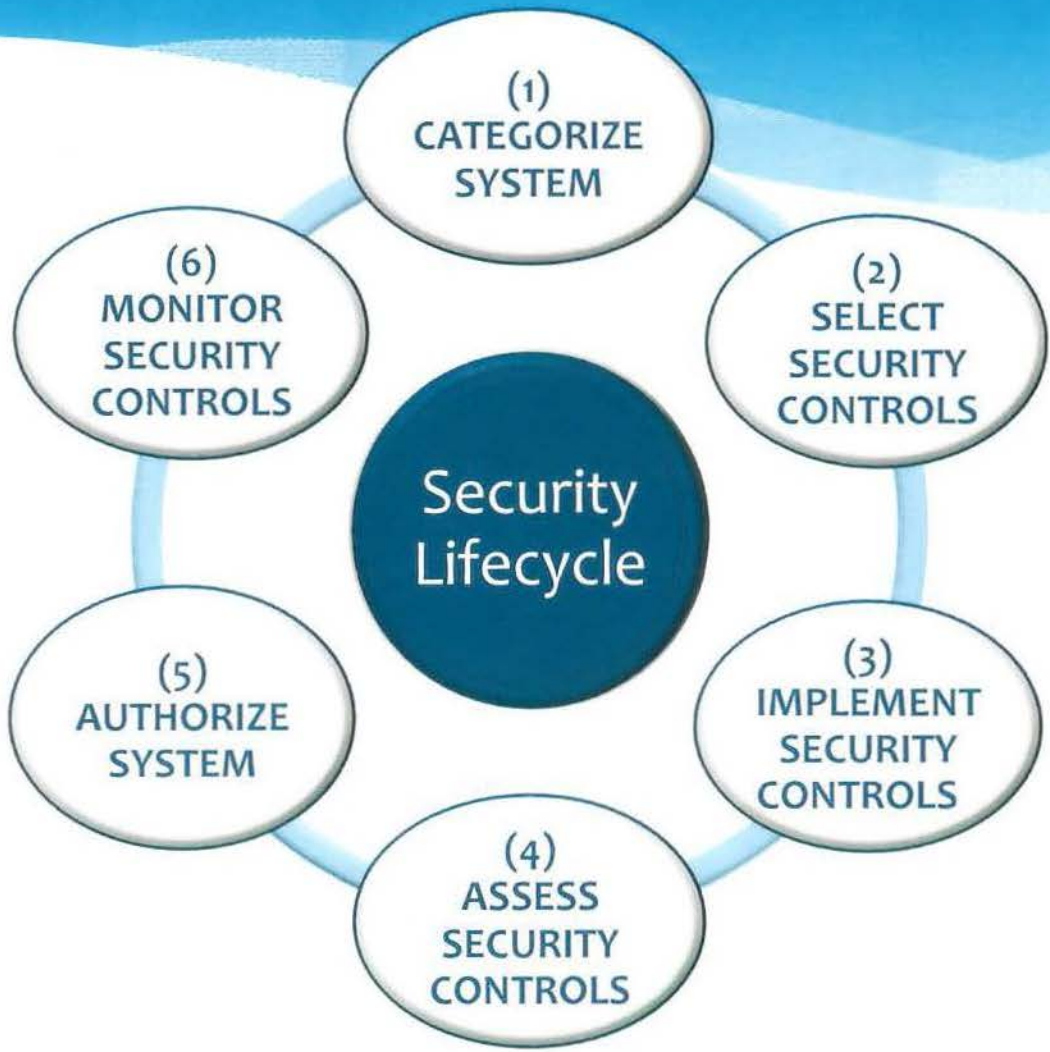
- CNSSP 22
- CNSSD 504
- CNNSI 1253
- CNSSI 4009

NISP

- DoD 5220.22-M (Change 2)

Risk Management Framework

Six-Step Process



Transition Timeline

System Accreditation Status	Transition Timeline / Instructions
SSP submitted prior to 1 August 2016	Cleared contractors continue using current Certification & Accreditation process with the latest version of the ODAA Process Manual. ATO will be no greater than 18 months starting August 1, 2016. Within 6 months of authorization, develop a POA&M for transition to RMF.
Stand-Alone Systems after 1 August 2016	Execute RMF Assessment and Authorization through the use of the DSS Assessment and Authorization Process Manual (DAAPM).

Transition Timeline Cont.

System Accreditation Status	Transition Timeline / Instructions
Local Area Network, Wide Area Network or Interconnected System between August 1, 2016 – 28 February 2017	Cleared contractors continue using the current Certification & Accreditation process with the latest version of the ODAA Process Manual. ATO will be no greater than 18 months starting August 1, 2016. Within 6 months of authorization, develop a POA&M for transition to RMF.
Local Area Network, Wide Area Network or Interconnected System after 1 March 2017.	Execute RMF Assessment and Authorization process through the use of the DSS Assessment and Authorization Process Manual (DAAPM).

RMF Training Provided by CDSE

Introduction to RMF (CS124.16)

Continuous Monitoring (CS200.16)

Categorization of the System (CS102.16)

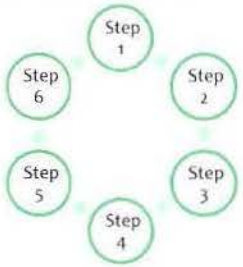
Selecting Security Controls (CS103.16)

Implementing Security Controls (CS104.16)

Assessing Security Controls (CS105.16)

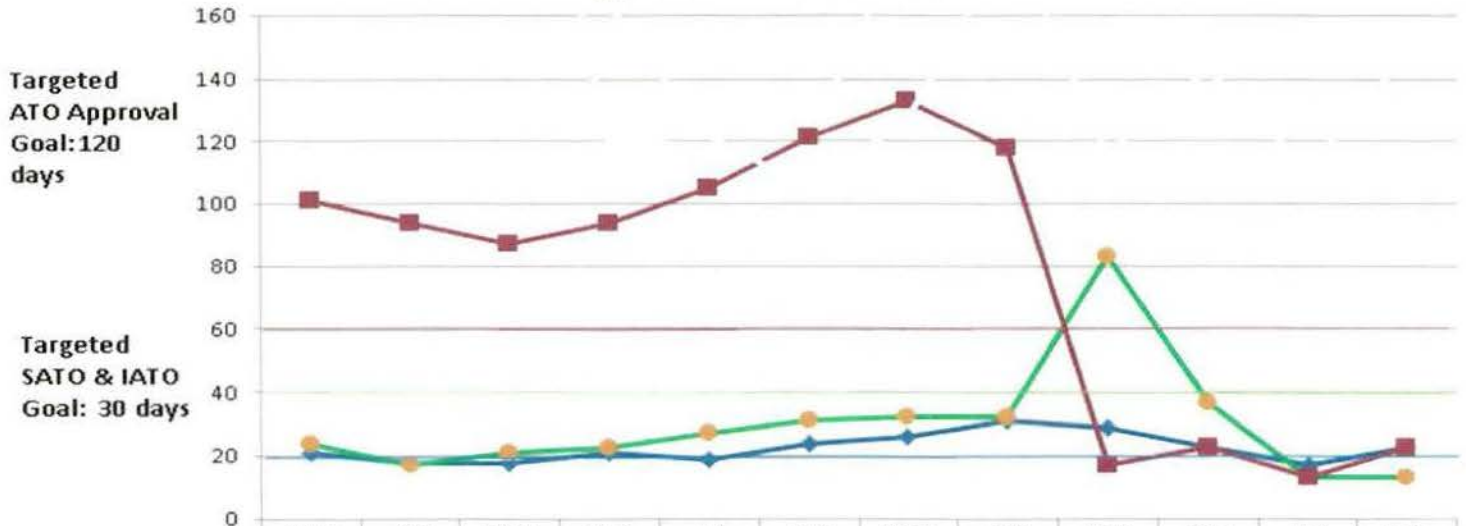
Authorizing Systems (CS106-16)

Monitoring Security controls (CS107.16)



BACKUP SLIDE

ODAA Approval Timeliness



	Mar	Apr	May	June	Jul	Aug	Sept	Oct	Nov	Dec	Jan	Feb
IATO Timeliness	21	18	18	21	19	24	26	31	29	23	17	23
IATO Amount	213	204	270	120	122	121	185	189	116	143	111	148
SATO Timeliness	24	17	21	23	27	31	32	32	83	37	13	13
SATO Amount	148	128	121	120	88	116	122	150	30	36	36	36
ATO Timeliness	101	94	87	94	105	121	133	118	17	23	13	23
Reg ATO Amount	212	191	187	164	122	105	127	181	215	253	193	219

Attachment #6

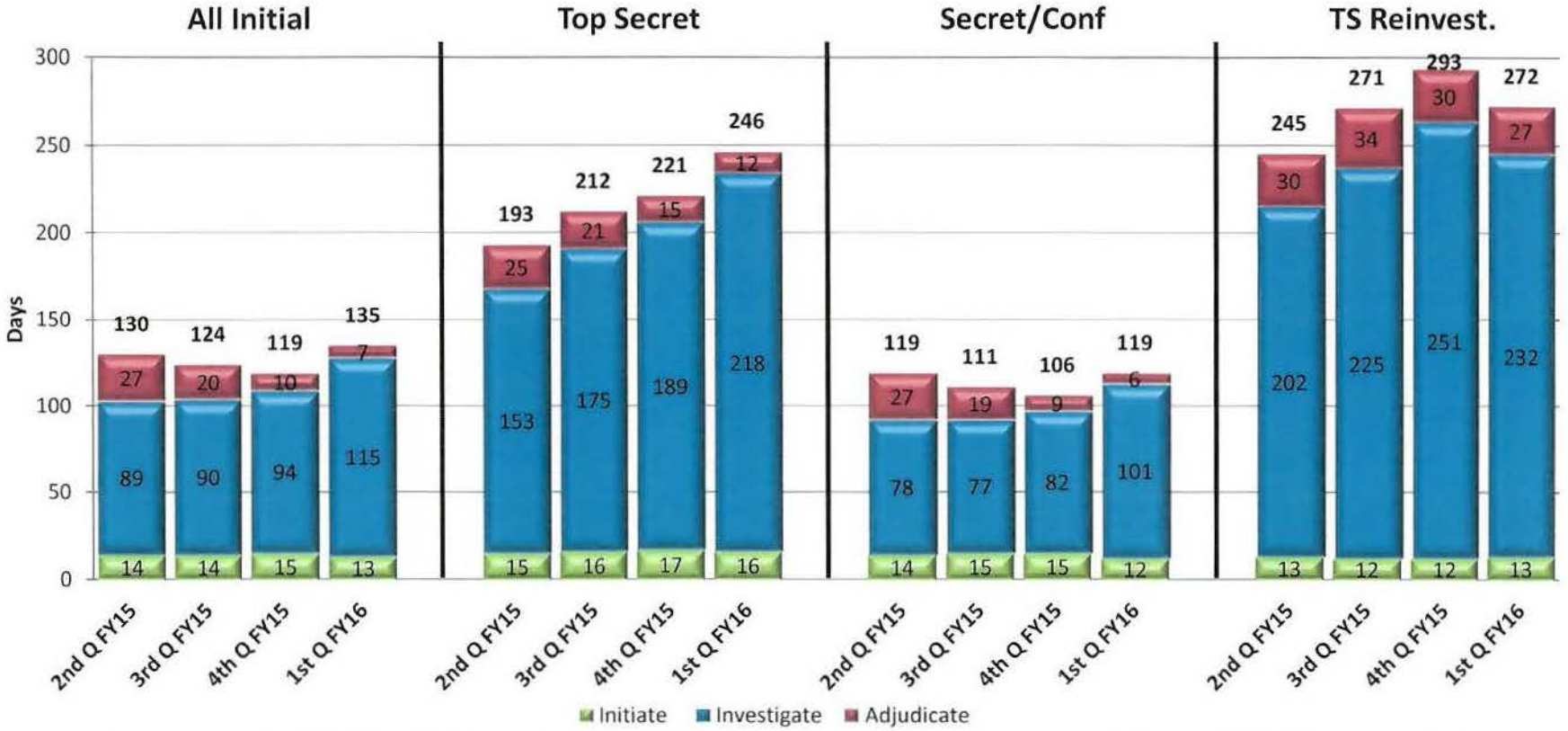
Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

DoD-Industry

March 2016

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

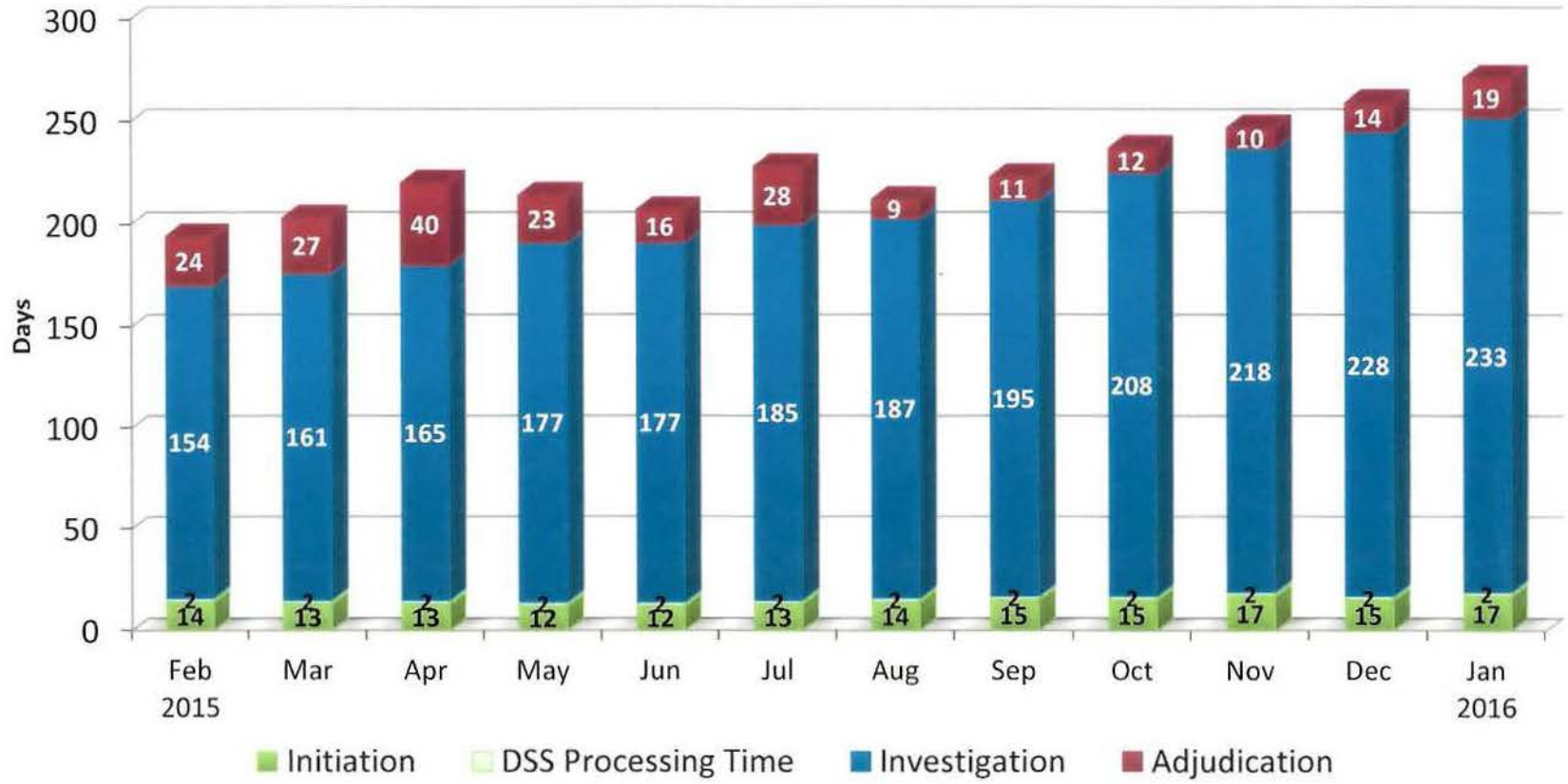
Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 2nd Q FY15	18,870	2,984	15,886	7,518
Adjudication actions taken – 3rd Q FY15	20,791	2,906	17,885	7,299
Adjudication actions taken – 4th Q FY15	21,047	2,597	18,450	7,357
Adjudication actions taken – 1st Q FY16	16,262	2,125	14,137	7,459

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

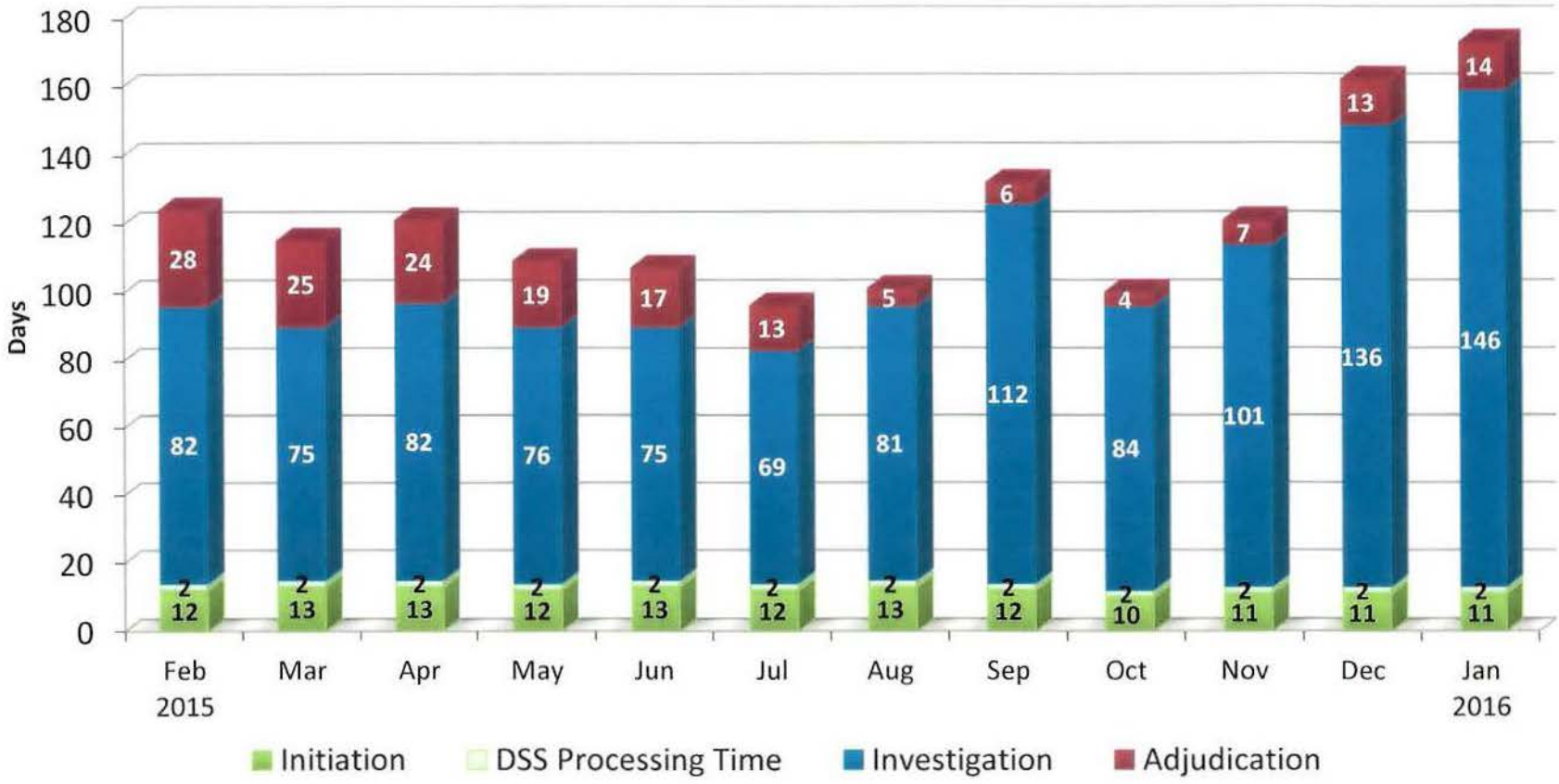
Industry's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



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

	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015	Oct 2015	Nov 2015	Dec 2015	Jan 2016
100% of Reported Adjudications	988	954	817	966	1,128	838	911	868	795	646	699	581
Average Days for fastest 90%	194 days	203 days	220 days	214 days	207 days	228 days	212 days	223 days	237 days	247 days	259 days	271 days

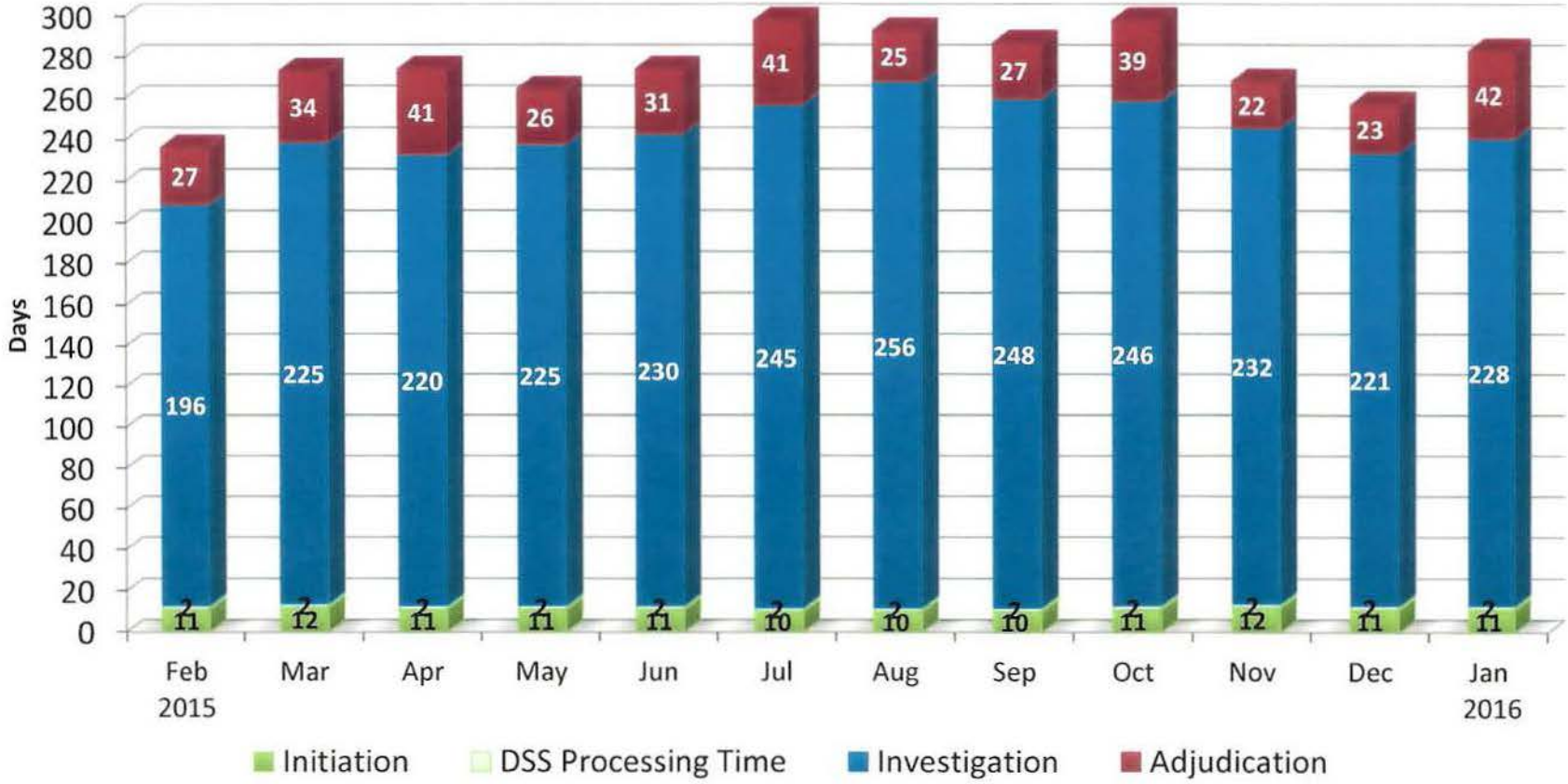
Industry's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions (NACLC/T3)



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

	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015	Oct 2015	Nov 2015	Dec 2015	Jan 2016
100% of Reported Adjudications	4,916	5,620	5,002	5,287	7,602	9,052	5,131	4,272	6,718	4,046	3,430	3,634
Average Days for fastest 90%	124 days	115 days	121 days	109 days	107 days	96 days	101 days	132 days	100 days	121 days	162 days	173 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 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015	Oct 2015	Nov 2015	Dec 2015	Jan 2016
100% of Reported Adjudications	2,442	2,745	2,597	1,985	2,688	2,233	2,596	2,548	2,266	2,479	2,753	2,221
Average Days for fastest 90%	236 days	273 days	274 days	264 days	274 days	298 days	293 days	287 days	298 days	268 days	257 days	283 days

Attachment #7

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Industry Performance Metrics

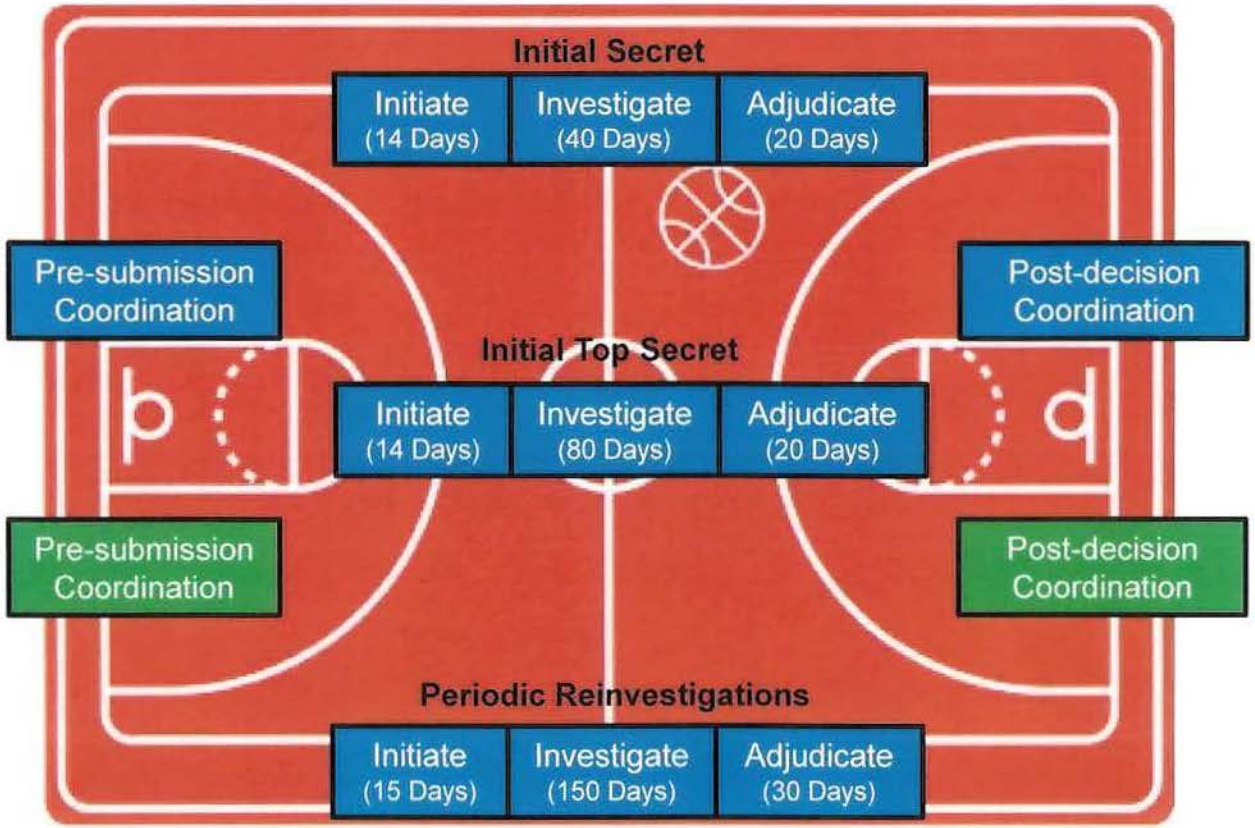
NCSC/Special Security Directorate

LEADING INTELLIGENCE INTEGRATION

16 March 2016

Performance Accountability Council (PAC) Security Clearance Methodology

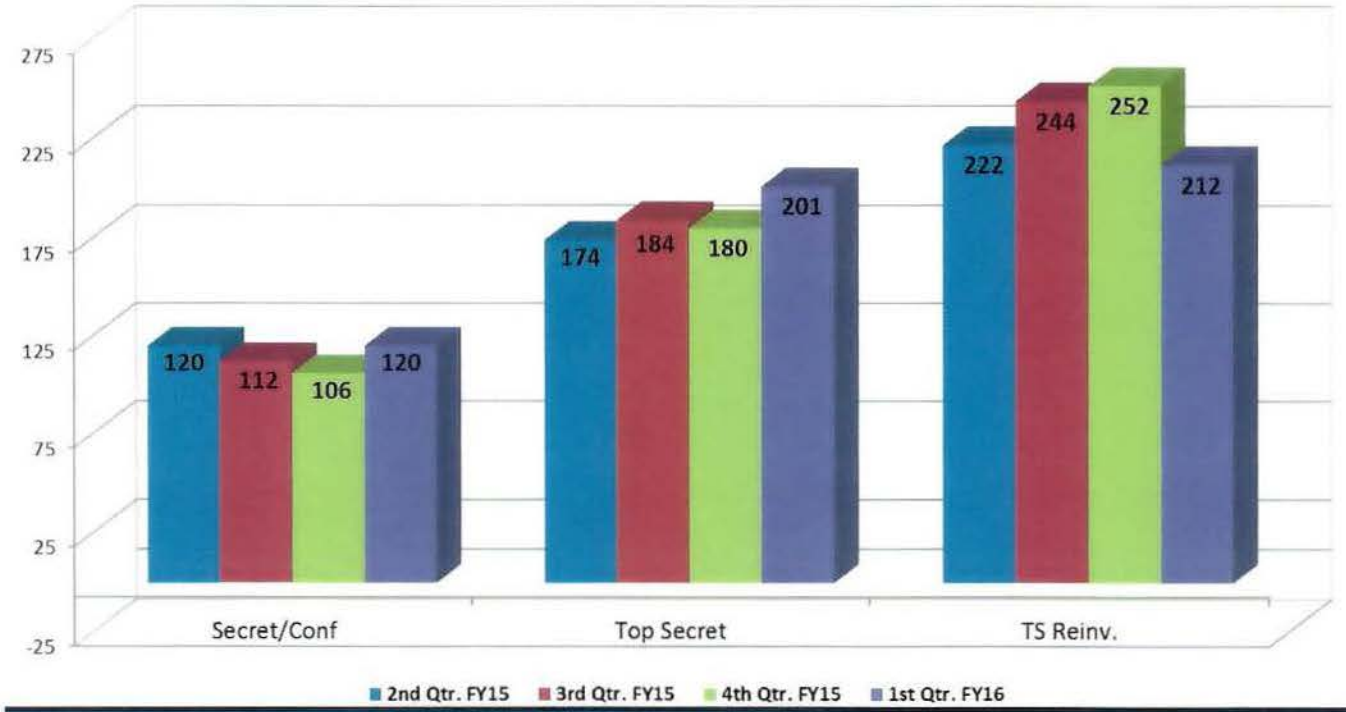
- Data on the following slides reflects security clearance timeliness performance on Contractor cases. DoD Industry data is provided by OPM and IC Contractor data is provided by the following IC agencies: CIA, DIA, FBI, NGA, NRO, NSA and Dept. of State.
- Timeliness data is being provided to report how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



Timeliness Performance Metrics for IC/DSS

Industry Personnel Submission, Investigation & Adjudication* Time

Average Days of Fastest 90% of Reported Clearance Decisions Made

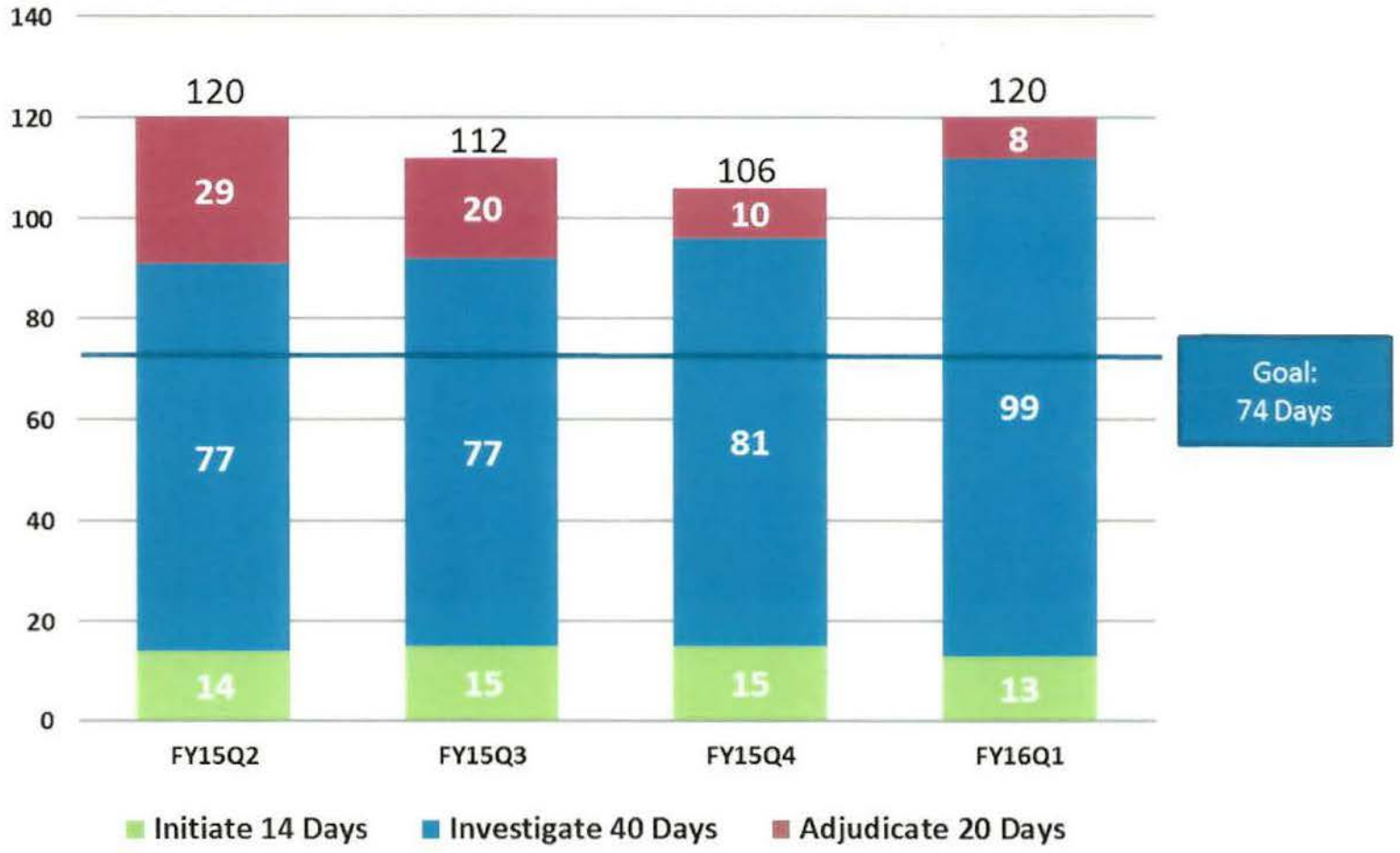


	Secret/ Confidential	Top Secret	Top Secret Reinvestigations
Adjudication actions taken – 2nd Q FY15	17,938	4,628	9,652
Adjudication actions taken – 3rd Q FY15	20,165	4,473	8,827
Adjudication actions taken – 4th Q FY15	19,007	4,436	10,519
Adjudication actions taken – 1st Q FY16	14,776	3,624	12,315

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

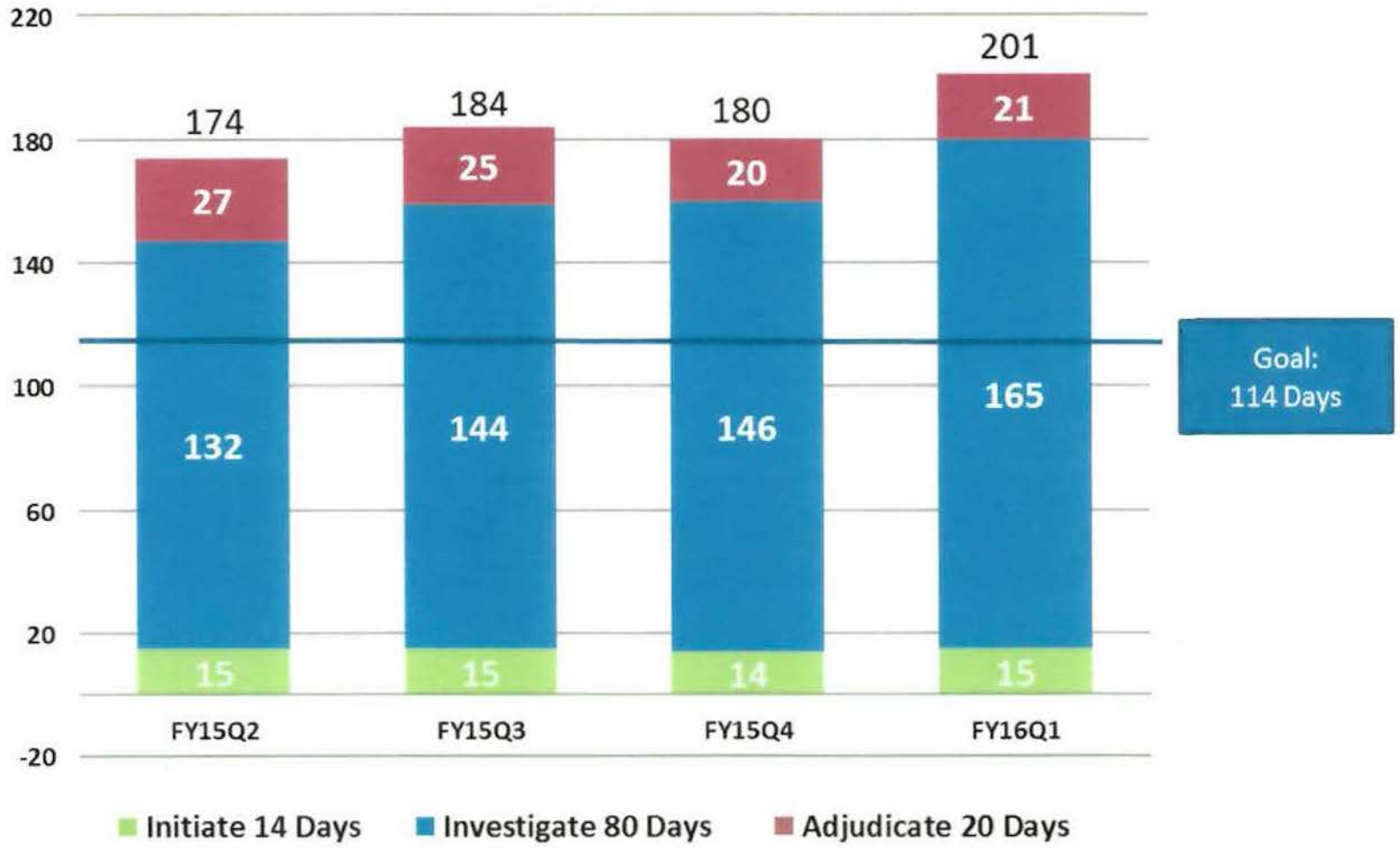
IC and DoD Industry – Secret Clearances

Average Days of Fastest 90% of Reported Clearance Decisions Made

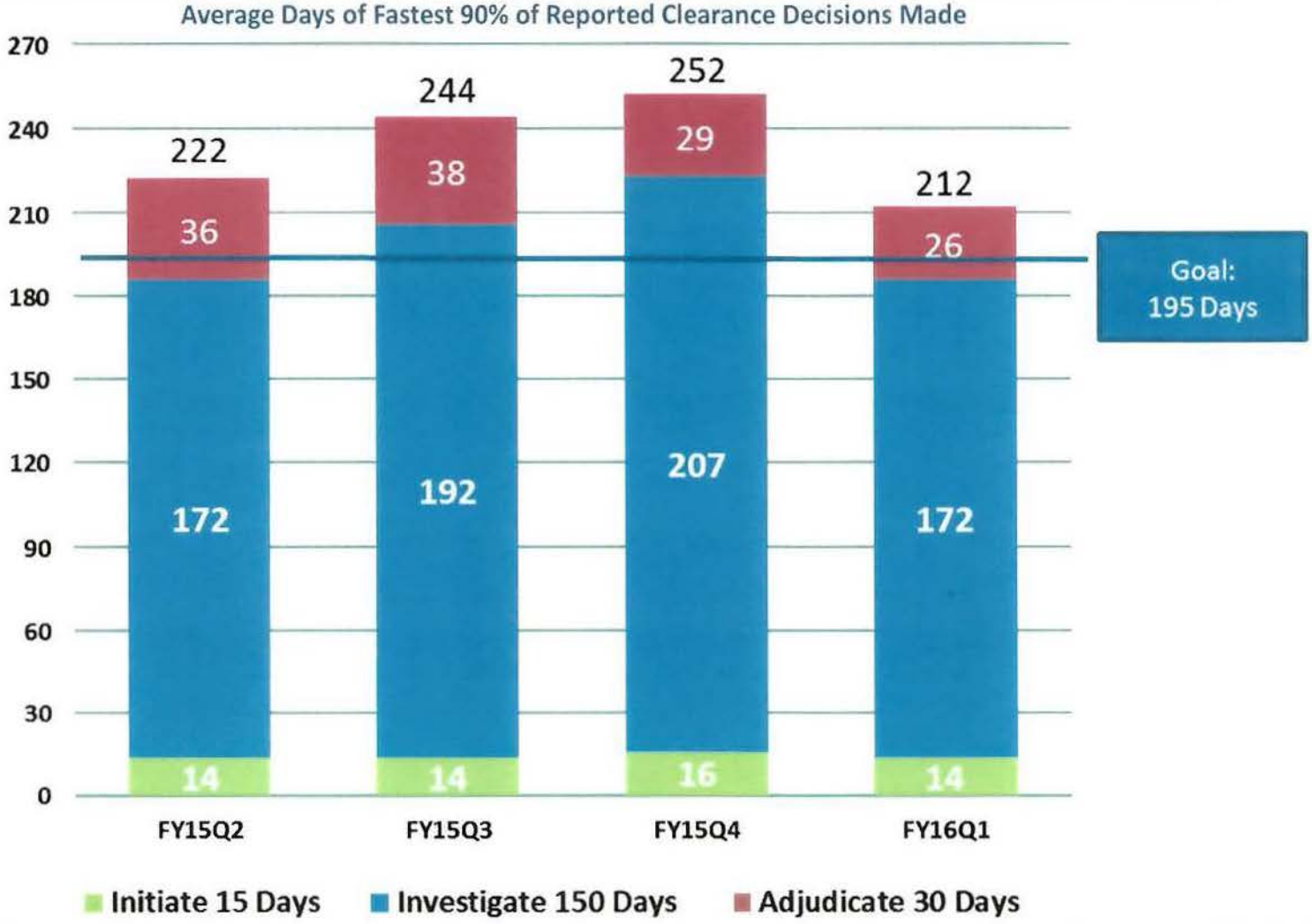


IC and DoD Industry - Top Secret Clearances

Average Days of Fastest 90% of Reported Clearance Decisions Made



IC and DoD Industry - Periodic Reinvestigations



ODNI Updates

- Quality Assessment Standards Implementation Plan
- Quality Assessment Reporting Tool
- Minimum Mandatory Reporting Requirements for Cleared Population
- Social Media Policy

For questions, please contact:

Gary Novotny
NCSC/SSD/PSG
Assessments Program Manager
Phone: 301-243-0474
Email: Garymn@dni.gov

Nilda Figueroa
NCSC/SSD/PSG
Metrics Team Lead
Phone: 301-243-0462
Email: Nilda.Figueroa@dni.gov

Diane Rinaldo
Metrics Team
Phone: 301-243-0464
Email: SecEAmetrics@dni.gov

Attachment #8

DEPARTMENT OF DEFENSE
CONSOLIDATED ADJUDICATIONS FACILITY

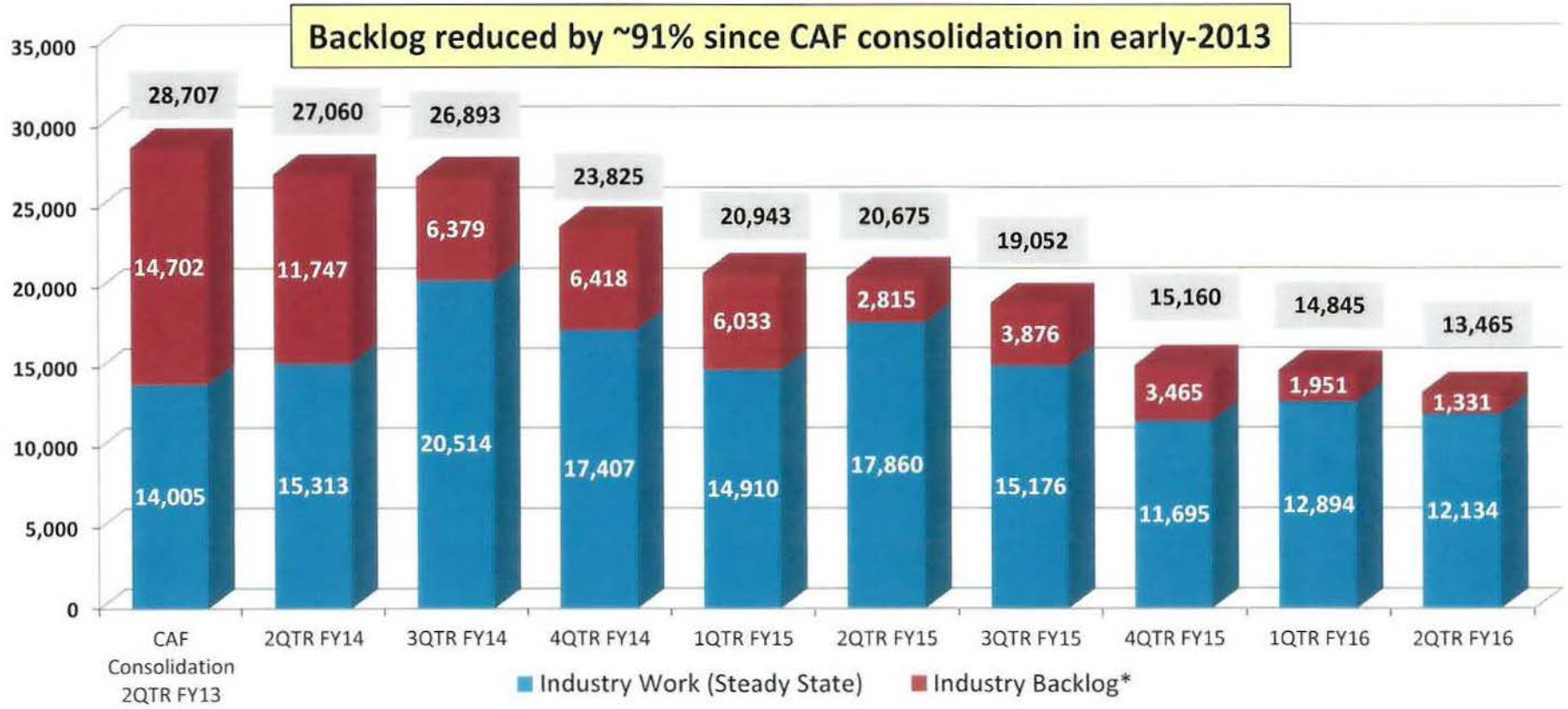
April 2016

PCL WORKING GROUP

Industrial Cases Pending Adjudication

Includes cases Undergoing Legal Sufficiency Review at DOHA

Backlog reduced by ~91% since CAF consolidation in early-2013



- **Backlog to be eliminated not earlier than late-FY16**
- **Potential Complications Remain:**
  - + **CATs v4 Deployment to reduce production by ~20% (Jun 16 - Jan 17)**
  - + **Full impact of CE implementation not yet realized**
  - + **FY16-18 – New FIS to both increase workload and reduce e-Adjudication**
  - + **Loss of e-Adj. in FY16 resulted in an increase of ~3,100 (+3%)**

Month	NISP Backlog	FY 15 NISP Receipt*	Backlog % of Total NISP
October 13	13,515		7.4%
March 16	1,331		0.7%
	-12,184	~ 183,000	

*Includes Personal Security Investigations, Incident Reports, Reconsiderations, etc. (does not include SACs)

Industry
Intelligence Reform and Terrorism Prevention Act Performance FY14-FY16 to Date

- FY 15 - Both NISP and non-NISP timeliness metrics fluctuated as backlogs were addressed
- FY 16 - Timelines to remain more stable, and within IRTPA mandates, as last vestiges of "old"/backlog cases are closed
- Increase in Initial and PR timeliness in 2nd Qtr FY 16 due to an emphasis on closing backlogged DOHA and suspense cases as well as OPM conversions of REO requests to RSI, IT issues, loss of e-adj, and high incoming volume. 23% of the PRs and Initials closed during February were "old"/backlog cases.

DoD CAF
Bldg. 600, 10th Street, FGGM

Attachment #9

Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

DOE

March 2016

Quarterly Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made

	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 2nd Q FY15	1,474	527	947	1,488
Adjudication actions taken – 3rd Q FY15	1,706	662	1,044	1,994
Adjudication actions taken – 4th Q FY15	1,768	698	1,070	2,153
Adjudication actions taken – 1st Q FY16	1,569	649	920	2,198

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

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

	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015	Oct 2015	Nov 2015	Dec 2015	Jan 2016
100% of Reported Adjudications	163	205	206	238	203	211	263	212	233	178	228	171
Average Days for fastest 90%	151 days	160 days	168 days	181 days	178 days	167 days	179 days	190 days	207 days	232 days	204 days	198 days

DOE's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions (NACLC/ANACI/T3)

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

	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015	Oct 2015	Nov 2015	Dec 2015	Jan 2016
100% of Reported Adjudications	248	391	254	397	356	523	301	219	355	249	278	183
Average Days for fastest 90%	83 days	88 days	92 days	99 days	103 days	104 days	123 days	140 days	123 days	112 days	124 days	145 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 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015	Oct 2015	Nov 2015	Dec 2015	Jan 2016
100% of Reported Adjudications	464	538	588	669	724	642	676	805	617	726	844	546
Average Days for fastest 90%	168 days	192 days	188 days	195 days	197 days	206 days	205 days	210 days	226 days	228 days	241 days	215 days

Attachment #10

Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

NRC

March 2016

Quarterly Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made

	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 2nd Q FY15	118	9	109	23
Adjudication actions taken – 3rd Q FY15	158	12	146	25
Adjudication actions taken – 4th Q FY15	147	18	129	37
Adjudication actions taken – 1tst Q FY16	108	12	96	17

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

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

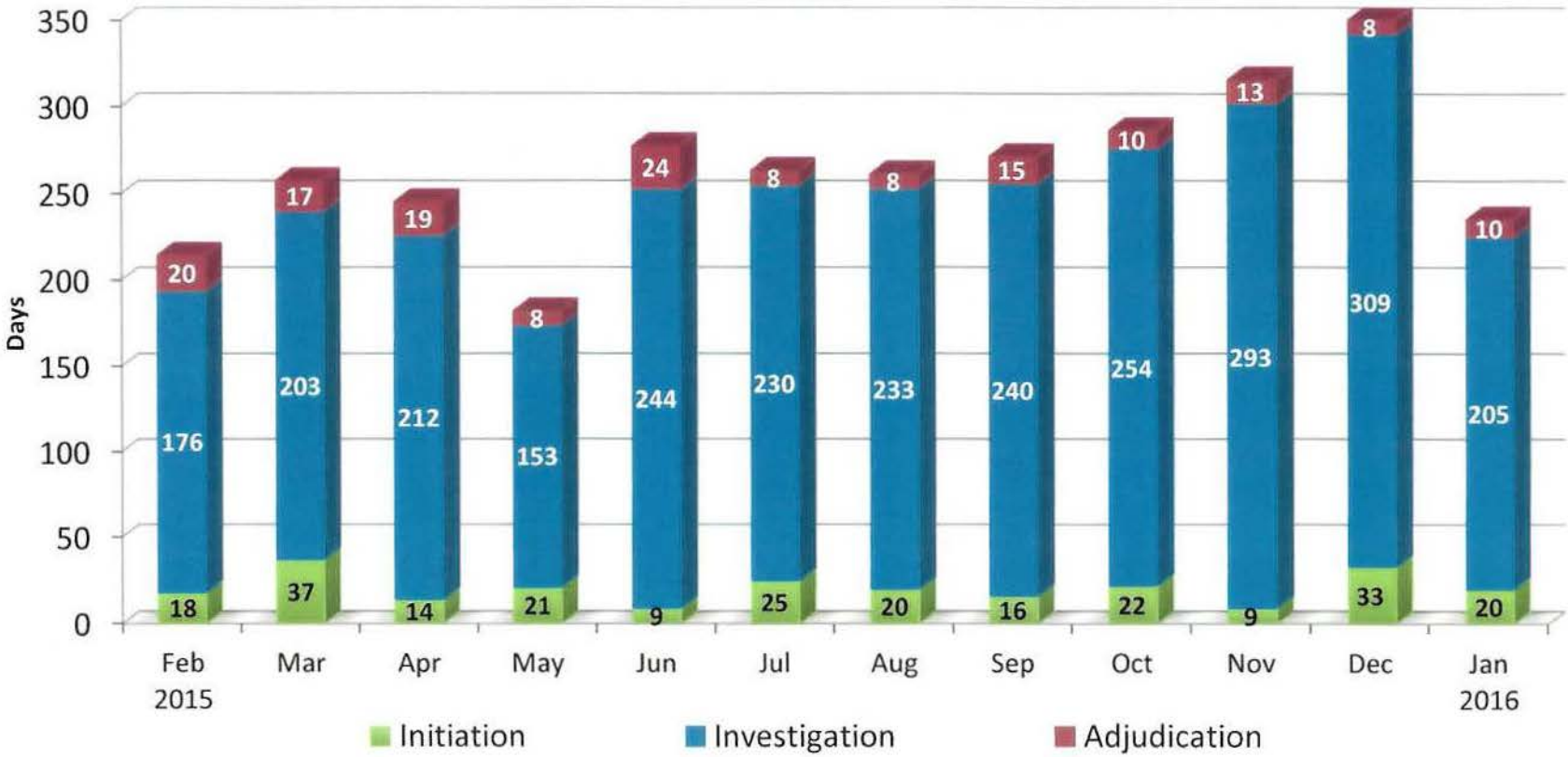
	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015	Oct 2015	Nov 2015	Dec 2015	Jan 2016
100% of Reported Adjudications	4	3	6	3	3	7	7	4	5	4	3	1
Average Days for fastest 90%	209 days	220 days	242 days	163 days	196 days	219 days	173 days	244 days	224 days	270 days	268 days	403 days

NRC's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions (NACLC/ANACI/T3)

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

	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015	Oct 2015	Nov 2015	Dec 2015	Jan 2016
100% of Reported Adjudications	39	41	31	60	55	57	39	34	38	28	31	18
Average Days for fastest 90%	141 days	115 days	124 days	130 days	117 days	120 days	152 days	204 days	182 days	212 days	194 days	190 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 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015	Oct 2015	Nov 2015	Dec 2015	Jan 2016
100% of Reported Adjudications	7	8	12	9	4	10	18	10	4	2	10	12
Average Days for fastest 90%	214 days	257 days	245 days	182 days	277 days	263 days	261 days	271 days	286 days	315 days	350 days	235 days