Minutes of the November 10, 2016, Meeting of the
National Industrial Security Program Policy Advisory Committee (NISPPAC)

The NISPPAC held its 55th meeting on Thursday, November 10, 2016, at the National Archives and Records Administration (NARA), 700 Pennsylvania Avenue, NW, Washington, DC. Bill Cira, Acting Director, Information Security Oversight Office (ISOO), served as Chair. The minutes of this meeting were certified on January 6, 2017.

I. Welcome and Administrative Matters:

The Chair opened the meeting by welcoming everyone. He advised that a new director for ISOO has not yet been announced. He also announced that he will be retiring on December 31, 2016.

After introductions, the Chair recognized the two new industry members starting a four-year term: Kirk Poulsen and Robert Harney, replacing Tony Ingenito and J.C. Dodson, whose terms expired on September 30, 2016. Kirk Poulsen is the Chief Security Officer at Leidos, Incorporated, and has been active in NISPPAC activities representing Tech America, one of the Industry MOU groups. Bob Harney is the Director of Security of the Mission Systems sector of Northrop Grumman, and has also been active through the MOU groups, particularly NDIA.

The Chair acknowledged Michelle Sutphin as the new industry spokesperson. He also thanked Tony Ingenito and J.C. Dodson for their support to the NISPPAC over the last four years.

The Chair reminded the government members of the NISPPAC that their annual confidential financial disclosures are due to be submitted to the NARA General Counsel.

The list of meeting attendees is at Attachment 1.

The Chair turned to Greg Pannoni, NISPPAC Designated Federal Official (DFO), to address old business.

II. Old Business

(A) Action Items from Previous Meetings

Mr. Pannoni addressed the NISPPAC action items from the April 14, 2016, meeting. These action items were not addressed at the June meeting, held in conjunction with NCMS in Nashville, TN, because the format was different at the conference venue.

The first action item: DSS will post current information on their website pertaining to the backlog of cases pending at PSMO-I. As a result of discussions in the PCL Working Group and with DSS, it was determined that it would be difficult to keep pace with posting because the backlog is changing daily. Instead, the DSS Personnel Security Management Office for Industry (PSMO-I) will brief on the status of the backlog at the NISPPAC meetings. DSS will brief later in the meeting during the Personnel Security Working Group update.

The next item: 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. The question was raised by one of the industry members at the April meeting about the intended use of the reported costs, and whether the collection is designed to reflect the major cost to industry to implement the NISP. Mr. Pannoni requested Keith Minard, DSS, give a status report.

Mr. Minard reported that he and a small group of NISPPAC industry members met in June to discuss the cost collection methodology. The current DSS cost collection survey asks for a cleared company's total cost, and the percentage break-out of the total cost that covers manpower. The group determined that a better methodology is needed to identify what is included in the total cost. The group considered the Standard Form 716, Agency Security Classification Cost Estimate, used by government agencies to determine the cost of agency information security programs under Executive Order 13526, Classified National Security Information. The form breaks out nine categories of security-related costs. DSS will continue the discussion with NISPPAC industry members over the next few weeks or a month to consider if the cost break-out on the SF 716 can be used to improve the instructions in the DSS cost collection survey of industry. Of the cost categories on the SF 716, seven appear to be pertinent to industry: physical security, classification management, classified information, OPSEC, education and training, security management, and unique area requirements. DSS will provide an update at the March 2017 NISPPAC meeting.

The third action item called for establishment of a NISPPAC Insider Threat Working Group. The working group was established, and the first meeting was held in May. The second meeting was held in October. The working group report will be presented later in this meeting.

(B) Proposed Change to NISPPAC Bylaws – Industry Spokesperson

Mr. Pannoni addressed a proposed amendment to the NISPPAC bylaws to formalize the industry spokesperson position. For the past several years, an industry NISPPAC member has been serving in that capacity, but the position is not recognized in the NISPPAC bylaws. Recognizing the position in the bylaws will ensure consistency in carrying out the role. ISOO and the NISPPAC Chair also find it very helpful to have a central point of contact representing the industry members.

Attachment 2 is the language for the amendment to the bylaws. Attachment 3 is a copy of the NISPPAC bylaws with the language inserted under Article 3, paragraph E.

Mr. Pannoni reminded the members that this proposed amendment to the bylaws was presented to the members at the June 2016 NISPPAC meeting. It was then sent out to all members in an email asking for a vote to approve. However, only one vote was submitted, so it is presented for a vote at this meeting. Mr. Pannoni summarized the amendment that covers the role of the NISPPAC Industry spokesperson, who represents the NISPPAC industry members. The position allows the NISPPAC chair to work through the industry spokesperson, who can then reach out to the other industry members, as well as the MOU groups. The spokesperson will assign industry leads to the various NISPPAC working groups, and recommend industry subject matter experts,

as necessary, for the working groups. The industry members themselves select the spokesperson from among the eight current NISPPAC industry members, and nominates that member to the chair for consideration and approval. It is helpful for the person to be in the local metropolitan D.C. area for participation in impromptu meetings.

There were no questions from the attendees, so the chair called for a motion from the committee. Mr. Pannoni reminded the committee members that, in order for the motion to pass, approval is required by two thirds of the eight industry members and two thirds of the 16 government members.

A motion was made, and the chair called for a show of hands by the members to approve the motion. The chair also called for votes from the members on the phone.

Kathy Branch, ISOO staff, advised that the motion passed with the requisite number of votes, with the caveat that several of the member agencies were not represented by either a designated member or alternate member from that agency. ISOO staff will reach out to those agencies to have the representative vote confirmed by a member or alternate from that agency.

Attachment 4 provides the voting results and confirms the final approval of the amendment to the bylaws.

III. New Business

(A) Proposed Change to NISPPAC Bylaws – Industry Nomination Process

Mr. Pannoni presented another proposed amendment to the bylaws regarding the nomination process for industry members to the NISPPAC. The proposed amendment is at Attachment 5.

Mr. Pannoni advised the committee that the NISPPAC industry members have been following the proposed process for a number of years. However, it has never been officially documented. ISOO has received questions in the past from industry about how the nomination process works, so in the interest of transparency and to ensure consistency in the nomination and appointment process, the procedures are proposed as an amendment to the bylaws.

Mr. Pannoni invited the members to review the proposed amendment provided in their handout packets. Members may submit questions by email to Kathleen.Branch@nara.gov or to Robert.Tringali@nara.gov. If ISOO staff do not receive any questions, then they will forward the proposed amendment to NISPPAC members for an email vote, with votes to be submitted within 30 days of the email request for vote.

(B) Proposal for a NISPPAC National Interest Determination (NID) Working Group

Mr. Pannoni advised the group of a proposal for a NISPPAC working group to look more closely at agency processes for making national interest determinations (NIDs). NIDs are a requirement for certain cleared companies that are under foreign ownership, control, or influence that has

been mitigated by a special security agreement, and that require access to proscribed information; i.e., top secret, special access program information, sensitive compartmented information (SCI), restricted data, or communications security information. The government contracting activity is required to make the NID, and seek concurrence if the information is under the control of another agency; for example, SCI under the control of the ODNI. The NID process has been in place for many years; however, implementation has been somewhat uneven across the NISP agencies. ISOO has made some adjustments to the NID process in the revision of the NISP implementing directive. When ISOO requested informal input from the NISPPAC industry members on the revision of the NISP implementing directive, the industry reviewers suggested that the NISPPAC should focus more attention on the issues with the NID process; i.e., the lengthy timeframes that companies under FOCI and under special security agreements are experiencing with getting NIDs in place in order to perform on contracts requiring access to proscribed information. The suggestion was that the NISPPAC could focus more attention by showing NID stats at the NISPPAC meetings, similar to how the NISPPAC has addressed personnel security clearance data, and the access and authorization data for systems. There isn't a decision yet regarding a way-forward. However, ISOO plans to meet with the NISPPAC industry members, the CSAs, and the concurring agencies in mid-December to discuss the next steps and whether to establish a NID working group. After that meeting, the group will make a recommendation to the Chair on next steps.

Phil Robinson, industry member, provided a comment. He noted discussions with DSS, and their efforts to reduce the backlog. Given the production of the backlog and where the NIDs lie today, he commented that a working group, a full committee working group, is probably not necessary, and recommended that monitoring the situation would be more advantageous at this point.

(C) National Background Investigations Bureau

The Chair reminded the committee of presentations at the last two meetings pertaining to the stand-up of the National Background Investigations Bureau (NBIB) by the NBIB transition team. The Chair noted that the transition team had done its work, and the NBIB is officially established. The Chair introduced Mr. Charles Phalen, recently appointed as the first director of the NBIB. Mr. Phalen was previously with Northrop Grumman, and has been active in the American Society for Industry Security, so he well understands industry's issues and concerns with the personnel security background investigations process. Prior to Northrop Grumman, Mr. Phalen spent 30 years in federal service as Director of Security for CIA and FBI.

Mr. Phalen discussed the stand-up of the NBIB and where he sees it headed, both in the near-term and longer-term.

The number one issue for the NBIB is what is referred to as the backlog, but more focused on the volume of the backlog; i.e., just how long it takes to get a clearance, which currently takes too long. He noted that the backlog has its roots in the demise of OPM's contract with USIS a couple of years ago. The breach of OPM's database didn't help, either, in terms of both credibility and timeliness, but the real cause was loss of capacity through the USIS contract,

which was never really fully recovered. National level capacity of people who could do investigations diminished by thousands.

Secondly, NBIB is considering the issue regarding what and when should a periodic investigation be conducted; i.e., every five years, seven years, ten years; or be done on an aperiodic basis.

Another issue that affected the volume of work that all investigators have to deal with is the change in the federal investigative tier standards. There is as much as 20 percent more work to be done for a tier three investigation versus the old secret investigation. That affects the timeliness of the investigations.

NBIB is looking at reciprocity on two fronts. One aspect has to do with reciprocity of investigations. The other aspect has to do with the repurposing of investigations. There are a fair number of collateral investigations that are conducted by NBIB and its predecessor organization for DoD that get repurposed for SCI clearances. There are also some number where the intelligence community has done an SCI clearance, and NBIB is able to piggyback on that work. NBIB needs to be able to leverage that more. Information sharing is absolutely critical. Data collection and sourcing are going to be critical as the NBIB works out those capabilities.

Starting December 1st, NBIB will have a new investigative contract in place with four suppliers. Ultimately, when everybody gets up and running, that will give NBIB about six thousand or so contract investigators across the country. In addition, NBIB will have about two thousand federal investigators. NBIB hired four hundred federal investigators in 2016. Another two hundred will probably be on board in early 2017. This means that capacity is going up. The existing contractors are already increasing capacity, and the two new ones will be ready to go online shortly after the first of the year.

NBIB has been working very closely with an ODNI-sponsored group to determine what can be done in the short-term to deal with the backlog in a way that will speed up the process and still provide a credible product at the end. The group came up with about 10 or 11 items for serious consideration. There is more to come on this.

In terms of some roadblocks to be encountered, one is the fact that the administration is in the middle of a transition. That will be keeping everybody's attention during this process. More importantly, there is a provision in the Defense Authorization Act that says that the investigations should be moved to DoD. That is a concern at this point in time, given all of the time and effort involved in establishing the NBIB within OPM.

Mr. Phalen addressed what might be different about NBIB from the investigations providers in the past. NBIB has picked up the investigative capacity and capabilities of the federal investigative service, and are adding to it. A federal investigative records enterprise is a new approach to find new sources both electronically and manually, if necessary, to build the capability to collect and store information and move it through both an initial investigation and the reinvestigation, and then through the evolving continuous evaluation process. Key to this is going to be a law enforcement liaison capability that is not fully flushed out, but is absolutely

critical. Those primary sources help investigators understand what is happening in the lives of individuals under investigation. NBIB consolidated both the contract investigative management and the federal investigative management under one leader and one manager in order to mix and match capabilities, mix and match taskings, and use the entire team far more effectively. Looking to the future, NBIB is also setting up a strategy and business transformation team, as continuous evaluation of the NBIB process to identify ways to do investigations better and faster, and get better information quicker to an adjudicator.

Mr. Phalen advised that the NBIB recognizes the need to better focus on privacy and civil liberties and more clearly understands the requirement to protect all of the information collected about people during the investigative process. He also advised that the NBIB is putting together newly-aligned funding models so that it can roll out the funding profile to agencies in sufficient time for them to actually fit it into their end of fiscal year preparation. He expects the FY18 information will be out not too long after the first of 2017. He expects an even longer lead time for FY19.

The NBIB is a semi-autonomous element of OPM. It has an infrastructure that will remain relatively independent from OPM both from an information systems standpoint and a management standpoint. OPM understands that it can't independently build the systems needed to back up all of the investigative processes. OPM has partnered with DoD to build the next generation systems. This is probably close to a two year timeline. In the meantime, NBIB has to use the legacy systems. NBIB is building a new front-end interface to the eQIP that will make it easier to get into and fill out. The partnership with DoD is key, both in helping to keep secure those systems up and running today, and more importantly, to build out that secure system for the future.

In closing, Mr. Phalen emphasized that NBIB is looking out into the future to determine what an investigation will look like five years from now. How investigations are done, where they are done, and the ability will all likely be very different in five years. The Insider Threat program will likely be a tremendous help to a continuous evaluation program.

The Federal Government has probably not been as transparent with their customer base as they should have been, so he offered that NISPPAC members have an opportunity and an obligation to advise NBIB about what needs to change. Nothing is off the table. NBIB relies on groups like this to help make the process better and move forward.

The Chair called for questions for Mr. Phalen.

Mr. Pannoni, ISOO, noted that Mr. Phalen emphasized transparency and commented on two issues:

- Regarding the new Federal Investigative Standards, Mr. Pannoni noted that it would be helpful for the government to share the standards with industry security personnel to facilitate their managing their personnel security programs.
- Regarding the backlog, particularly of PRs, Mr. Pannoni noted that PR investigations are falling out of scope. The government's policy is that "clearances don't expire". However, the ODNI policy on that cannot be shared with industry because the ODNI

has the policy marked as "for official use only" (FOUO). He noted that the policy of the emerging controlled unclassified information (CUI) program is that if the information serves a lawful government purpose it can and should be shared.

Mr. Pannoni asked if there was anything that Mr. Phalen could do in his new position to facilitate sharing this information with industry.

Mr. Phalen responded that the ODNI would have to address the FOUO determination. However, he was surprised that these things have not been shared with industry. He didn't know there is a restriction on telling people in the security business what the investigative standards were. Regarding the PRs, he advised that there's nothing magic about five years. It was a decision made many years ago in the cold war environment with no scientific basis. Nothing changes at five years and one day. However, that also falls under the purview of the ODNI as a security executive. All organizations that are executing have to accept the five year policy, but the averages right now for PRs that are in the system are beyond five years, and probably closer to the six-year mark. It affects industry far more than the government. Industry personnel get turned away from access to government sites all the time because a PR hits a five-year mark, but that rarely happens to government personnel. The only concern should be that there is some known issue about an individual, which takes us to continuous evaluation and insider threat programs. The company should be able to advise that they have looked at the person, and that there is nothing of concern. He then turned to the ODNI representative to address the FOUO marking that prohibits sharing.

Gary Novotny answered for the ODNI. He advised that these issues have been discussed in the NISPPAC PCL working group. Mr. Novotny further advised that he is willing to engage with the appropriate government agency if an industry employee is being walked off of a government site because their PR is at five years and one day. He advised industry members to notify Michelle Sutphin, industry spokesperson, Greg Pannoni, or Kathy Branch, so that they can notify him of the issue, and he will troubleshoot those instances on a government to government basis to tell the government agency that clearances don't expire. He is working on trying to get a portion of an FOUO memo released for posting on either the ODNI or DSS website where industry can refer to it, as well as the Federal Investigative Standards. There is a redacted version of the investigative standards, so it's a matter of authority to officially release it. Mr. Novotny noted that he is actively working both of the issues with NBIB/OPM.

Mr. Pannoni responded to Mr. Novotny that it is helpful to hear that he is working the issues.

Tony Ingenito, industry, raised the point that companies learn about the issue of the overdue PRs and inability to get access to government sites when badges have to be redone and when the military has to reissue CAC cards.

Ben Richardson, DoD, advised that DoD is working to provide guidance and get information down to the lower level commands.

Michelle Sutphin, industry spokesperson, asked if NBIB had hired the 400 additional investigators they had planned to bring on board.

Mr. Phalen responded that the 400 additional investigators had been hired.

Ms. Sutphin then asked if they were trained.

Mr. Phalen responded that some are trained and that some are in training. NBIB has another 200 targeted to come on-board in 2017, so that is a net plus up of 600.

Mary Eddington, industry, noted the lack of sharing of information across the different systems that house clearance information; i.e., Scattered Castles, JPAS, CVS. She asked if NBIB would be able to influence fixing the lack of information sharing across the various systems.

Mr. Phalen responded that part of the work with DoD is to create a larger database that is much more sharable, and not just an NBIB database. He saw two issues. Scattered Castles should not be on an open system, so that needs to get worked out. The other issue is that in the newest version of Scattered Castles, industry is not able to get to the data that they used to be able to get to in the system. It's not a good thing to know that an investigation was conducted by an intelligence agency, but then be precluded from seeing that investigation. DoD is working with NBIB to build the capability to retain a broader amount of data that is accessible by a broader population.

(D) Defense Office of Hearings and Appeals – Industry Cases

The Chair introduced Mr. Perry Russell-Hunter, the Director of the Defense Office of Hearings and Appeals (DOHA). DOHA plays a key role in the personnel security process for Industry, providing the due process for individuals subject to having their eligibility for access to classified information denied or revoked.

Mr. Russell-Hunter addressed DOHA's role in the personnel security clearance process and the status of DOHA's industry cases. He noted that DOHA's work is at the tail-end of the personnel security process. Cases at DOHA represent historically and currently less than 1.5 percent of the cases in the process, which does not represent a large volume of cases. However, they represent the most complex of the issue cases. He shared an anecdote, noting that in an earlier day, the then-director of OPM, John Berry, responded to a question from then Senator Roland Burris in a Senate committee hearing, when he was asked, why are those cases not subject to the timelines of the Intelligence Reform and Terrorism Prevention Act (IRPTA). His response was perfect. He said, "We're not giving out driver's licenses here. We're giving out security clearances." These are the cases that are the very toughest.

Because issue resolution is important, Mr. Russell-Hunter advised that he welcomed Mr. Phalen's arrival to lead NBIB, and the opportunity to work with him on issue resolution, as it has been a chronic problem for the past 10 years. Adjudicators at the DoD CAF and the DOHA administrative judges and department council have wrestled with the fact that many cases come to DOHA with major issues not resolved. Starting back in 2007 as part of the Clearance Reform Movement the federal government managed to build a standard form 86 that had branching questions that were the questions that adjudicators were mostly like to ask. If an applicant said

"yes" to a question, the system opened a bunch of other questions. This was a reform that was designed to do something that appears counterintuitive; when you increase the public burden of a form like the SF-86, you generally do not expect thanks. The idea was to meet the clearance reform goal of resolving cases at the earliest possible point in the process. That is a shared goal by everybody in this room. The idea is to be able to make a determination at the earliest reasonable point in the process, but that includes making sure that any issues are resolved.

The first time DOHA touches a case is when the DoD CAF sends a draft statement of reasons to DOHA for a legal review. There was some question at the last NISPPAC meeting as to whether there was a backlog. The answer is, there used to be, but there isn't anymore. One of the things that DOHA had to address was the fact that as the DoD CAF worked through their growing pains, they also successfully addressed a significant backlog, which had a temporary effect on DOHA.

A year before the last NISPPAC meeting in June, DOHA had four thousand cases for legal review. By the time of the NISPPAC meeting in June, DOHA had twelve hundred. Now DOHA has 126. DOHA has completed legal reviews of all of the substantial number of draft Statements of Reasons in issue cases that the DoD CAF had passed to DOHA. In so doing, DOHA got word out to the members of industry whose clearances were in jeopardy as to the reasons for the Government's concerns. The Statement of Reasons is, by Executive Order, required to be the notice to the individual that tells them in as detailed and comprehensive a manner as the national security will allow, the real facts, so that the individual has a fair opportunity to respond. That is the national standard for providing this notice to the affected individuals. All those statements of reasons have now been issued. The DoD CAF and DOHA worked together. It took resources, planning, and figuring out how to do things a little differently. But the good news is that it got done. DOHA asked for more resources and got them; i.e., 15 three-year term appointments; to get through not only reviewing the statements of reasons, but also getting them to hearing and getting the hearings done.

Mr. Russell-Hunter addressed the DoD CAF slides that will be presented as part of the NISPPAC PCL working group update later in the meeting. The DoD CAF presentation is at Attachment 6.

Mr. Russell-Hunter noted a correction to be made to the second of the two slides. The slide suggests that there is a larger number of cases with DOHA for due process than there actually are. This is because the DoD CAF took over industry SCI cases from DIA on July 1. A number of those cases were quite dated and old. So where it says, "IT latency issues and challenges from the legacy CATS", that is because the DoD CAF has been running without E-adjudication for the past year." E-adjudication is back in place and working again. That's a really important thing, because anytime we can decide a completely clean case or a no-issue case on day one, that's good for everybody. That's one of the basic clearance reforms proposed back in 2007. Also, that third bullet that says, "Increase in closed older cases, including older cases reviewed by DOHA" -- it should not say "cases reviewed by DOHA". It should say "SCI cases gained by the CAF on June 1st, 2016", because that's what actually happened. The DoD CAF has taken on something that will cause industry SCI cases to move much more quickly in the future. Their proven model for success is going to get applied to these cases. They just haven't had a chance to do it yet.

And that's why you see that bulge for July, August and September there. However, those cases are not DOHA cases.

DOHA currently has 978 cases for hearing, 811 non-hearing cases, and 54 cases on appeal. That is a very manageable workload with 35 administrative judges and 35 department counsel. If any NISPPAC industry members have a case in question, industry should contact DOHA to ask about its status. DOHA can provide the update and move the case.

As discussed in a prior NISPPAC meeting, there are still cases that are incorrectly shown in JPAS as being with DOHA, when they actually aren't. That was because the old DISCO setup in CATS, which was the case management system the CAF was using, was showing cases when they moved from a non-issue adjudicator to an issue adjudicator, literally just moving down the hall, or in some cases down a few cubicles, as having been sent to DOHA, because that's the way DISCO had essentially hard-wired the system back when there were separate DISCO and DOHA adjudicators. So when DISCO's hundred-odd adjudicators and DOHA's 35 adjudicators joined forces as the Industry division in the DoD CAF, thousands of cases were showing as being DOHA cases that were, in fact, not DOHA cases. Part of the reason that there had been a perception of a backlog at DOHA was because of those false numbers in JPAS. The good news is that those old cases are almost gone. The work is flowing smoothly now between DOHA and the DoD CAF.

Mr. Russell-Hunter shared that he is looking forward to working with the new NBIB director on issue resolution. He noted that through the aftermath of the Washington Navy Yard case, and knowing what had really happened with Aaron Alexis, one of the lessons learned was that issues in the case had not been resolved, which was why he was not identified in the system.

IV. Working Groups

(A) Personnel Security Clearance Working Group

The Chair called for the report from the Personnel Security Clearance Working Group, starting with the DSS Personnel Security Management Office for Industry (PSMO-I) by Ms. Heather Green. He advised the committee that the performance metrics for DOE and NRC are provided in the handout packets but are not being briefed at this meeting. See Attachments 7 and 8.

PSMO-I:

PSMO-I slides are at Attachment 9.

Ms. Green noted that DSS is involved in the front-end processing of investigation submissions for contractors under DoD cognizance. DSS is experiencing significant funding challenges for industry personnel security investigations this fiscal year. There is a combination of factors that are contributing to this shortfall. DSS received less funding in the FY 17 initial budget. DSS had an unfunded inventory carry-over from FY 16 into FY 17, representing one of the largest carry-overs they ever had. DSS also had the NBIB increase and investigation crisis, plus an increase in demand for Tier 5, the top secret investigations. DSS is metering submissions to

NBIB due to that significant budget shortfall in order to spend the money soundly. This is impacting the front-end processing timelines. The current PSMO-I inventory is approximately twenty-five thousand. Of those, about 72 percent are periodic reinvestigations, and the remaining 28 percent are initials. The delays at this point continue to grow, so DSS is prioritizing the initials first, as those impact the ability to make interim determinations. The delays for an interim as a result of the metering of submissions result in timeframes that are about 30 days for initials. Understanding that interims are critical, DSS is looking for some short-term as well as long-term sustainable solutions.

PSMO-I has a critical priority request process. If companies have any cases that are sitting in the PSMO-I inventory, the company can contact PSMO-I by calling the knowledge center and advising of a critical priority need. PSMO-I will consider those priority needs that are impacting classified contract performance. PSMO-I is focusing on the initials, will work through that inventory, prioritize them, and then prioritize the back end once PSMO-I has received the appropriate investigative product from NBIB in order to make those interim determinations.

PSMO-I expects that the backlog will continue to grow until DSS receives appropriate reprogramming of funding. Some other potential solutions being considered include potentially temporarily suspending the periodic reinvestigations. In the meantime, DSS is working through reprogramming efforts.

OPM

The chair introduced Christy Wilder, NBIB, to provide the OPM report.

The OPM slides are at Attachment 10.

The report is a roll-up of all the different types of investigations that NBIB conducts for industry. The report covers quarter four, so the investigations were technically conducted by the Federal Investigative Services, as NBIB launched on October 1. For each of the investigative types, there's an uptick in timeliness for investigations. The initials include both SECRET and TOP-SECRET investigations. Ms. Wilder pointed out a few anomalies significant for the committee. The increases in time for the initiate phase of the investigations; i.e., the time it takes to get the cases in the door to NBIB; is 29 days for all initial investigations. For the SECRET and CONFIDENTIAL investigations, there is an uptick to 32 days to initiate. The time to initiate SECRET reinvestigations is up to 42 days. Those increases show the impact of the DSS funding issue that Ms. Green referenced. DSS has to wait to submit the investigations pending funding, so there is the uptick in timeliness.

Regarding adjudications, one of the anomalies is the uptick to 80 days for the TOP SECRET reinvestigations. This appears to be the result of the DoD CAF focusing their resources on adjudications of initial so that people can go to work.

ODNI

The Chair called for Gary Novotny to make the ODNI report.

Mr. Novotny reported the timeliness metrics for DoD industry as provided by OPM, as well as the data provided by intelligence agencies for the intelligence community contractors: CIA, DIA, FBI, NGA, NRO, NSA and Department of State. The ODNI slides are at Attachment 11.

The report covers initiation, investigation and adjudication of the contractor cases. It does not address any kind of pre-submission or post-decision coordination. The slides are very similar to the OPM slides that Ms. Wilder just presented. There is an uptick in quarter four FY 16 timeliness overall for the SECRET, TOP SECRET and reinvestigations; however, the volume of cases stayed consistent throughout FY 16. The data is also broken down separately for the SECRET, TOP SECRET and reinvestigations. As Ms. Wilder and Ms. Green already reported, DSS PSMO-I is metering their submissions, so the initiate time has increased from the 14-day goal.

ODNI broke down quarter four data to show the difference between legacy SECRET cases compared to the new tier three cases. As Mr. Phalen said, there is more field work for the tier three cases, but for quarter four, there was a significant decrease in time for the tier three investigations. The tier three time is still over the 74-day goal, but it does show a decrease. ODNI will continue to track the difference in timeliness between the legacy SECRET cases versus tier three investigations.

Mr. Novotny addressed other Security Executive Agent initiatives. The development of the e-adjudication business rules was a great initiative jointly worked by DOD, OPM and ODNI. The e-adjudicative business rules were approved for use on the cleanest cases; i.e., the tier 3 and tier 3 reinvestigations. The DoD CAF will use them to electronically adjudicate the clean tier 3 and tier 3 reinvestigation cases. This will going to free up the DoD adjudicators to review issue cases while the clean cases will move right through.

Mr. Novotny noted that both Mr. Phalen and Mr. Russell-Hunter talked about issue resolution. In addition to the timeliness slides that have been briefed over the last few years, there is also an initiative to address the quality of the background investigations. Since the Aaron Alexis shooting at the Navy Yard and the subsequent 90-day and 180-day reviews, one of the major recommendations was to improve the quality of the background investigations. The ODNI as the Security Executive Agent was able to push out quality assessment standards across the government to provide for a common lexicon and a common way to assess the quality of background investigations. The implementation plan was issued at the beginning of this year. Just yesterday, ODNI launched a quality assessment reporting tool across the government. It provides an opportunity for all the agencies that are receiving background investigations to go into the tool and rate the quality of the background investigations. For GAO audits and other types of reviews, ODNI didn't know the percentage of background investigations across the government that met quality standards. With the tool, the ODNI will be able to assess the quality of background investigations, and show which investigative service providers are providing a quality product and which ones need help. When they're not meeting the standard for issue resolution, or there are gaps in the background investigation, this tool will be able to track trends to help inform training for investigators. The intent is to have issue resolution on the first go-

around when the investigation gets to the CAF. Using the tool, ODNI would like to be able to provide quality metrics at future NISPPAC meetings.

DoD CAF

The Chair introduced Dan Purtill to give the report for the DoD CAF.

The DoD CAF slides are at Attachment 6.

Mr. Purtill noted that everyone saw the DoD CAF slides earlier in the meeting. He advised that over the past several quarters the CAF has been maintaining a steady state in spite of a number of challenges. As already noted by Mr. Russell-Hunter, Mr. Purtill reported that the DoD CAF took over the SCI mission from DIA and also took the non-DIA employees from the DIA CAF. As a result, the DoD CAF experienced an increase in the volume of cases. The DoD CAF had hoped to eliminate its backlog by this time, in line with the goal established when the CAF was stood up about three and a half years ago. The CAF is still pushing to eliminate the backlog during this FY.

With regard to IRPTA compliance, timelines have been creeping up, particularly for the tier five reinvestigations. The DoD CAF has been focusing its resources on the initials. Some of this is also impacted by the fact that the DoD CAF took a fair number of SCI periodic reinvestigations from DIA. The fact that the DoD CAF lost the ability to use e-adjudication on October 1st of last year, and didn't get it back until just the past couple of weeks had a big impact on the CAF. There were about forty to fifty thousand cases that would have been electronically adjudicated over that year that ended up having to be manually adjudicated. The DoD CAF has e-adjudication back in place for most of the populations covered by the CAF, to include industry cases. The DoD CAF is actively working e-adjudication for the tier one investigations, as well. There is less impact because there are fewer cases, but it represents about fifteen thousand cases, creating efficiencies that can be focused onto the more complex work. This will facilitate more improvement over time.

Mr. Purtill referred to Mr. Russell-Hunter's presentation, recognizing that there are numbers on the DoD CAF slides that incorrectly refer to DOHA and legal sufficiency reviews. Mr. Purtill advised that future briefings will correctly display that data. He expressed that this is being successfully worked out with DOHA.

(B) Information Systems Authorization Working Group Report

The Chair reported to the committee that the Certification and Accreditation (C&A) Working Group has changed its name to the NISPPAC Information Systems authorization Working Group. The new name is a better fit with the risk management framework (RMF) for authorizing systems that process classified information.

A summary of the working group's purpose and scope is at Attachment 12.

DSS

The Chair introduced Mr. Karl Hellmann, the DSS designated authorizing official for contractor information systems under DoD cognizance, to make the working group's presentation.

The working group presentation is at Attachment 13.

Mr. Hellman provide an update DSS' transition to RMF. DSS instituted a phased implementation approach to transitioning the assessment and authorization of contractor systems to classified information systems. DSS released their process manual. They are working on a streamlined system security plan template in coordination with the working group.

In order to prepare to transition to RMF, DSS provided more than 70 outreach briefings at industry events through FY 2016, to include the NISPPAC working group, this NISPPAC meeting, local industry security advisory council meetings, local NCMS meetings, corporate security meetings, the NDIA/AIA Industrial Security conference; anywhere that DSS was invited. DSS also spent a couple of weeks doing internal training on the RMF process.
In order to make all the information for RMF easy to locate for contractors, DSS created an RMF resource center on the DSS.mil homepage: DSS.mil/rmf. There are a variety of products, from technical assessment guides to tools to job aids for industry information system security managers.

The DSS Center for the Development of Security Excellence (CDSE) has a separate course for each of the six steps of the RMF process, as well as an overall RMF class and an online class on continuous monitoring. 52 industry personnel have completed all of those classes, and several hundred are in the process of taking the individual classes. CDSE is in the process of developing three additional courses; the Introduction to RMF, an RMF Walkthrough, and Configuring Systems for RMF.

NRC

The Chair introduced Will Ewald from NRC to give an overview of the authorization process for NRC contractors and licensees.

The NRC presentation is at Attachment 14.

Mr. Ewald provided a high-level overview of the NRC industrial security program. He reported that NRC maintains two separate industrial security programs; one for NRC-cleared contractors, much like any DoD contractor, and another program for NRC licensees and licensee contractor companies who operate and oversee commercial reactors, fuel cycle facilities, transportation of nuclear waste and the like. Because NRC's program is small, NRC has an MOU with Department of Energy to perform certification and accreditation and reviews of the NRC licensee and licensee contractor classified networks. NRC has a total of 10 classified licensee networks accredited by DOE on behalf of the NRC.

NRC has no cleared contractor companies requiring classified IT systems at their facility. NRC is in the process of working with DOE to modify the current MOU, which will allow DOE to

perform RMF functions for NRC-cleared contractors like the one in place for our NRC licensees right now, in the event that any of the NRC contracts require classified systems in the future.

The Chair thanked Mr. Ewald and noted that the NISPPAC would like to have other CSAs brief their information system authorization processes at future NISPPAC meetings.

(C) Insider Threat Working Group Report

The Chair asked Mr. Pannoni to give the report of the Insider Threat Working Group.

Mr. Pannoni reported that the Insider Threat Working Group has met twice. The first time in May, and then in October with industry, the CSAs, DSS and CIA, and the National Insider Threat Task Force.

Mr. Pannoni recognized two key areas for the working group: information sharing and integration.

The group recognized integration of personnel security and information systems security as two key areas that impact an insider threat program. The group recommended that at least annually, all three of those NISPPAC working groups (Personnel Security, Information Systems, and Insider Threat) meet jointly to discuss issues of mutual concern; such as trying to build an insider threat program so that the personnel security program has the information to make better-informed decisions about issuing/continuing clearances.

Regarding information sharing, the working group provided opportunity for all the CSAs to share information about how they are implementing insider threat for their contractors, and for the industry members to share their experience thus far. It is still early for industry implementation. The NISPOM change two that established the requirement for an insider threat program was just issued in May. One of the challenges noted for the CSAs is sharing among CSAs. This is important because industry personnel often move from company to company, with the companies sometimes coming under different CSAs. There may be vital information that one CSA has that needs to be shared with another.

The group recognized the importance of hearing more from the smaller companies and the challenges they have. Implementation of insider threat in smaller companies will be different than in a large company that has separate departments for HR, information systems, etc. In a small company, the security officer may be doing everything.

V. Reports and Updates

(A) Industry Presentation

The chair requested Michelle Sutphin, the new industry spokesperson, give the industry presentation.

The industry presentation is at Attachment 15.

Ms. Sutphin recognized the two new industry NISPPAC members; Kirk Poulsen, who was not present, and Bob Harney. She also recognized the two outgoing industry NISPPAC members; Tony Ingenito and J.C. Dodson.

Ms. Sutphin updated the committee on the current MOU representatives. Steve Kipp is replacing J.C. Dodson for AIA. She advised that the MOU representatives are discussing the potential to revise the MOU agreement. It appears that the last time the agreement was addressed was in 2005.

Industry anticipates much change in 2017, to include insider threat implementation, CUI, rick management framework (RMF) standards, the new Joint Verification System (JVS) system, and the NISP Contract Classification System (NCCS). Industry's concern is being able to stay on top of all of the daily churn in addition to all of these new requirements and systems. Industry is concerned about the growing backlog of personnel investigations and its impact on hiring new personnel, especially junior personnel who have never been cleared before. Industry is also concerned with the increasing length of time for interim secret determinations and its impact on the onboarding processes. Industry, obviously, is going to continue to be responsive to all of these new initiatives, and is looking forward to a continued partnership with the government. The increase in communication over the past few years has definitely helped industry prepare for all of these changes.

With regard to the personnel security clearance timelines, Ms. Sutphin thanked Mr. Phalen for the update NBIB's hiring additional investigators. The next thing that industry would like to see is the ODNI memo to components advising that clearances don't expire at the five year mark so that industry personnel can appropriately get access to government sites and bases.

With regard to the Department of Commerce and DSS survey, Ms. Sutphin noted that several meetings had been held with ISOO, Commerce, and DSS to address the additional burden that filling out this survey is going to have, especially for the larger companies. Boeing, L3, and Harris are currently working with the government as beta testers to determine how best to respond from the perspective of multiple facility organizations.

Ms. Sutphin referred to the CUI implementation, the DFARS clause pertaining to unclassified covered defense information and cyber incident reporting, and the FAR clause pertaining to federal contract information, all of which are in the process of being implemented. She advised that industry is preparing to conform to NIST 800-171 by December of 2017. The large companies have a good handle on it, but the concern is the smaller companies who don't have a good understanding of the 800-171. Those smaller companies are in the supply chain. Industry wants to ensure the supply chain is secure.

Industry has been involved with the NISPOM rewrite. Ms. Sutphin noted that there has been much progress. She advised that she has more than 70 industry representatives on her team to provide comments. She reported that industry is pleased with the progress of the NISPOM rewrite so far. She advised that industry is interested in learning more about the progress of

various policy issuances being worked right now by the ODNI, specifically regarding reporting requirements and reciprocity. It would be beneficial for industry to see drafts and provide input and feedback just as they have on the NISPOM. Industry understands that drafts may be marked as FOUO, and not releasable to industry, but industry is making the request to review the draft policies.

Ms. Sutphin addressed the industry involvement in the NISPPAC working groups. Industry is very interested in the lengthy personnel security timelines right now, especially the interim clearance timelines and the impacts that they have. Industry is eagerly awaiting full implementation of e-adjudication to help decrease timelines. Industry is also looking at the implementation of the various new applications in development right now and the impact, especially with having to learn how to use the new systems. NCCS will go live in December, and industry is concerned that there is just one person at DSS handling NCCS. Industry requests more information about whether NCCS will be integrated into the knowledge center, have a help desk to call, and whether DSS will be prepared for the influx of new user applications as industry tries to go live with that system. Industry is also eagerly awaiting JVS and its training resources so that the 13,000 cleared contractors can be trained. Industry is also concerned that JPAS and JVS will both be running and mirroring each other between December and March, and even further into 2017. Based on prior experiences, industry is concerned about the accuracy of the data in the systems during that timeframe.

Industry understands there will be a governance review board for JVS, and that all of the changes to JVS will go through this board. Industry would like to have an advocate on that board to ensure the industry voice is represented when changes take place.

Industry was involved in the development of the DSS NISP Information System for Security (NISS) about a year and a half ago, but haven't heard anything more recently. Industry requests a NISS update.

With regard to the Insider Threat Working Group, Ms. Sutphin noted that industry is most concerned with how their insider threat programs are going to be evaluated by DSS. The larger companies will be looking at how their programs are evaluated at the enterprise level versus the local level, and what DSS will be looking for in terms of enterprise versus local.

With regard to the Information Systems Authorization Working Group, industry is preparing for RMF and its challenges.

(B) Department of Defense (DoD) Update

The Chair called for Ben Richardson from the Office of the Under Secretary of Defense for Intelligence to provide the update for DoD.

Mr. Richardson reported that DoD is continuing development of its continuous evaluation program, working with the ODNI. DoD is refining its process of identifying the population groups, the risk population, and whether or not there were adjudication issues identified by the process.

Mr. Richardson thanked DSS for their leadership and thanked industry for their initiative on insider threat. DoD appreciates the effort DSS has taken to get information out to the industry. DoD also appreciates industry's motivation to understand the importance of the program as it relates to the larger issues associated with personnel security and continuous evaluation.

Mr. Richardson reiterated that DoD has been working with industry on the NISPOM rewrite, along with the other CSAs, DSS, and others, with a goal of getting the NISPOM into the informal coordination process in FY 17. The NISPOM will ultimately be accompanied by a federal rule. DoD hopes to have that companion federal rule is process in FY 18.

(C) Defense Security Service (DSS) Update

The Chair then called for the DSS update, which was presented by Keith Minard.

Mr. Minard began by reminding the committee that the implementation date for insider threat is November 30. He reported that industry has been working to submit and nominate their insider threat officials, certify their plans, and get their programs in place to make sure that they meet the requirements of NISPOM Change 2. DSS has met with Lockheed Martin, DRS and L3 to talk about corporate program implementation. DSS came up with a plan to conduct mock assessments in December to see how the DSS oversight procedures will apply in a corporate setting. This is much different than the way DSS has approached NISP oversight in the past. Mr. Minard advised the industry members that DSS has a full range of tools on their website to enable industry insider threat implementation; i.e., the ISL and NISPOM, training courses, and templates for insider threat program plans. When DSS conducts the initial assessments of contractor insider threat programs, they will be looking for implementation of the basic, fundamental, minimum requirements: officials are appointed, training accomplished, and a certified plan. Later follow-on assessments will look at the effectiveness of the insider threat programs. DSS will evolve in its oversight as industry evolves in its implementation. Ultimately, insider threat needs to be something that adds value to security programs and protection of national security information.

With regard to NCCS, phased implementation has begun. Efforts are underway with non-DoD government customers to finalize agency implementation. DSS is working separately with the military departments and services; based on their size, as they take a bit more work. Industry implementation will be a phased approach. DSS will use NCMS, the NISPPAC, and other associations for outreach. User guides, webinars, and other information is available on the DSS website. Mr. Minard referenced industry's concern about DSS manpower to support NCCS. He advised that DSS will use the knowledge center expertise as an option for future account setup and assistance. He anticipates the knowledge center capability to be available about the second quarter of this FY.

Version 5.9.1 of NCCS deployed in October. DSS expects final operating capability around the 23rd of December after eight weeks of testing. Northrop Grumman and Leidos have had their global accounts established, and DSS is currently working with Raytheon. Given the thousands of contractors and hundreds of government customers, implementation has to be a step-by-step

process. DSS will look at every opportunity to use resources to the best advantage to assist industry in getting accounts. DSS is working with NCMS to have a location at the annual seminar where DSS can assist industry with establishing accounts.

With regard to NISS, DSS is halfway through development and on track for fourth quarter FY 17 deployment. Industry testing will be scheduled for February and May. DSS will work again with NCMS and the NISPPAC for testing. DSS will have webinars and other information on the DSS website to make sure that both industry and government are informed.

Michelle Sutphin, industry, asked if Ryan Deloney is still the DSS POC for NISS. Mr. Minard answered affirmatively.

(D) NISP Implementing Directive Update

The Chair reminded the committee that ISOO has reported over the last two meetings about the revision to the NISP directive, 32 CFR 2004. He asked Kathy Branch of the ISOO staff to give a status report.

Ms. Branch reported that the Office of Management and Budget (OMB) had sent the 32 CFR 2004 revision to executive branch agencies for formal interagency coordination. ISOO is in the process of clearing the comments provided to OMB through the interagency coordination. NARA is still on track for OMB to issue a proposed rule with a request for public comment.

(E) Controlled Unclassified Information (CUI) Update

The Chair advised the committee that the CUI regulation was published in the Federal Register on September 14. It goes into effect on November 14. He asked Mark Riddle from the ISOO CUI to give an update.

Mr. Riddle reiterated that the 32 CFR part 2002 to implement the CUI program will become effective on November 14th. That means that executive branch agencies will officially start implementation activities. Implementation activities are highlighted in CUI notice, 2016-01, which is available on the ISOO website. All agencies need to develop a policy that realigns their current practices to the standards of the CUI program. Then, as associated with any information security program, there are requirements for training, physical safeguarding, the modification of computer systems, and eventually the development and initiation of a self-inspection program within agencies. With regard to industry, ISOO has begun development of a CUI federal acquisition regulation (FAR) clause. The clause will standardize the way in which agencies give guidance to industry when it comes to protecting CUI. There will be direct references in the FAR clause to the NIST special publication 800-171, which is already referenced in the 32 CFR 2002. ISOO expects the FAR clause to be out about November of 2017.

Mr. Riddle addressed CUI markings. He referred the committee to the CUI registry on the ISOO website. The registry contains the categories and sub-categories of information that are CUI. Currently, there are 23 categories and 84 subcategories, all of which can be linked back to law, regulation or government-wide policy. The registry also contains the category markings

associated with each one of those CUI categories. There is a marking handbook, and information about how to mark or alert recipients that information is CUI. Mr. Riddle advised everyone to go to the registry and download the marking handbook. It will answer many questions that most people have.

Mr. Riddle advised that ISOO considers the CUI registry to be a living document, because it is a reflection of current laws and regulations. As agencies with regulatory authority issue revisions to laws, the CUI registry will also be modified to reflect those requirements.

Mr. Riddle addressed references made during this meeting to FOUO classification of documents that industry wants to see but which cannot be released to them. Many see CUI as a replacement of FOUO. However, CUI is a refinement of what needs to be protected as CUI. Under the CUI program, executive branch agencies will only be able to protect what can be linked back to a law, regulation, or government-wide policy that says that it must be protected. Agencies can only apply CUI markings if the information or material qualifies as CUI. Based on discussions here today, Mr. Riddle advised that he can't make a ruling on whether or not the information that has been discussed is CUI or not. Part of the implementation of the CUI program within that particular agency will be to evaluate products or documents that bear that FOUO marking, and then assess whether or not they fall into the program.

There is a dissemination standard in the CUI program. Dissemination is based on a lawful government purpose versus need-to-know; meaning that the CUI program errs more on the side of sharing information with those who have an operational need for it in the furtherance of the government in some way.

Mr. Stephen Ulate, Navy, requested clarification of the dissemination standard; i.e., not based on need-to-know.

Mr. Riddle responded that the concept generally used for the sharing of sensitive information is need-to-know. The dissemination or sharing standard for information under the CUI program was revised to lean more towards authorized information sharing. If you can recognize a need for access to CUI to fulfill a lawful government purpose, the information can be shared. A great example would be that if DHS came into possession of some actionable unclassified, terrorism-related intelligence information, and they had a need to share it with a state and local entity, they would be compelled to share that for a lawful government purpose. A lawful government purpose does not mean a lawful federal government purpose, it means a lawful government purpose; so it encourages the sharing with state and local officials in the interest of protecting the country.

Mr. Pannoni asked Mr. Riddle to address DoD's unclassified controlled technical information (UCTI) and the CUI program.

Mr. Riddle responded that UCTI is a category of CUI. The CUI registry is a catalog of what the government should be protecting today. As part of the development of the CUI program, ISOO as the executive agent asked agencies and major stakeholders to identify what they were currently protecting, and to identify the regulatory basis for that protection. DoD identified the

UCTI category. The CUI registry contains the categories and their descriptions, and the listings and links to the underlying authorities of why it is considered to be CUI. This is an important part of the CUI program. Currently, throughout the executive branch agencies, and major components within DoD, there is no clear standard for what is being protecting. An agency head or an operational component can arbitrarily identify a dataset and say that it's going to start protecting it, and call it FOUO, but with no basis for that protection under the CUI program. The CUI program is a way to narrow the scope of what is being protected, and ensure that agencies are protecting those things that can be linked back to laws and regulations.

Mr. Riddle advised that he and others from the ISOO CUI staff go out and brief industry; i.e., large and small companies, and academic institutions; about what it takes to implement the CUI program within those organizations. They address the NIST SP-800-171, as well. Mr. Riddle advised that he is one of the co-authors of that document, so is in a good position to speak with pretty good authority about what is in it, the intent behind it, and also speak to the new revision which is going to be coming out here in a couple of months.

VI. General Open Forum/Discussion

The Chair opened the meeting for anyone to present new business or to speak to the committee. There was no discussion.

VII. Closing Remarks and Adjournment

The Chair thanked attendees for coming, and thanked all the presenters. He announced the dates for the 2017 NISPPAC meetings: March 15th, July 12th, and November 14th, all to be held in the Archivist's Reception Room. The chair adjourned the meeting.

SUMMARY OF ACTION ITEMS

- DSS will provide an update on the cost collection methodology, in collaboration with industry, at the next NISPPAC.
- ISOO will confirm the votes for the industry spokesperson amendment to the NISPPAC bylaws that were made by agency representatives that are not either the member or an alternate. (Note that this was completed, and the vote confirmation is at Attachment 2.)
- ISOO will request an email vote from NISPPAC members on the proposed amendment to the bylaws to include the industry member nomination process. The request for votes will be made after all members have an opportunity to review the proposed amendment and pose any questions.
- NISPPAC industry members and CSAs will make a recommendation to the NISPPAC chair regarding establishment of a NISPPAC NID working group after meeting in mid-Dec. to discuss the issue. (Note that due to scheduling, the meeting will be held on Jan. 11, 2017.)

- Industry requests an update from DSS on the status of the NISP Information System for Security (NISS). ISOO will include an update on the agenda for the March 2017 NISPPAC meeting.

Attachments:

1. Attendee List
2. Summary language of proposed amendment to NISPPAC bylaws: NISPPAC Industry Spokesperson
3. NISPPAC bylaws with proposed amendment for NISPPAC industry spokesperson inserted
4. Voting results for proposed amendment to the NISPPAC bylaws for an industry spokesperson
5. Proposed amendment to the NISPPAC bylaws to include the nomination process for industry members to the NISPPAC
6. DoD CAF Metrics
7. DOE Personnel Security Performance Metrics
8. NRC Personnel Security Performance Metrics
9. Briefing: DSS Personnel Security Management Office for Industry
10. Briefing: Office of Personnel Management
11. Briefing: Office of the Director of National Intelligence
12. Summary of name change, purpose and scope of NISPPAC Information Systems Authorization Working Group
13. Briefing: NISPPAC Information Systems Authorization Working Group
14. Briefing: Nuclear Regulatory Commission Information Systems Authorizations
15. Briefing: NISPPAC Industry

Attachment #1

NISPPAC MEETING ATTENDEES

The following individuals attended the November 10, 2016, NISPPAC meeting:

William Cira	Information Security Oversight Office	Acting **Chair**
Greg Pannoni	Information Security Oversight Office	**Designated Federal Official**
Charles Phalen	Office of Personnel Management/National Background Investigations Bureau	Attendee/Presenter
Perry Russell-Hunter	Defense Office of Hearings and Appeals	Attendee/Presenter
Heather Green	Defense Security Service	Attendee/Presenter
Christy Wilder	Office of Personnel Management/National Background Investigations Bureau	**Observer**/Presenter
Gary Novotny	Office of the Director of National Intelligence	Attendee/Presenter
Dan Purtill	DoD Central Adjudication Facility	Attendee/Presenter
Karl Hellman	Defense Security Service	Attendee/Presenter
William Ewald	Nuclear Regulatory Agency	Attendee/Presenter
Michelle Sutphin	Industry Spokesperson	**Member**/Presenter
Ben Richardson	Department of Defense	Attendee/Presenter
Keith Minard	Defense Security Service	**Alternate**/Presenter
Kathleen Branch	Information Security Oversight Office	Attendee/Presenter
Mark Riddle	Information Security Oversight Office	Attendee/Presenter
Valerie Heil	Department of Defense	Attendee
Priscilla Matos	Department of Defense	Attendee
Heather Sims	Defense Security Service	Attendee
Jamaar DeBoise	Defense Security Service	Attendee
Jeff Spinnanger	Defense Security Service	Attendee
David Grogan	Defense Security Service	Attendee
Carla Leigh-Ronan	DoD Central Adjudication Facility	Attendee
James Anderson	Army	Attendee
Glenn Clay	Navy	**Alternate**
Stephen Ulate	Navy	Attendee
David Lowy	Air Force	**Member**
Dennis Hanratty	National Security Agency	**Member**
Victoria Francis	Office of the Director of National Intelligence	Attendee
George Ladner	CIA	**Alternate**
Mark Pekrul	Department of Energy	**Alternate**
Natasha Wright	Department of Energy	Attendee
Scott Ackiss	Department of Homeland Security	**Member**
Rich McComb	Department of Homeland Security	Attendee
Kathleen Berry	Department of Justice	Attendee
Zudayaa-Taylor Dunn	NASA	**Member** (by phone)
Michael Hawk	Department of State	**Alternate**
Dan Schoettinger	PMO-PAC	**Observer**
Sandy Day	Office of Personnel Management	Attendee
Bill Davidson	Industry	**Member**
Dennis Keith	Industry	**Member** (by phone)

Quinton Wilkes	Industry	**Member**
Phil Robinson	Industry	**Member**
Robert Harney	Industry	**Member**
Dan McGarvey	MOU Representative	Attendee
Marc Ryan	MOU Representative	Attendee
Dennis Arriaga	MOU Representative	Attendee
Mitch Lawrence	MOU Representative	Attendee
Dave Winnegren	MOU Representative	Attendee (by phone)

Other Attendees:

Aprille Abbott
Jennifer Brown
Jane Dinkel
Aaron Drewiske
Jim Harris
Vincent Jarvie
Steve Kipp
Joseph Kraus
Cory Klein
Stephen Lewis
Noel Matchett
Joseph Morris
Leonard Moss (by phone)
Rick Ohlemacher
Norman Pashoian
Emmett Price
Dorothy Rader
Rashid Shakir
Trellis Tribble
Richard Weaver
Rod Webb

Robert Tringali	Information Security Oversight Office	Staff
Joseph Taylor	Information Security Oversight Office	Staff
Alegra Woodard	Information Security Oversight Office	Staff
Carolina Klink	Information Security Oversight Office	Staff

Attachment #2

NISPPAC Bylaws

Proposed change to the bylaws:

NISPPAC Industry Spokesperson

The NISPPAC industry spokesperson serves as the focal point representative to the NISPPAC on behalf of the industrial base to coordinate collective points of view from the eight non-government NISPPAC members on national security policy regulations. The industry spokesperson is responsible for representing the NISPPAC non-government members at each NISPPAC meeting; recommends to the NISPPAC Chairman the addition or deletion of NISPPAC working groups, assignment of an industry lead to all NISPPAC working groups, and recommends industry subject matter expertise representation to all NISPPAC working groups.

The NISPPAC industry spokesperson is selected from among the eight current NISPPAC non-government members and nominated to the NISPPAC Chairman for consideration and approval. The spokesperson is expected to be flexible for attendance at impromptu government meetings where industry representation is required. The spokesperson engages with various facets of industry, to include the governing boards of professional, trade and other organizations whose membership is substantially comprised of employees of business concerns involved with classified contracts, licenses, or grants.

Attachment #3

National Industrial Program Policy Advisory Committee (NISPPAC)
Bylaws (As amended on November 18, 2015)

Article 1. Purpose.

The purposes of the NISPPAC are to advise the Chairman on all matters concerning the policies of the National Industrial Security Program (NISP), including recommended changes to those policies; and to serve as a forum to discuss policy issues in dispute.

Article 2. Authority.

Executive Order 12829, "National Industrial Security Program," as amended, (the Order) establishes the NISPPAC as an advisory committee acting through the Director, Information Security Oversight Office (ISOO), who serves as the Chairman of the Committee, and who is responsible for implementing and monitoring the NISP, developing directives implementing the Order, reviewing agency implementing regulations, and overseeing agency and industry compliance. The framework for the Committee's membership, operations, and administration is set forth in the Order. The NISPPAC is subject to the Federal Advisory Committee Act (FACA), the Freedom of Information Act (FOIA), and the Government in the Sunshine Act (GISA).

Article 3. Membership.

A. **Primary Membership.**
The Order conveys to the Chairman of the NISPPAC the authority to appoint all members. The Committee's total membership of 24 voting members shall be comprised of 16 representatives from those executive branch departments and agencies (including the Chairman) most affected by the NISP and eight non-government representatives of contractors, licenses, grantees involved with classified contracts, licenses, or grants. At least one industry member shall be representative of small business concerns, and at least one shall be representative of Department of Energy/Nuclear Regulatory Commission contractors or licensees. An industry member serves as a representative of industry, not as a representative of their employing company or corporation. All members must comply with the following guidelines: (1) Any federal employees who are appointed to the Committee must annually file a confidential financial disclosure report with the National Archives and Records Administration (NARA) Office of General Counsel (NGC) on or before the date of their first participation in a Committee meeting, and (2) For purposes of federal ethics law, the non-federal members of the NISPPAC have been determined to be "representatives" rather than "special government employees." NARA will ensure the Committee's non-federal composition does not violate President Obama's June 18, 2010, Presidential Memorandum on "Lobbyists of Agency Boards and Commissions." 75 Fed. Reg. 35.955 (Directing "heads of executive departments and agencies not to make any new appointments or reappointments of federally registered lobbyists to advisory committees or other boards and commissions...")

B. **Nominations.** The Chairman will solicit and accept nominations for Committee membership: (1) for representatives of the respective agencies, from the agency head; and (2) for representatives of industry, from the governing boards of professional, trade and other organizations whose membership is substantially comprised of employees of business concerns involved with classified contracts, licenses, or grants. Although an industry representative does not represent his or her employing company, the Chairman will solicit the approval of the Chief Executive Officer of that company to allow the nominated individual to serve on the NISPPAC.

C. **Appointment.** The Chairman shall appoint all Committee members. Membership includes the responsibility of the member to attend NISPPAC meetings personally as often as possible. However, a member may select one or more alternates, who may, with advance written notification to the Chairman, serve for the member at meetings of the Committee when the member is unable to attend. An alternate so selected shall have all rights and authorities of the appointed member.

D. **Term of Membership.** The term of membership for Government representatives shall be four years. When renominated by the head of their agency, a representative of a Government agency may be selected to serve successive four year terms. The term of membership for industry representatives shall be four years. The terms of industry representatives shall be staggered so that the terms of two industry representatives are completed at the end of each fiscal year. Industry representatives may not serve successive terms. When a Government or industry member is unable to serve their full term, or when, in the view of the Chairman, a member has failed to meet their commitment to the NISPPAC, a replacement shall be selected in the same manner to complete the unexpired portion of that member's term. Each representative's term of membership shall be conveyed by letter from the Chairman.

E. **NISPPAC Industry Spokesperson.** The NISPPAC industry spokesperson serves as the focal point representative to the NISPPAC on behalf of the industrial base to coordinate collective points of view from the eight non-government NISPPAC members on national security policy regulations. The industry spokesperson is responsible for representing the NISPPAC non-government members at each NISPPAC meeting; recommends to the NISPPAC Chairman the addition or deletion of NISPPAC working groups, assignment of an industry lead to all NISPPAC working groups, and recommends industry subject matter expertise representation to all NISPPAC working groups.

The NISPPAC industry spokesperson is selected from among the eight current NISPPAC non-government members and nominated to the NISPPAC Chairman for consideration and approval. The spokesperson is expected to be flexible for attendance at impromptu government meetings where industry representation is required. The spokesperson engages with various facets of industry, to include the governing boards of professional, trade and other organizations whose membership is substantially comprised of employees of business concerns involved with classified contracts, licenses, or grants.

F. **Security Clearance.** If it becomes necessary to hold a classified meeting, members and alternates in attendance must possess a current security clearance at or above the level of the meeting's classification. Clearance certification shall be provided in advance of the meeting to the Chairman by the employing agency or company. ISOO and NARA's Security Management Division will verify that members have been approved for access to classified national security information and ensure that classified information utilized in association

with a Committee meeting is managed in accordance with national policy (i.e., E.O. 13526, "Classified National Security Information.")

G. **Compensation.** Federal Government employees serving on the Committee are not eligible for any form of compensation. The Government will pay travel and per diem for industry members at a rate equivalent to that allowable to Federal Government employees. Industry members will submit travel vouchers to the Executive Secretary within 15 days after each meeting.

H. **Observers.** Any NISP participating organization (industry or Government) may send observers to attend meetings of the Committee. Such observers will have no voting authority and will be subject to the same restrictions on oral presentations, as would any member of the public. As determined by the Chairman, observers may be permitted to attend closed meetings. Industry observers will not receive travel or per diem compensation.

Article 4. Meetings.

A. **General.** The NISPPAC will meet at least twice each calendar year as called by the Chairman. As the situation permits, the Executive Secretary will canvass the membership in advance of the scheduling of meetings in order to facilitate attendance by the largest number of members. The Chairman will also call a meeting when so requested by a majority of the 16 Government members, and a majority of the eight industry members. The Chairman will set the time and place for meetings and will publish a notice in the Federal Register at least 15 calendar days prior to each meeting.

B. **Quorum.** NISPPAC meetings will be held only when a quorum is present. For this purpose, a quorum is defined as two-thirds of the 16 Government members, or alternates, and two thirds of the eight industry members, or alternates.

C. **Open Meetings.** Unless otherwise determined in advance, all meetings of the NISPPAC will be open to the public. Once an open meeting has begun, it shall not be closed for any reason. All matters brought before or presented to the Committee during the conduct of an open meeting, including the minutes of the proceedings of an open meeting, shall be available to the public for review or copying.

D. **Closed Meetings.** Meetings of the NISPPAC will be closed only in limited circumstances and in accordance with applicable law. When the Chairman has determined in advance that discussions during a Committee meeting will involve matters about which public disclosure would be harmful to the interests of the Government, industry, or others, an advance notice of a closed meeting, citing the applicable exemptions of the GISA, will be published in the Federal Register. The notice may announce the full or partial closing of a meeting. If, during the course of an open meeting, matters inappropriate for public disclosure arise during discussions, the Chairman will order such discussion to cease, and shall schedule it for a closed session. Notices of closed meetings will be published in the Federal Register at least 15 calendar days in advance.

E. **Agenda.** The Chairman shall approve the agenda for all meetings. The Chairman will distribute the agenda to the members prior to each meeting and will publish a brief outline of the agenda with the notice of the meeting in the Federal Register. Items for the agenda may be submitted to the Chairman by any regular, or alternate, member of the Committee. Items may also be suggested by non-members, including members of the public. To the extent possible, all written recommendations for NISP or National Industrial Security Program Operating Manual policy changes, whether or not they are placed on the agenda, will be provided to the Committee membership prior to the start of any scheduled meeting. The

Chairman will advise the party making the recommendation what action was taken or is pending as a result of the recommendation.

F. **Conduct of Meetings.** Meetings will be called to order by the Chairman, following which the Chairman or Executive Secretary will call the roll or otherwise take attendance and read or reference the certified minutes of the previous meeting. The Chairman will then make announcements, ask for reports from subgroups or individual members (as previously arranged), open discussion of unfinished business, introduce new business, and invite membership comment on that business. Public oral comment may be invited at any time during the meeting, but most likely at the meeting's end, unless the meeting notice advised that written comment was to be accepted in lieu of oral comment. Upon completion of the Committee's business, as agreed upon by the members present, the meeting will be adjourned by the Chairman.

G. **Minutes.** The Committee's Executive Secretary shall prepare minutes of each meeting, which will be certified by the Designated Federal Official (DFO) within 90 calendar days. Copies of the minutes will be distributed to each Committee member once certified. Minutes of open meetings will be accessible to the public. The minutes will include a record of the persons present (including the names of committee members, names of staff, and the names of members of the public from whom written or oral presentations were made) and a complete and accurate description of the matters discussed and conclusions reached, and copies of all reports received, issued or approved by the Committee.

H. **Public Comment.** Members of the public may attend any meeting, or a portion(s) of a meeting, that is not closed to the public, and may at the determination of the Chairman, offer public comment during a meeting. The meeting announcement published in the Federal Register may note that oral comment from the public is excluded and in such circumstances invite written comment as an alternative. Also, members of the public may submit written statements to the Committee at any time.

I. **Sub-committee Meetings.** The Chairman may establish a sub-committee(s), to include sub-groups or working groups. Each sub-committee shall brief the members of the NISPPAC on its work, and any recommendations of a sub-committee shall be presented to the NISPPAC for deliberation.

Article 5. Voting.

When a decision or recommendation of the NISPPAC is required, the Chairman shall request a motion for a vote. Any member, or approved alternate of the NISPPAC, including the Chairman, may make a motion for a vote. No second after a proper motion shall be required to bring any issue to a vote.

A. **Voting Eligibility.** Only the Chairman and the appointed members, or their designated alternates, may vote on an issue before the Committee.

B. **Voting Procedures.** Votes shall ordinarily be taken and tabulated by a show of hands. Upon a motion approved by two-thirds of the members present, a vote by secret ballot may be taken. However, each ballot must indicate whether the vote is from an industry or Government representative.

C. **Reporting of Votes.** The Chairman will report to the President, Executive Agent of the NISP, or other Government officials the results of Committee voting that pertain to the responsibilities of that official. In reporting or using the results of NISPPAC voting, the following terms shall apply: (1) Unanimous Decision. Results when every voting member,

except abstentions, is in favor of, or opposed to, a particular motion; (2) Government and Industry Consensus. Results when two-thirds of those voting, including two-thirds of all Government members and two-thirds of all industry members, are in favor of, or are opposed to, a particular motion; (3) General Consensus. Results when two-thirds of the total vote cast are in favor of, or are opposed to, a particular motion; (4) Government and Industry Majority. Results when the majority of the votes cast, including a majority of all Government members and a majority of all industry members, are in favor of or are opposed to a particular motion; (5) General Majority. Results when a majority of the total votes cast are in favor of or are opposed to a particular motion.

Article 6. Committee Officers and Responsibilities.

A. **Chairman.** As established by the Order, the Committee Chairman is the Director, ISOO. The Chairman will: (1) call meetings of the full Committee; (2) set the meeting agenda; (3) determine a quorum; (4) open, preside over and adjourn meetings; and (5) certify meeting minutes. The Chairman also serves as the Committee's DFO, a position required by the FACA.

B. **Designated Federal Officer.** The FACA requires each advisory committee to have a DFO and an alternate, one of whom must be present for all meetings. The Director and Associate Director, Operations and Industrial Security, ISOO, are, respectively, the DFO and alternate for the NISPPAC. Any meeting held without the DFO or alternate present will be considered as a subgroup or working group meeting.

C. **Executive Secretary.** The Executive Secretary shall be a member of the staff of the ISOO and shall be responsible for: (1) notifying members of the time and place for each meeting; (2) recording the proceedings of all meetings, including subgroups or working group activities that are presented to the full Committee; (3) maintaining the roll; (4) preparing the minutes of all meetings of the full Committee, including subgroups and working group activities that are presented to the full Committee; (5) attending to official correspondence; (6) maintaining official Committee records and filing all papers and submissions to the Committee, including those items generated by subgroups and working groups; (7) acting as Committee Treasurer to collect, validate and pay all vouchers for preapproved expenditures presented to the Committee; (8) preparing a yearly financial report; and (9) preparing and filing the annual Committee report as required by the FACA.

D. **Committee Staff.** The staff of the ISOO shall serve as the NISPPAC staff on an as needed basis, and shall provide all services normally performed by such staff, including assistance in the fulfilling of the functions of the Executive Secretary.

Article 7. Documents.

Documents presented to the Committee by any method at any time, including those distributed during the course of a meeting, are part of the official Committee files, and become agency records within the meaning of the FOIA, and are subject to the provisions of that Act. Documents originating with agencies of the Federal Government shall remain under the primary control of such agencies and will be on loan to the Committee. Any FOIA request for access to documents originating with any agency shall be referred to that agency. Documents originating with industry that have been submitted to the NISPPAC during the course of its official business shall also be subject to request for access under the FOIA. Proprietary information that may be contained within such documents should be clearly identified at the time of submission.

Article 8. Committee Expenses and Cost Accounting.

Committee expenses, including travel and per diem of non-Government members, will be borne by the ISOO to the extent of appropriated funds available for these expenditures. Cost accounting will be performed by the Committee's Executive Secretary. Expenditures by the Committee or any subgroup or working group must be approved in advance by the Chairman or the Executive Secretary.

Article 9. Amendment of Charter and Bylaws.

Amendments to the Charter and Bylaws of the Committee must conform to the requirements of the FACA and the Order and be agreed to by two-thirds of the 16 Government members or alternates and two-thirds of the eight industry members or alternates. Confirmed receipt of notification to all Committee members must be completed before any vote is taken to amend either the Charter or Bylaws.

Attachment #4

Proposed Change to NISPPAC Bylaws – Industry Spokesperson

Results of voting that took place during the meeting

Approval of the amendment requires agreement by two-thirds of the 16 Government members or alternates (11 needed to approve) and two-thirds of the 8 industry members (5 needed to approve).

Government

NISPPAC Chair	yes
DOE (alternate)	yes
DHS (member)	yes
Air Force (member)	yes
Navy (alternate)	yes
DSS (alternate)	yes
CIA (alternate)	yes
NSA (member)	yes
State Department (alternate)	yes

A member or alternate was not present from the following Government member agencies. An attendee representative voted to approve. The votes were confirmed by email by a member or alternate of the agency subsequent to the meeting.

ODNI (member)
DoD (alternate)
NRC (alternate)
Department of Justice (member)
Army (alternate)

The following agency member was present by phone but did not submit a vote:

NASA

The following member agency was not present at the meeting:

Department of Commerce

Result: 14 Government members or alternates (representing more than 2/3 of the Government membership) voted to approve the amendment.

Industry

Members present and voting to approve:

Michelle Sutphin
Bill Davidson
Phil Robinson
Quinton Wilkes
Bob Harney
Dennis Keith (by phone)

Result: Six of the eight industry members (representing more than 2/3 of the industry membership) voted to approve the amendment.

The amendment is approved for inclusion in the bylaws.

Attachment #5

B. (rewritten) Nominations. The Chairman solicit and accept nominations for Committee membership: (1) for representatives of the respective agencies, from the agency head: and (2) for non-government representatives, from the NISPPAC industry spokesperson designated in accordance with Article 3, paragraph E. Although a non-government representative does not represent his or her employing company, the Chairman will solicit the approval of the chief executive official of that company to allow the nominated individual to serve on the NISPPAC.

C. (new) Nomination Process for Non-government Representatives.

The NISPPAC industry spokesperson will solicit nominations from the other non-government members of the Committee and from the governing boards of professional, trade and other organizations whose membership is substantially comprised of employees of business concerns involved with classified contracts, licenses, or grants.

The nomination process will allow sufficient time to ensure that two incoming non-government NISPPAC members are in place by Oct. 1 of each year to replace the two outgoing non-government members.

Each non-government NISPPAC member and aforementioned professional and trade organizations will be permitted to submit a nomination to replace the two outgoing NISPPAC members whose terms end on Sept. 30 of the current year. The nominations from such professional and trade organizations must be endorsed by the board of the nominating organization. No such endorsement is necessary for nominations submitted by the current NISPPAC non-government members.

Nomination packages must include a resume, at minimum, and any other information that supports a nominee's qualifications for NISPPAC membership.

The NISPPAC industry spokesperson will convene a panel comprised of non-government NISPPAC members to review the submitted nomination packages.

The panel will rank the submitted nomination packages based on criteria that they determine, but that ensures alignment with the criteria established in paragraph 12 of the NISPPAC charter for non-government members. This includes the requirements that (1) non-government members represent all types and sizes of NISP contractor entities, whose scope of operations range from a one person entity having a single classified contract to some of the largest U.S. corporations, having numbers of classified contracts; and (2) that non-government members have expertise in carrying out the primary functions of an industrial security program.

While non-government NISPPAC members represent all of industry and do not represent their company organizations, nominees who are employed by a company that already has current representation on the NISPPAC will not be considered. Similarly, if a non-government member becomes an employee of a company that already has a member on the committee, one of those two members will resign. The spokesperson will solicit a new nominee to replace the resigning members and submit the nomination to the committee chair for consideration.

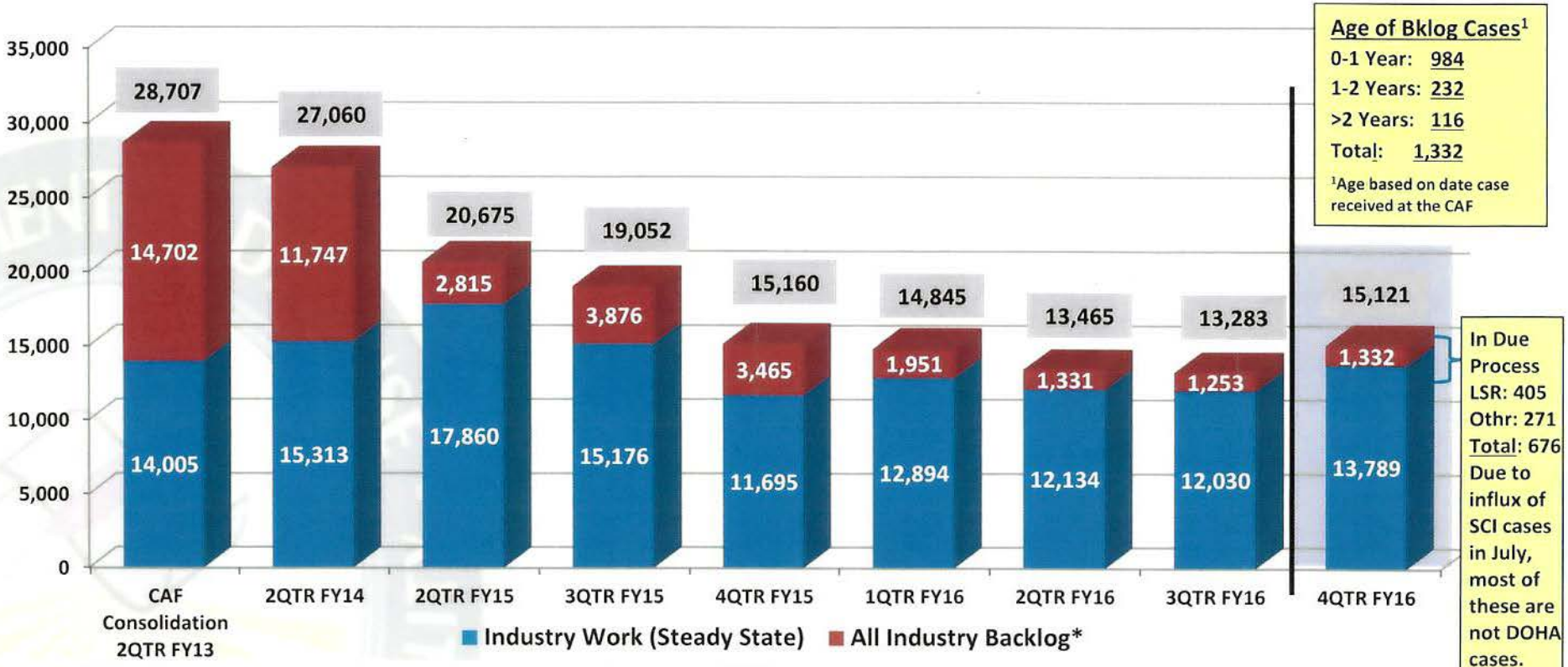
At the conclusion of panel deliberations, the NISPPAC industry spokesperson submits a copy of all submitted nomination packages to the NISPPAC chair, along with an endorsement of two nominees for the NISPPAC chair's consideration for NISPPAC membership. The industry spokesperson submits the nomination packages and endorsements to the NISPPAC chair no later than September 1 of each year.

The NISPPAC Chairman will request management approval from the employing companies of the two endorsed nominees for their participation on the NISPPAC for a four-year period. If company management cannot approve participation of any nominee, that individual will not be further considered for NISPPAC membership. The NISPPAC Chairman will request that the panel endorse a replacement nominee from the pool of submitted nominations.

The NISPPAC Chairman is not obligated to select a panel-endorsed nominee, and may make alternative selections from the nomination pool. Such a determination by the Chairman should only be in exceptional circumstances, with rationale provided to the NISPPAC industry spokesperson.

Attachment #6

Industrial Cases Pending Adjudication



Age of Bklog Cases[1]
0-1 Year: 984
1-2 Years: 232
>2 Years: 116
Total: 1,332
[1]Age based on date case received at the CAF

In Due Process
LSR: 405
Othr: 271
Total: 676
Due to influx of SCI cases in July, most of these are not DOHA cases.

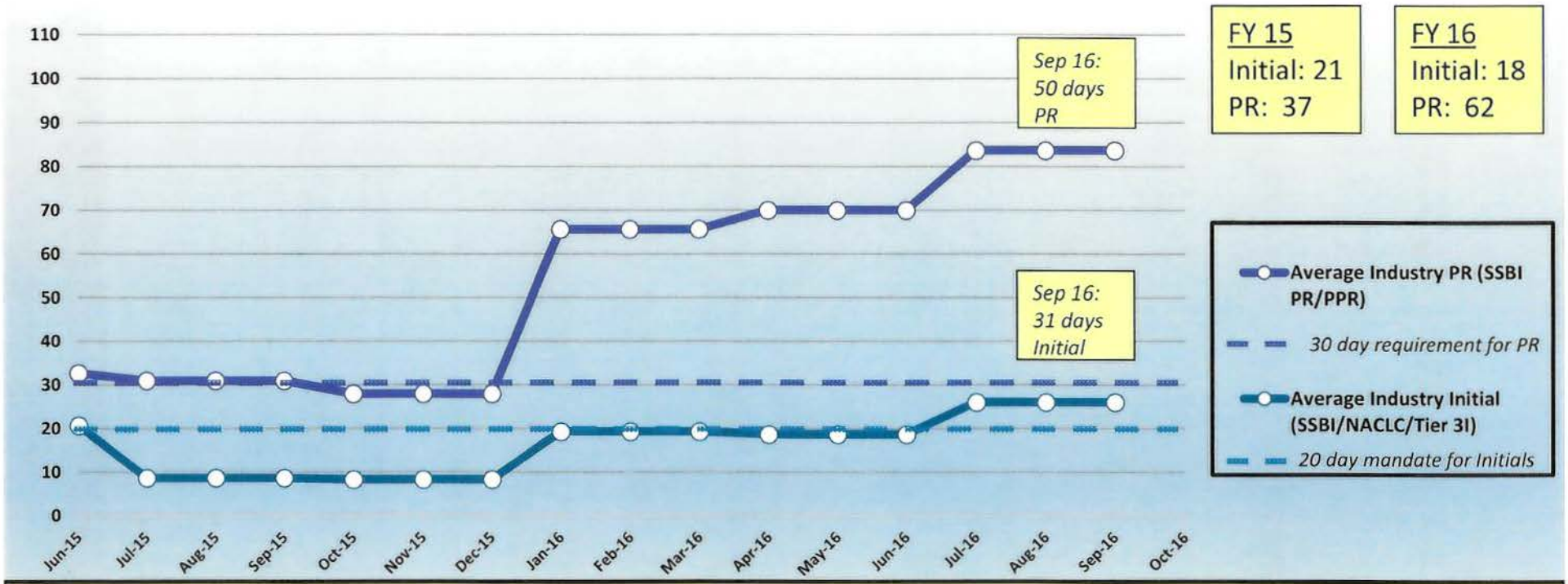
- **4QTR FY16 (highlighted bar): increase due to addition of DIA SCI cases and re-baselined calculations to include *all* Industrial SCI cases**
- **Non-DOHA SCI Backlog to be eliminated not earlier than 4QTR FY17**
- **DOHA backlog eliminated and LSRs are stabilized at well under 200**

Month	NISP Backlog	FY 16 NISP Receipt*	Backlog % of Total NISP
October 13	13,515		7.4%
September 16	1,332		0.7%
	-12,183	~ 183,000	

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

As Of: 30 September 2016

All Industry Cases
CAF Performance Jun 15-Sep 16



- Anticipate continued focus on initial investigations as the priority until the backlog is eliminated and CATSv4 implementation occurs. Timelines for Periodic Reinvestigations expected to remain high, especially for SCI.
- Spike in caseload during July through September of 2016 is the result of:
  - 4th Estate SCI/DIA case ingest which added many very dated SCI cases to the CAF industry workload
  - IT latency issues and challenges from legacy CATS, including not having e-Adjudication available during FY 2016
  - Increase in closed older cases--including older SCI cases gained by the CAF on July 1, 2016
  - Final determinations in JPAS on older Industry cases after being transferred to Non-CAF organizations (DIA, etc.)

As Of: 30 September 2016

Attachment #7

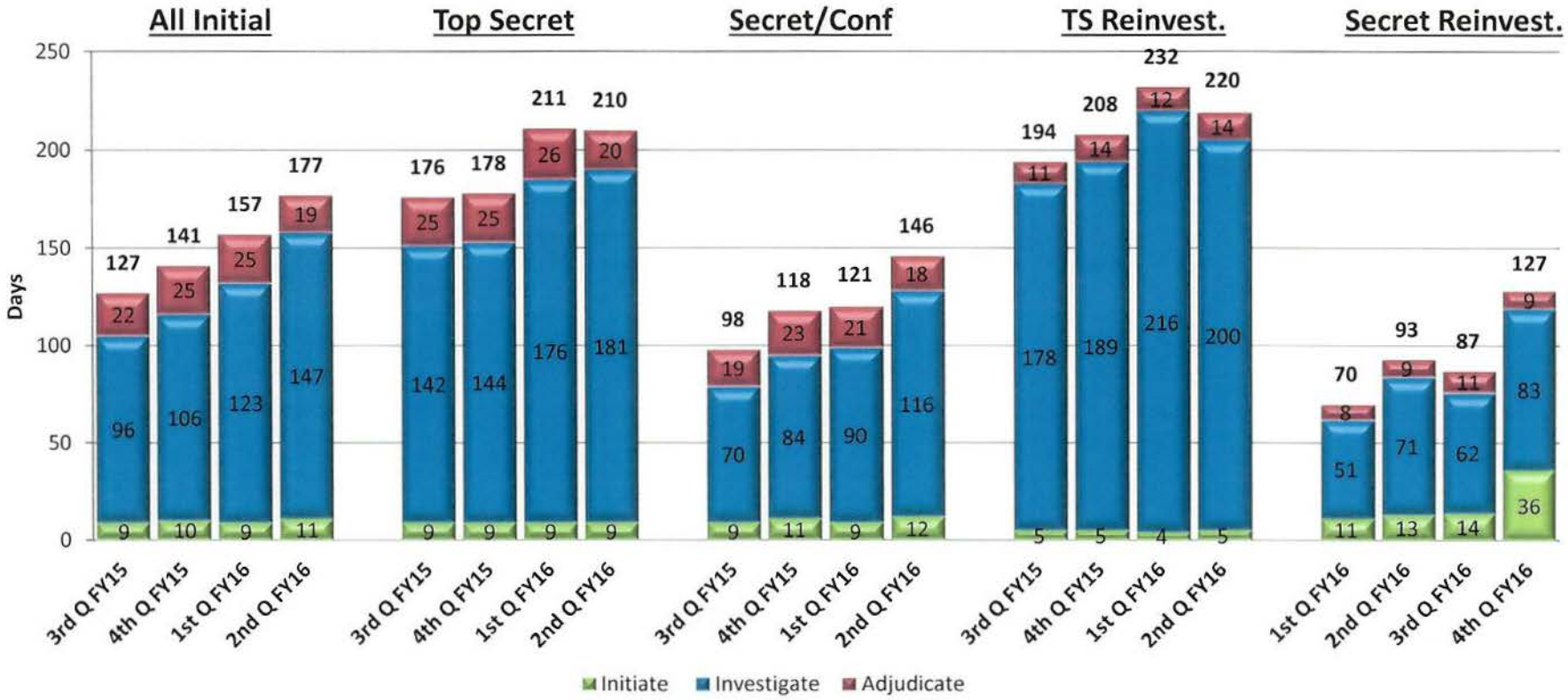
Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

DOE

October 2016

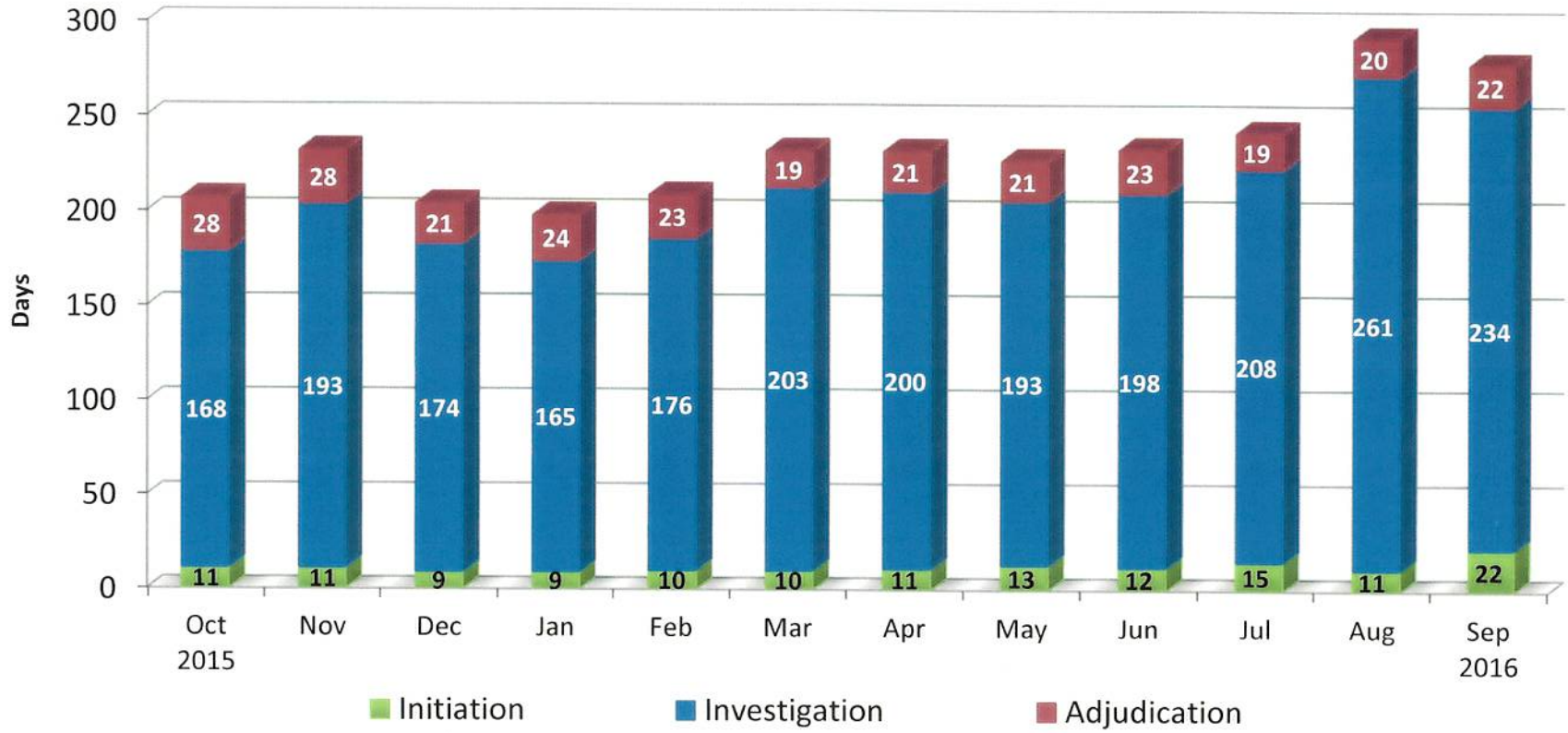
Quarterly Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations	Secret Reinvestigations
Adjudication actions taken – 1st Q FY16	1,569	649	920	2,198	96
Adjudication actions taken – 2nd Q FY16	1,206	601	605	1,921	309
Adjudication actions taken – 3rd Q FY16	1,536	745	791	1,855	672
Adjudication actions taken – 4th Q FY16	1,395	788	607	1,962	643

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



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

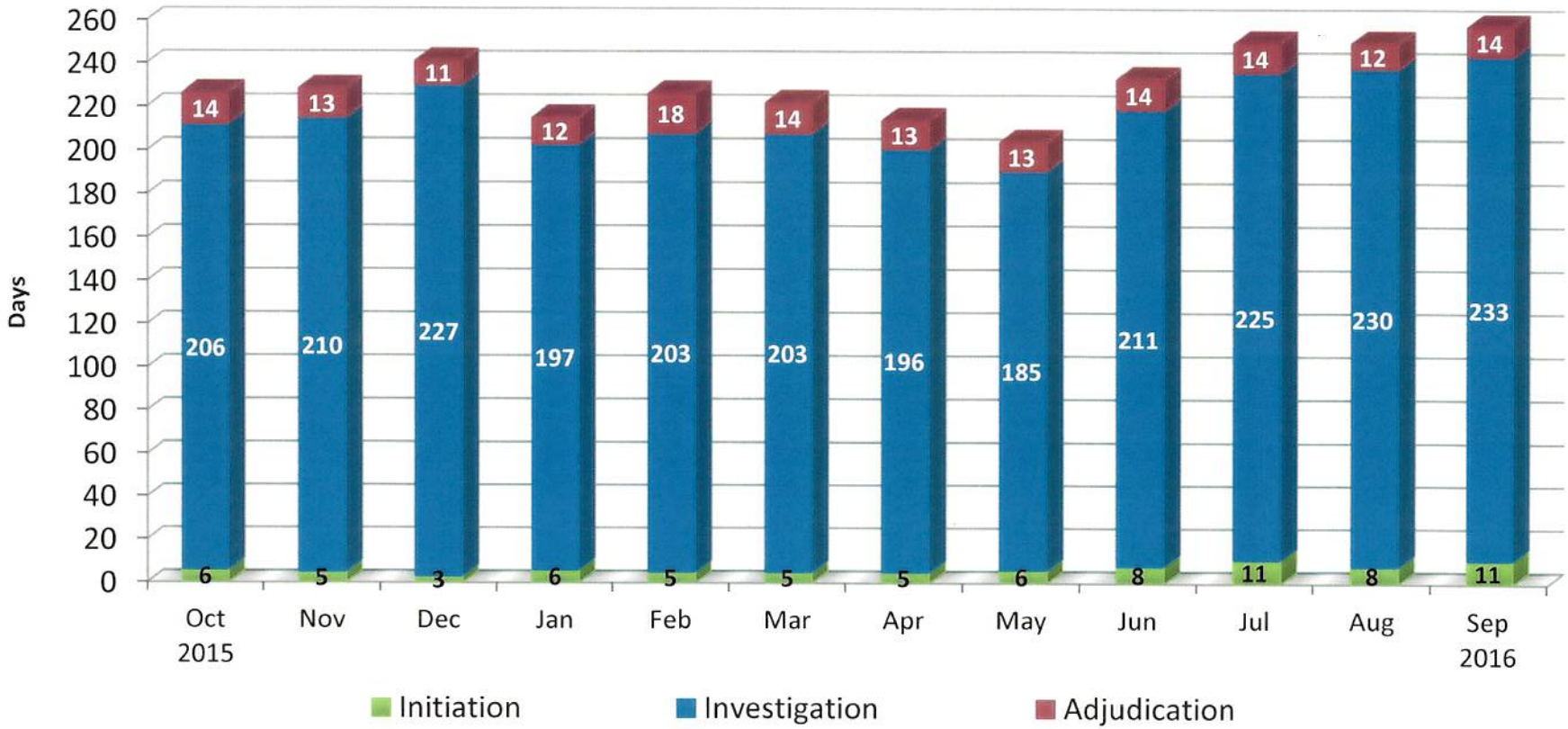
	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Mar 2016	Apr 2016	May 2016	Jun 2016	Jul 2016	Aug 2016	Sep 2016
100% of Reported Adjudications	233	178	228	171	206	240	229	271	242	244	274	265
Average Days for fastest 90%	207 days	232 days	204 days	198 days	209 days	232 days	232 days	227 days	233 days	242 days	292 days	278 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***

	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Mar 2016	Apr 2016	May 2016	Jun 2016	Jul 2016	Aug 2016	Sep 2016
100% of Reported Adjudications	355	249	278	183	200	254	209	274	299	242	201	146
Average Days for fastest 90%	123 days	112 days	124 days	145 days	138 days	166 days	159 days	152 days	148 days	150 days	165 days	194 days

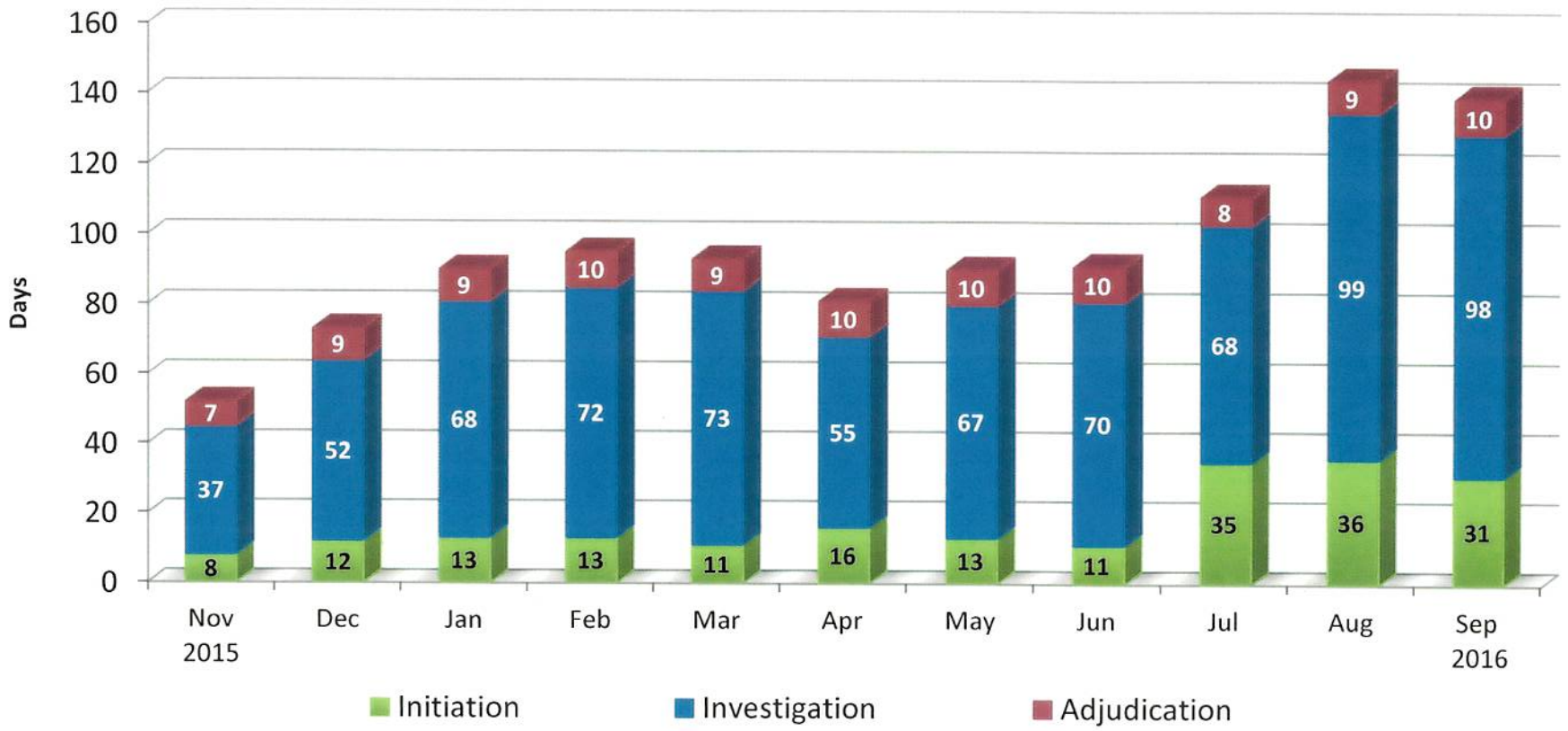
DOE's Average Timeliness Trends for 90%
Top Secret Reinvestigation Security Clearance Decisions



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

	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Mar 2016	Apr 2016	May 2016	Jun 2016	Jul 2016	Aug 2016	Sep 2016
100% of Reported Adjudications	617	726	844	546	647	744	680	671	497	555	738	660
Average Days for fastest 90%	226 days	228 days	241 days	215 days	226 days	222 days	214 days	204 days	233 days	250 days	250 days	258 days

DOE's Average Timeliness Trends for 90% Secret Reinvestigation Security Clearance Decisions (T3R)



	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Mar 2016	Apr 2016	May 2016	Jun 2016	Jul 2016	Aug 2016	Sep 2016
100% of Reported Adjudications	0	9	85	37	142	131	284	172	201	252	192	165
Average Days for fastest 90%	-	52 days	73 days	90 days	95 days	93 days	81 days	90 days	91 days	111 days	144 days	139 days

Attachment #8

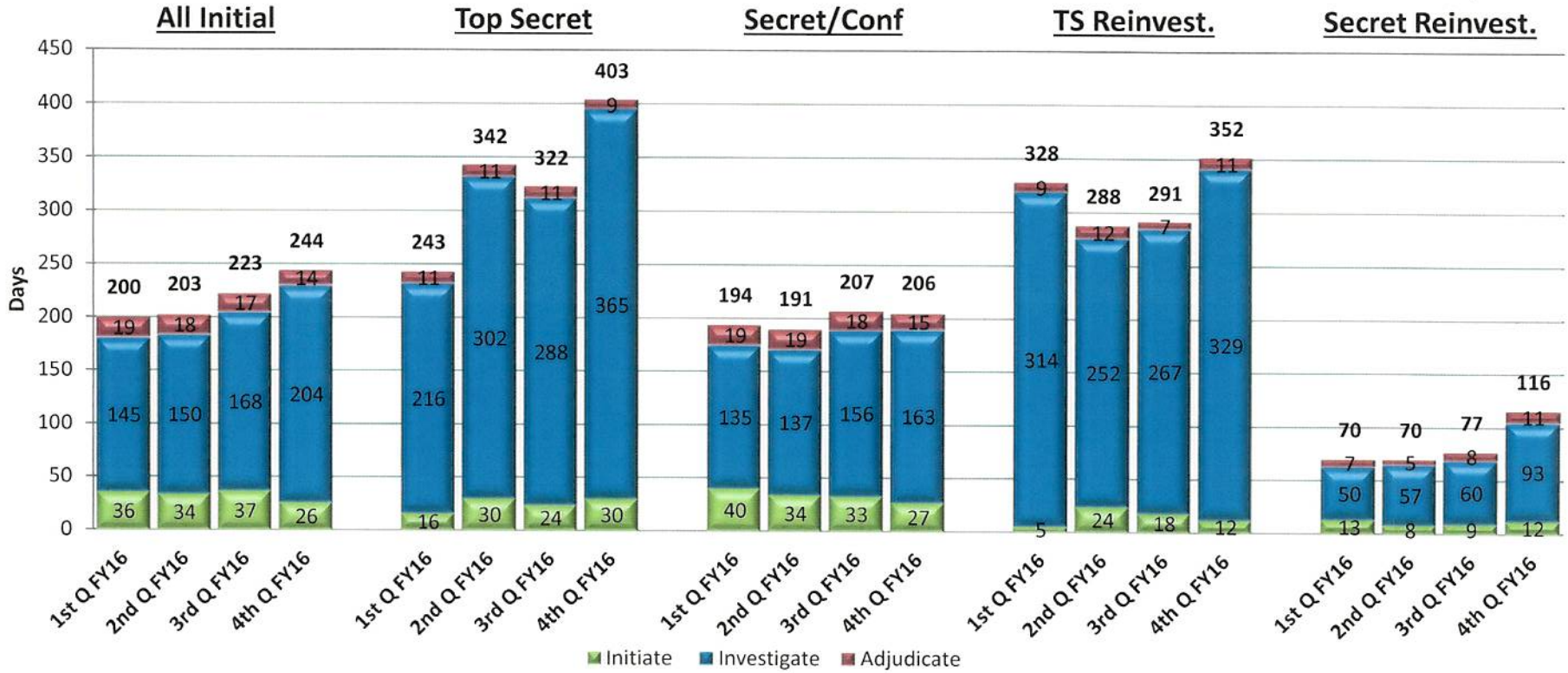
Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

NRC

October 2016

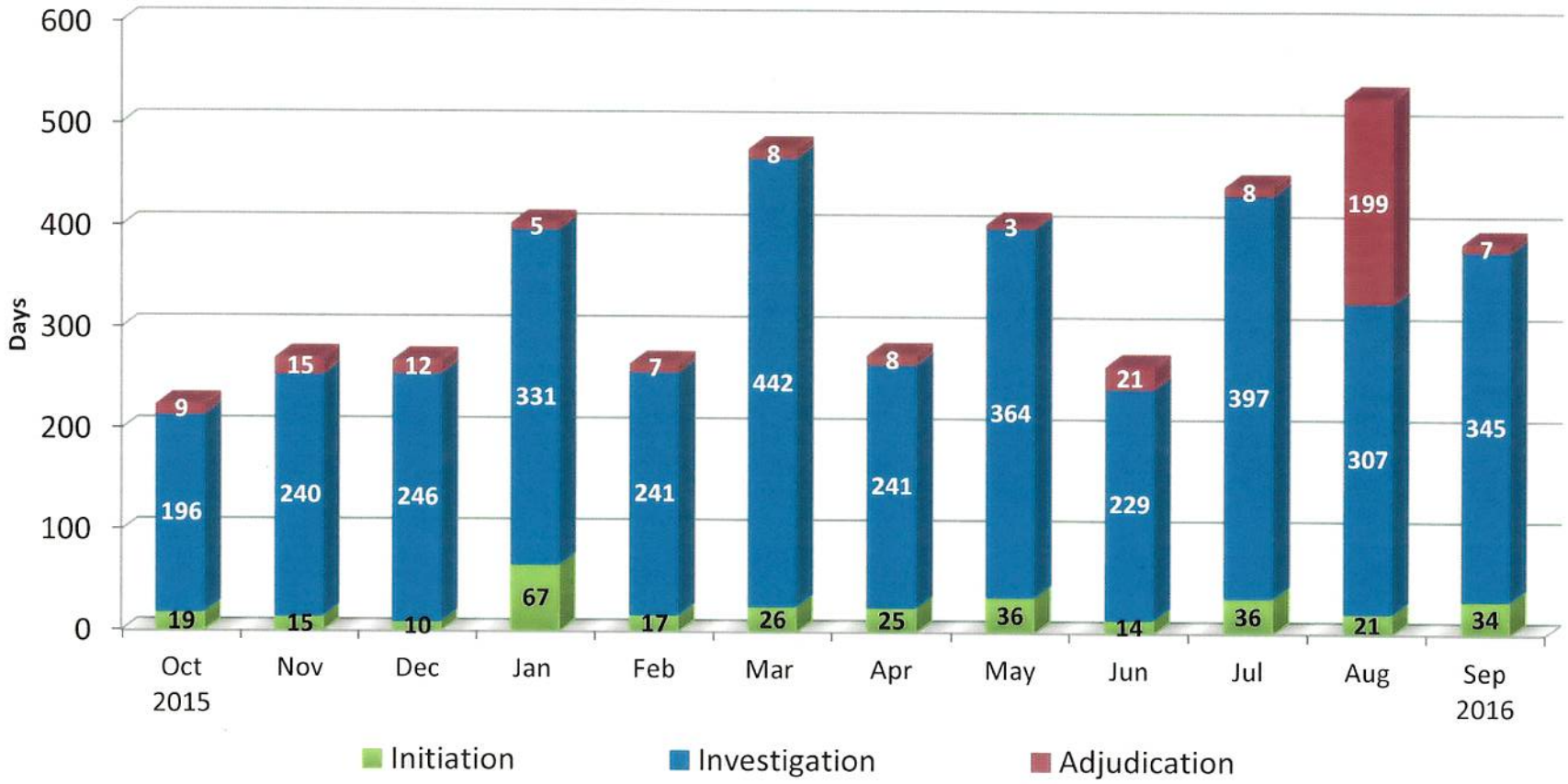
Quarterly Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations	Secret Reinvestigations
Adjudication actions taken – 1st Q FY16	108	12	96	17	3
Adjudication actions taken – 2nd Q FY16	84	9	75	33	71
Adjudication actions taken – 3rd Q FY16	102	15	87	20	44
Adjudication actions taken – 4th Q FY16	62	13	49	46	83

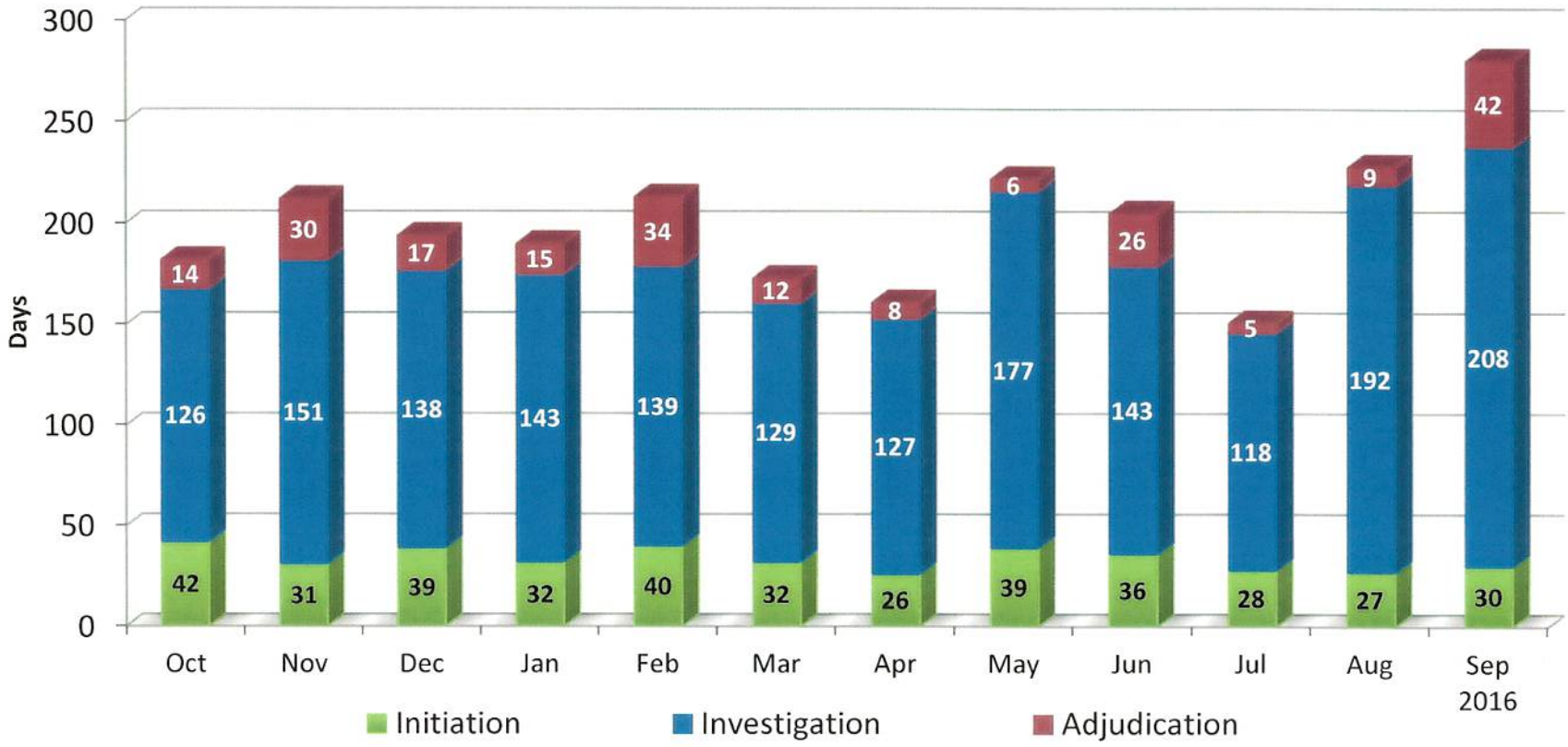
NRC's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



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

	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Mar 2016	Apr 2016	May 2016	Jun 2016	Jul 2016	Aug 2016	Sep 2016
100% of Reported Adjudications	5	4	3	1	4	3	6	4	6	3	5	5
Average Days for fastest 90%	224 days	270 days	268 days	403 days	265 days	476 days	274 days	403 days	264 days	441 days	527 days	386 days

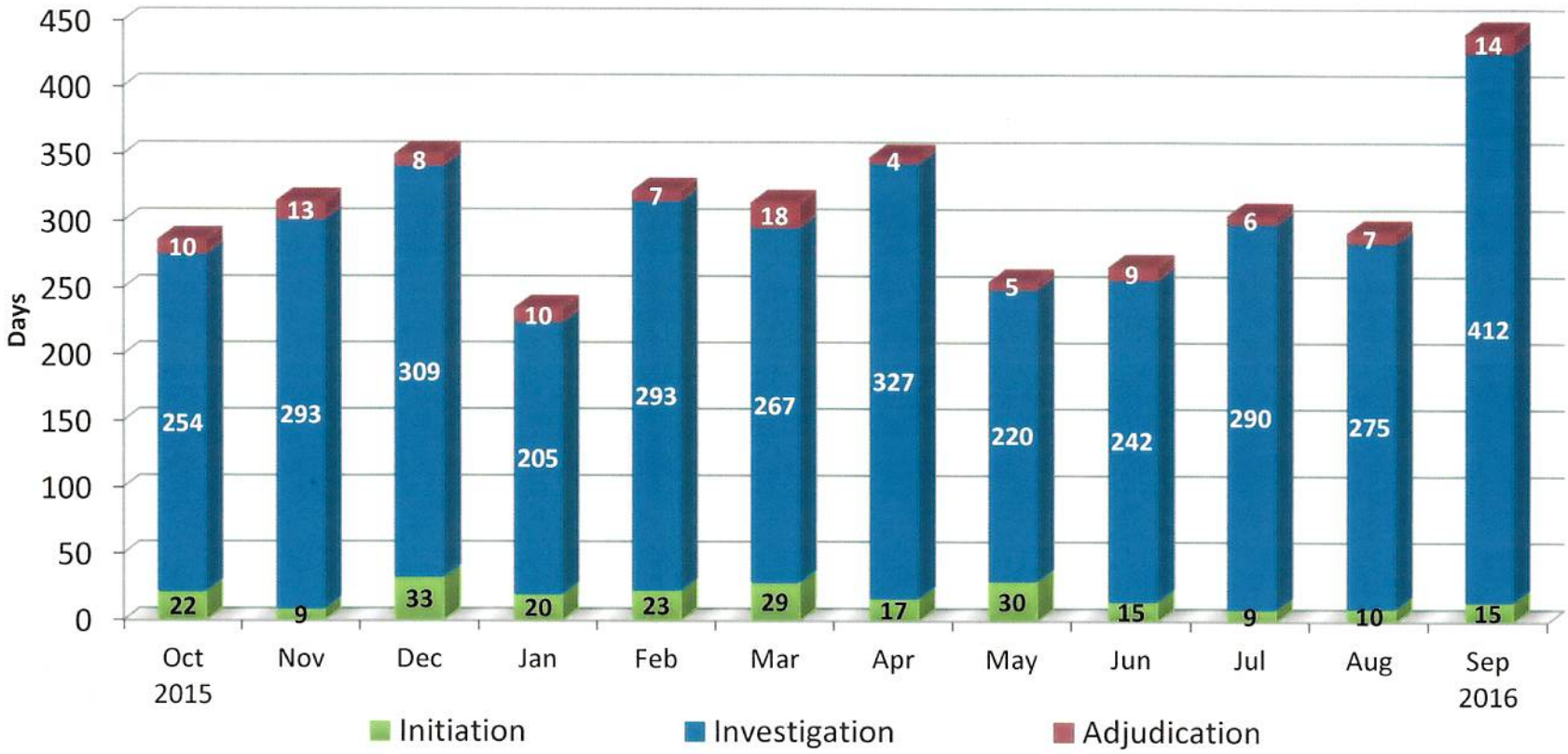
NRC's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions (NACLC/ANACI/T3)



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

	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Mar 2016	Apr 2016	May 2016	Jun 2016	Jul 2016	Aug 2016	Sep 2016
100% of Reported Adjudications	38	28	31	18	26	32	19	30	37	21	17	11
Average Days for fastest 90%	182 days	212 days	194 days	190 days	213 days	173 days	161 days	222 days	205 days	151 days	228 days	280 days

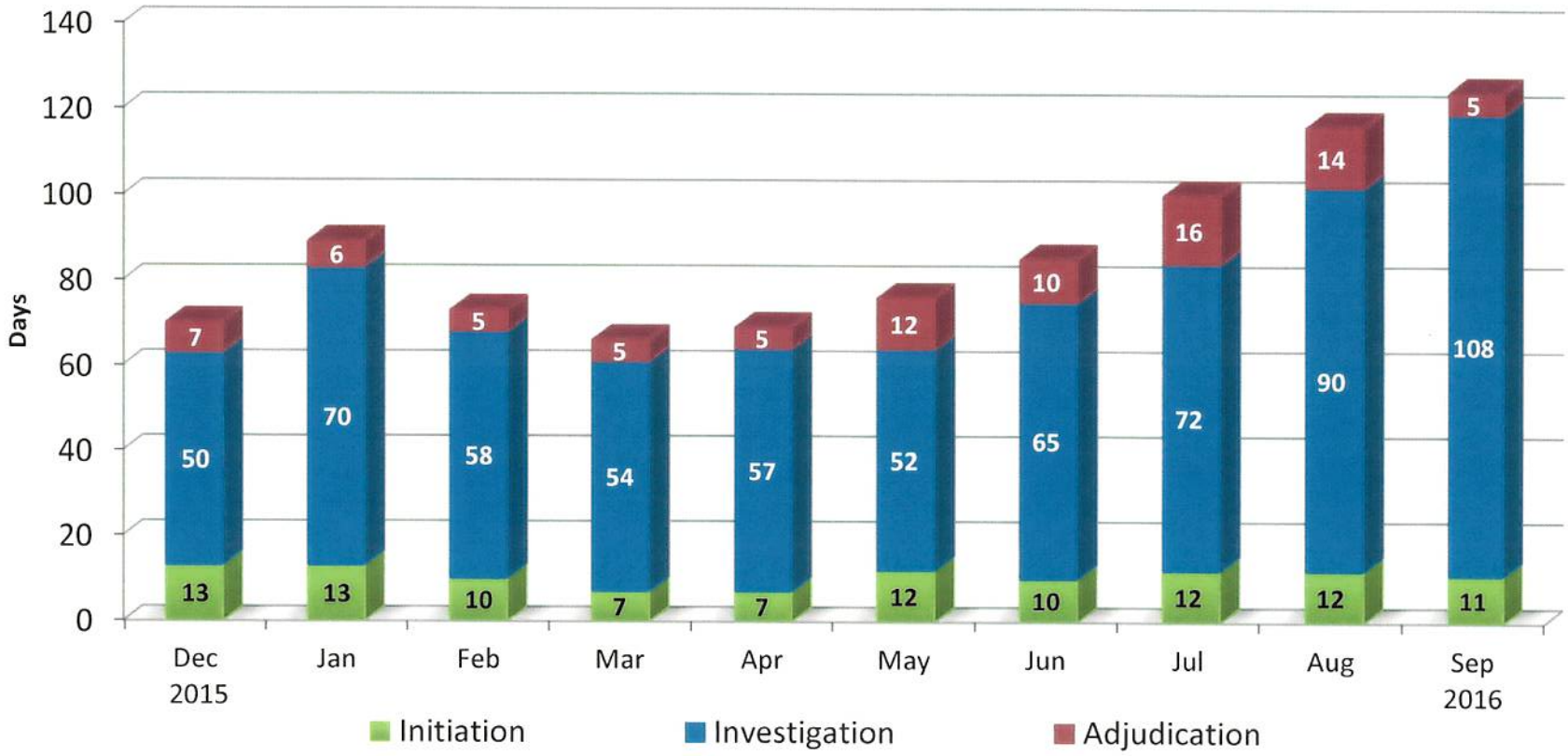
NRC's Average Timeliness Trends for 90%
Top Secret Reinvestigation Security Clearance Decisions



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

	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Mar 2016	Apr 2016	May 2016	Jun 2016	Jul 2016	Aug 2016	Sep 2016
100% of Reported Adjudications	4	2	10	12	10	11	7	3	10	12	14	19
Average Days for fastest 90%	286 days	315 days	350 days	235 days	323 days	314 days	348 days	255 days	266 days	305 days	292 days	441 days

NRC's Average Timeliness Trends for 90% Secret Reinvestigation Security Clearance Decisions (T3R)



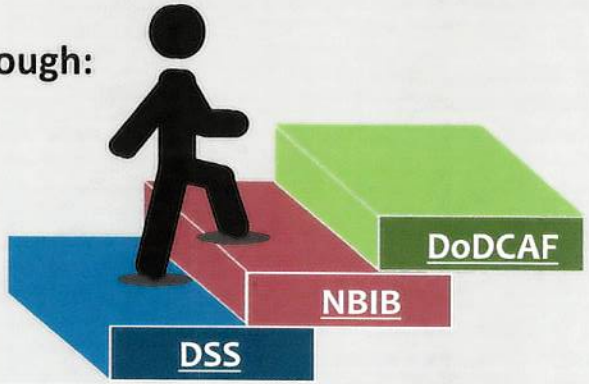
	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Mar 2016	Apr 2016	May 2016	Jun 2016	Jul 2016	Aug 2016	Sep 2016
100% of Reported Adjudications	0	0	3	3	33	35	20	7	16	21	26	36
Average Days for fastest 90%	-	-	70 days	89 days	73 days	66 days	69 days	76 days	85 days	100 days	116 days	124 days

Attachment #9

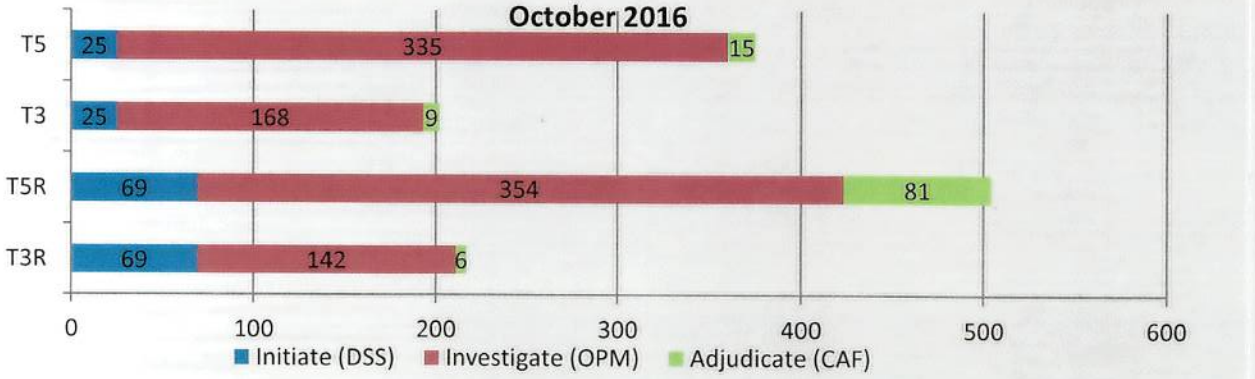
State of Play - Personnel Security Investigations (PSI)

Addressing the PSI-I Shortfalls - Short term & sustainable solutions through:

- ✓ **Critical Priority Requests (CPR)**
- ✓ **Expeditious processing for interim determinations**



Industry Personnel Clearance Timeliness



DSS - Review e-QIP for completeness and submittal to NBIB

NBIB - Schedules and completes investigation

DoDCAF - Reviews completed investigation against adjudicative guidelines

Attachment #10

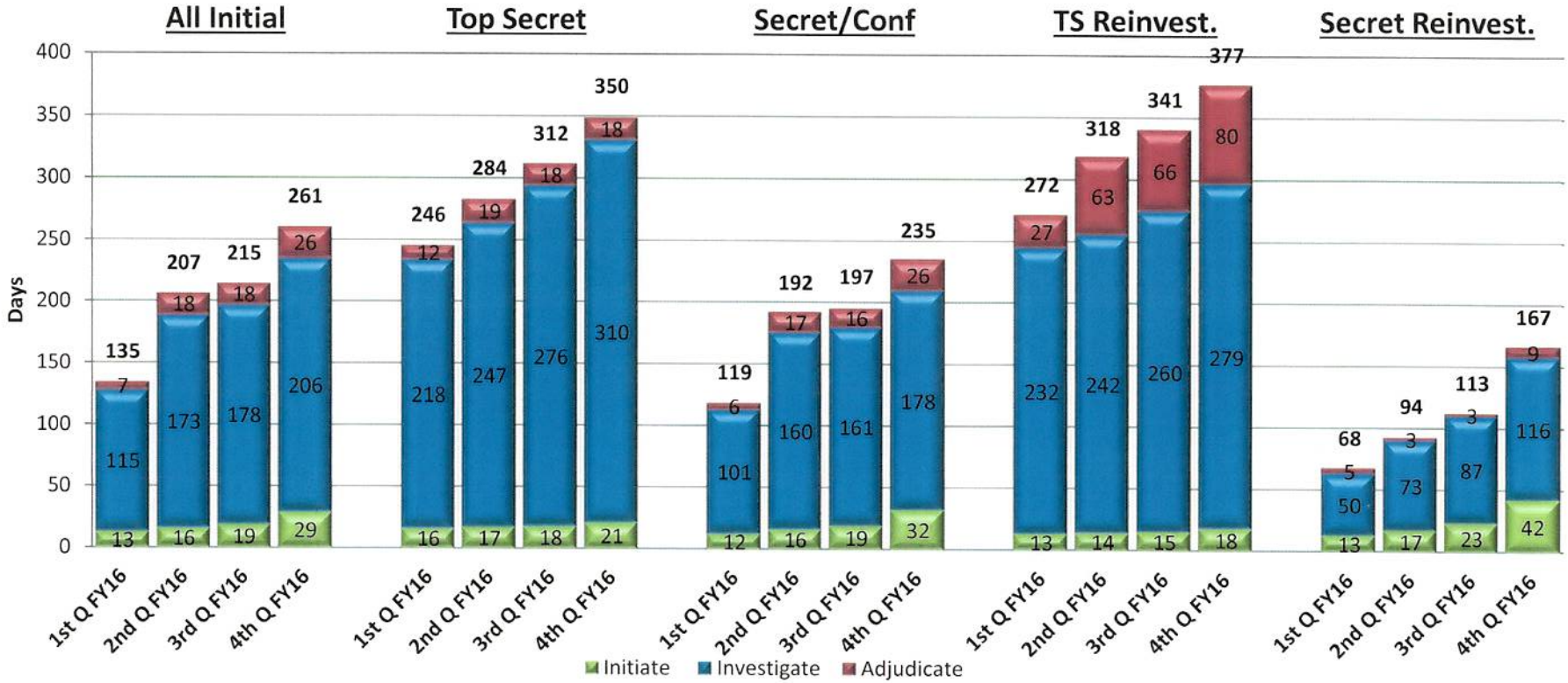
Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

DoD-Industry

November 2016

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

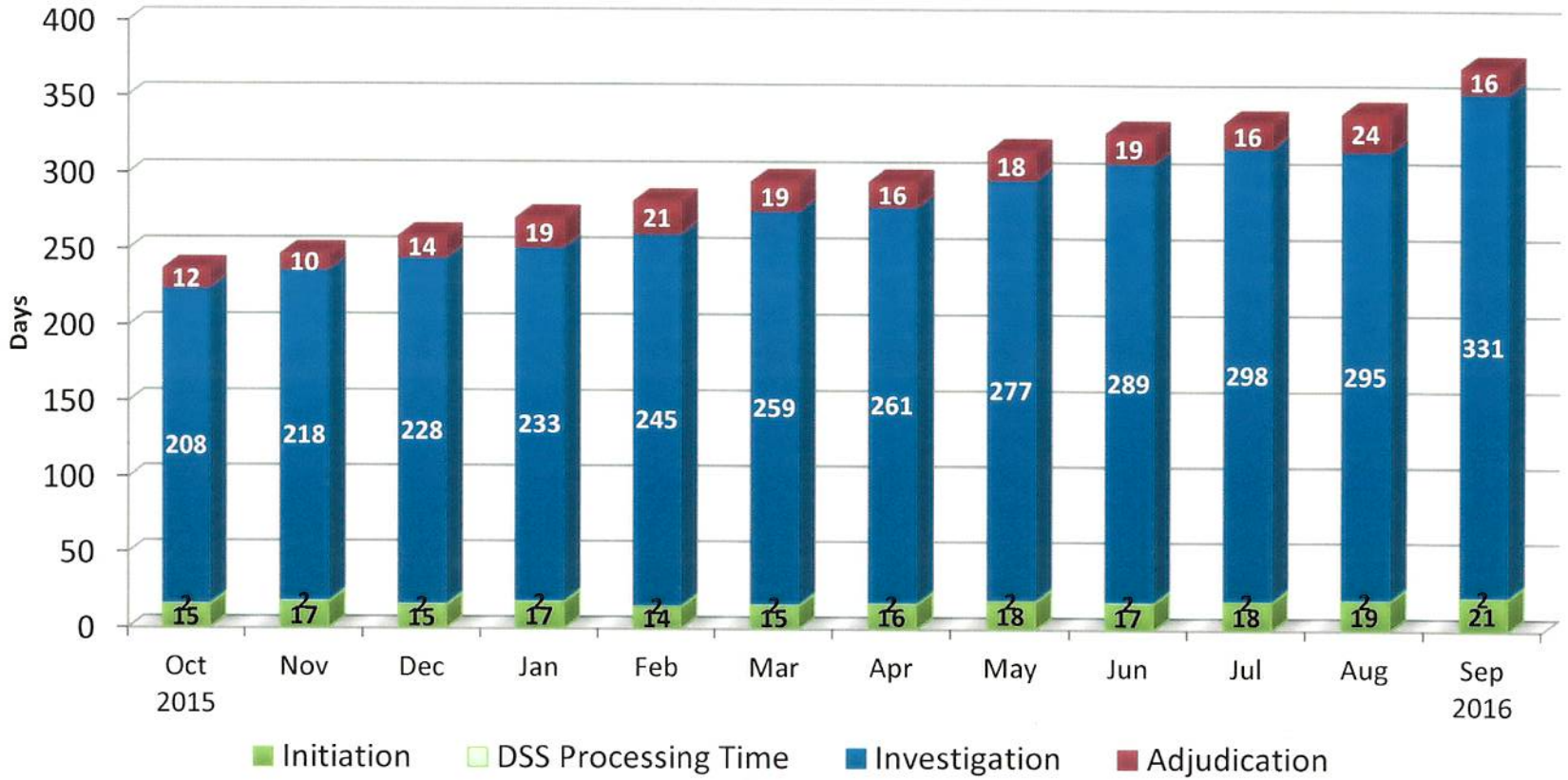
Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations	Secret Reinvestigations
Adjudication actions taken – 1st Q FY16	16,262	2,125	14,137	7,459	1,879
Adjudication actions taken – 2nd Q FY16	12,809	2,085	10,724	7,300	4,354
Adjudication actions taken – 3rd Q FY16	13,455	2,230	11,225	7,710	3,849
Adjudication actions taken – 4th Q FY16	10,265	2,310	7,955	7,770	3,257

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

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



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

	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Mar 2016	Apr 2016	May 2016	Jun 2016	Jul 2016	Aug 2016	Sep 2016
100% of Reported Adjudications	795	646	699	581	741	764	721	759	755	697	681	935
Average Days for fastest 90%	237 days	247 days	259 days	271 days	282 days	295 days	295 days	315 days	327 days	334 days	340 days	370 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***

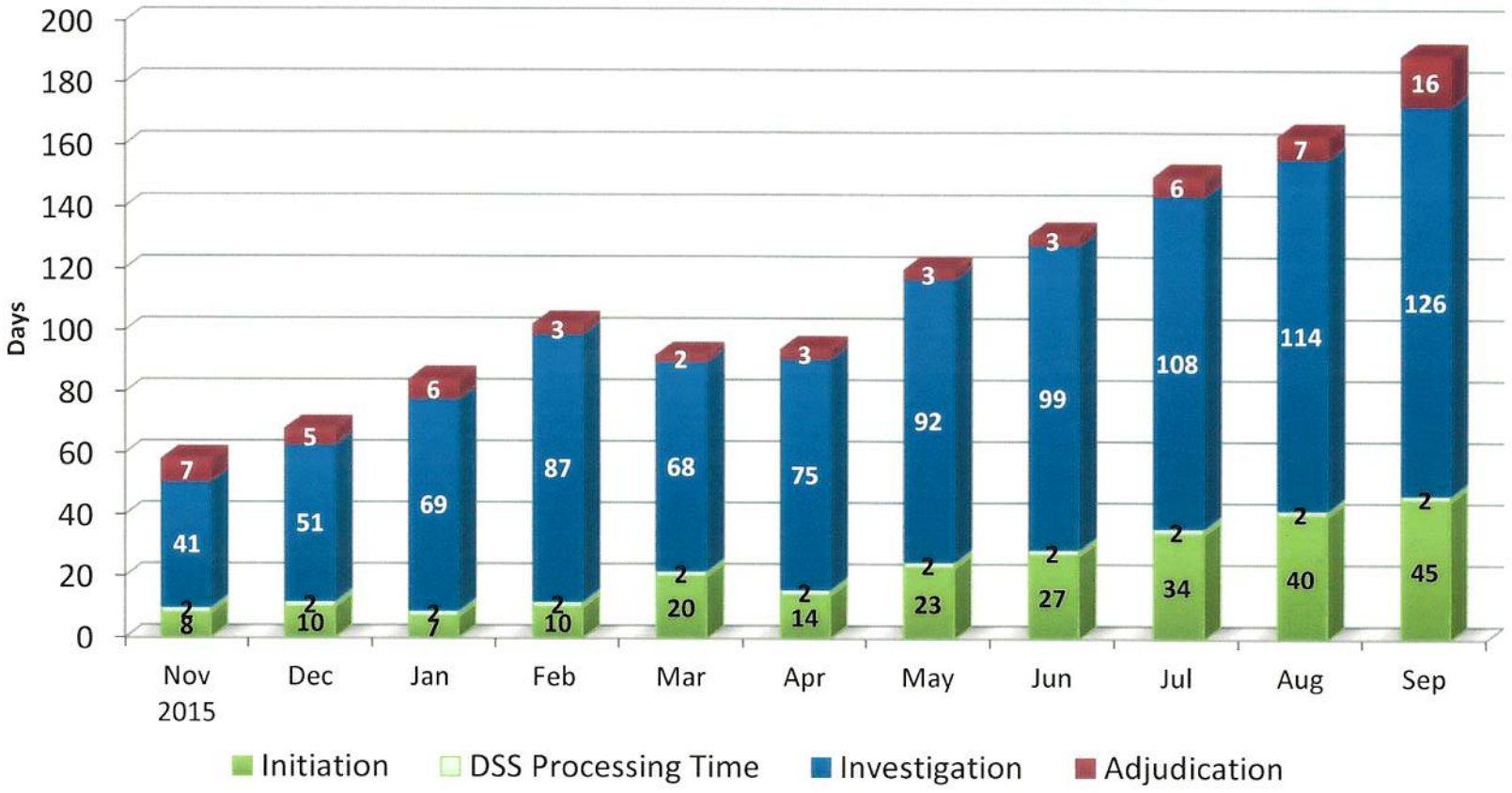
	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Mar 2016	Apr 2016	May 2016	Jun 2016	Jul 2016	Aug 2016	Sep 2016
100% of Reported Adjudications	6,718	4,046	3,430	3,634	3,206	3,893	3,464	3,582	4,188	2,352	3,413	2,191
Average Days for fastest 90%	100 days	121 days	162 days	173 days	208 days	198 days	189 days	198 days	201 days	233 days	226 days	253 days

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

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

	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Mar 2016	Apr 2016	May 2016	Jun 2016	Jul 2016	Aug 2016	Sep 2016
100% of Reported Adjudications	2,266	2,479	2,753	2,221	2,222	2,870	2,635	2,568	2,519	2,627	2,436	2,710
Average Days for fastest 90%	298 days	268 days	257 days	283 days	318 days	355 days	312 days	327 days	392 days	370 days	409 days	359 days

Industry's Average Timeliness Trends for 90%
Secret Reinvestigation Security Clearance Decisions (T3R)



	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Mar 2016	Apr 2016	May 2016	Jun 2016	Jul 2016	Aug 2016	Sep 2016
100% of Reported Adjudications	0	114	1,765	787	1,391	2,185	1,532	1,122	1,195	762	1,489	1,008
Average Days for fastest 90%	-	58 days	68 days	84 days	102 days	92 days	94 days	120 days	131 days	150 days	163 days	189 days

Attachment #11

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

INDUSTRY PERFORMANCE METRICS

NCSC/Special Security Directorate

LEADING INTELLIGENCE INTEGRATION

Gary Novotny

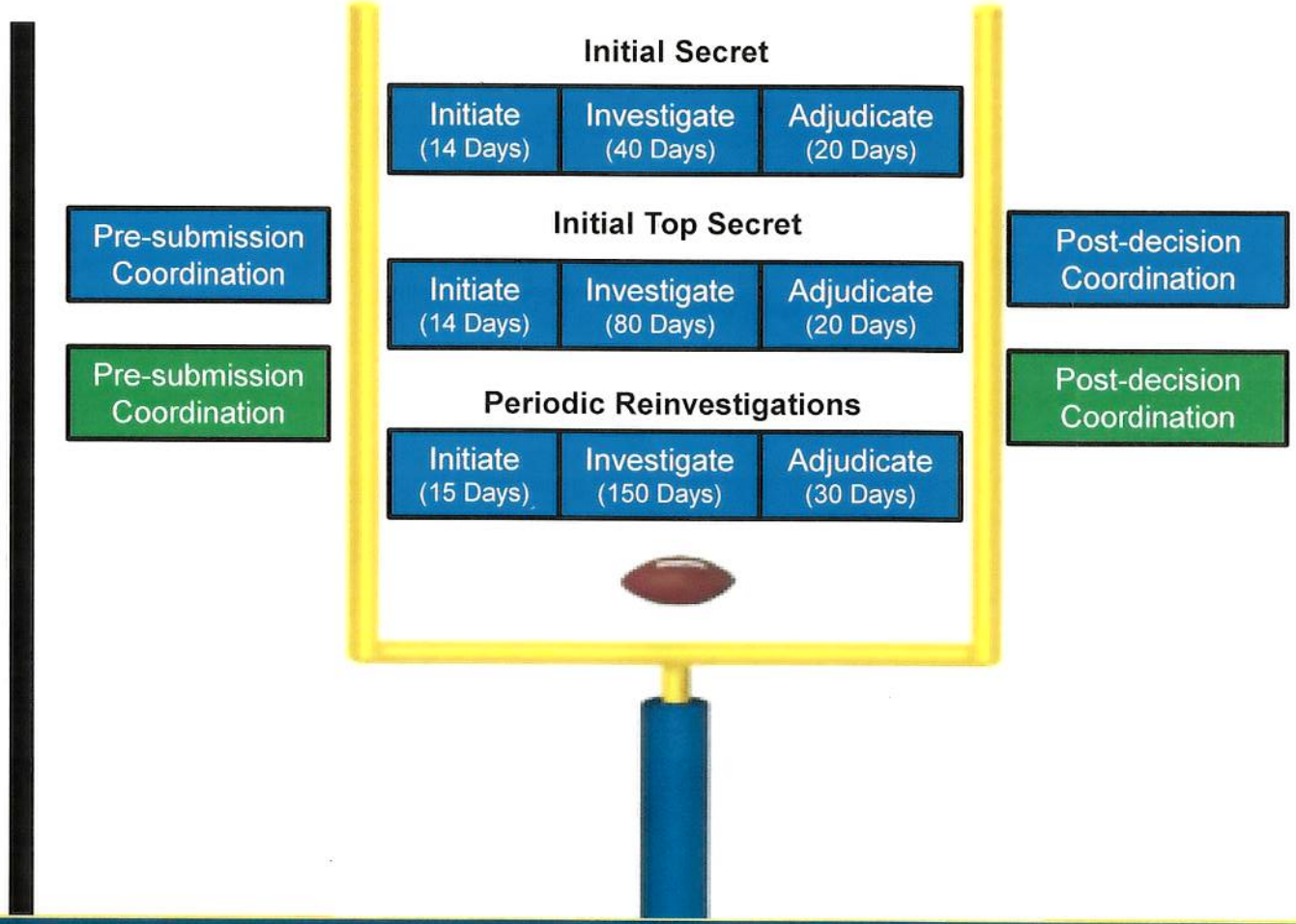
Briefing to NISPPAC

November 10, 2016

UNCLASSIFIED

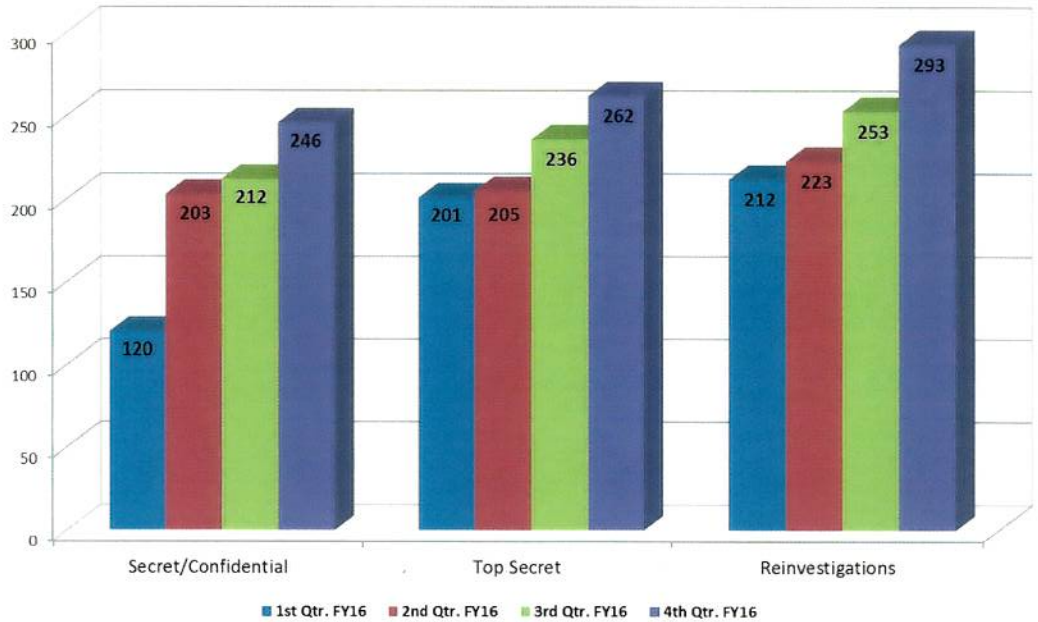
Performance Accountability Council (PAC) Security Clearance Methodology

- 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
- Unless otherwise specified, Initial Secret data is a combination of Legacy investigative types and Tier 3 investigations.



Timeliness Performance Metrics for IC/DSS
Industry Personnel Submission, Investigation & Adjudication* Time

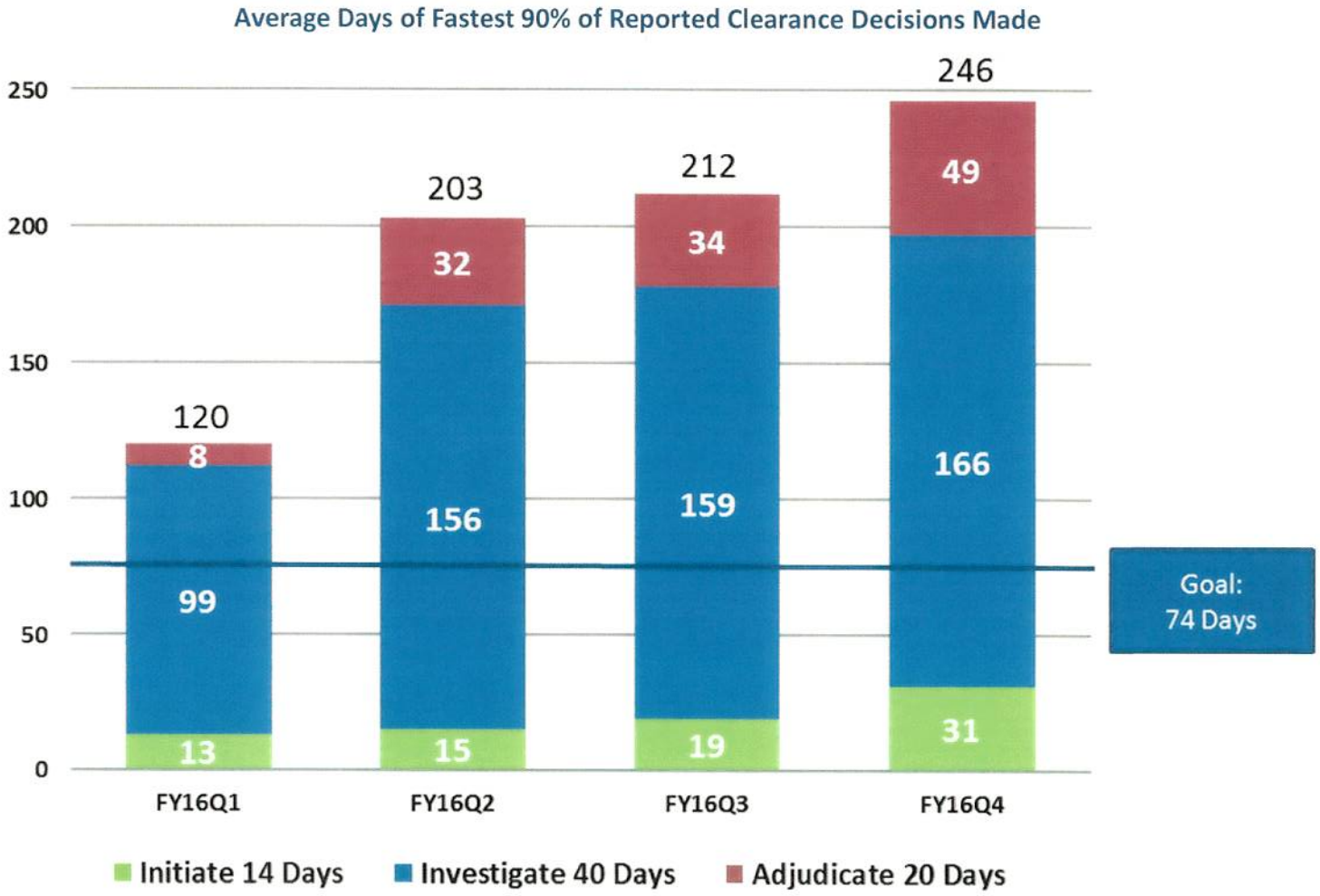
Average Days of Fastest 90% of Reported Clearance Decisions Made



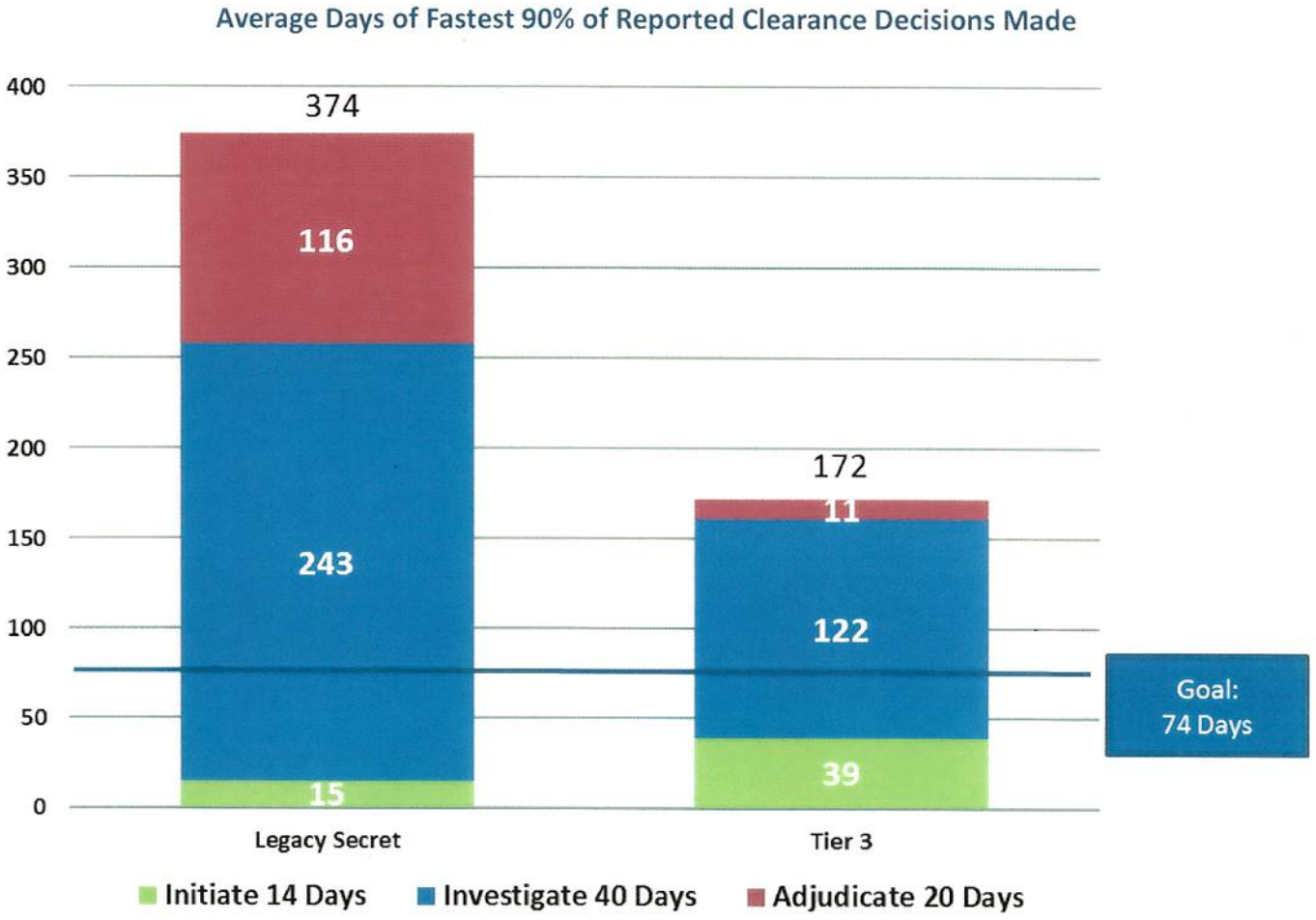
	Secret/ Confidential	Top Secret	Periodic Reinvestigations
Adjudication actions taken – 1st Q FY16	14,776	3,624	12,315
Adjudication actions taken – 2nd Q FY16	11,340	4,176	14,110
Adjudication actions taken – 3rd Q FY16	11,820	3,857	13,356
Adjudication actions taken – 4th Q FY16	8,697	4,145	12,995

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

IC and DoD Industry – Secret Clearances

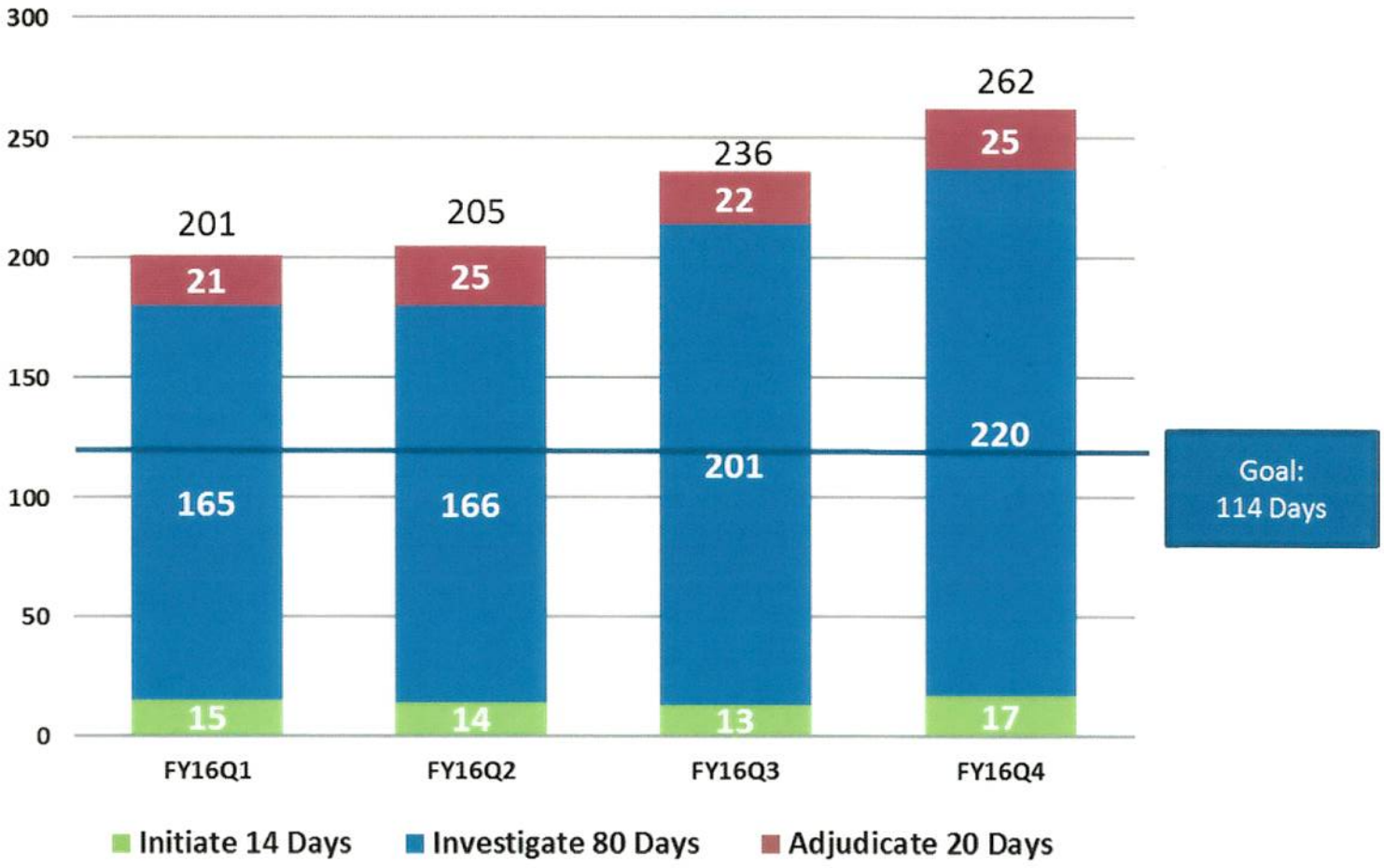


IC and DoD Industry – Legacy Secret vs Tier 3 (FY16 Q4)

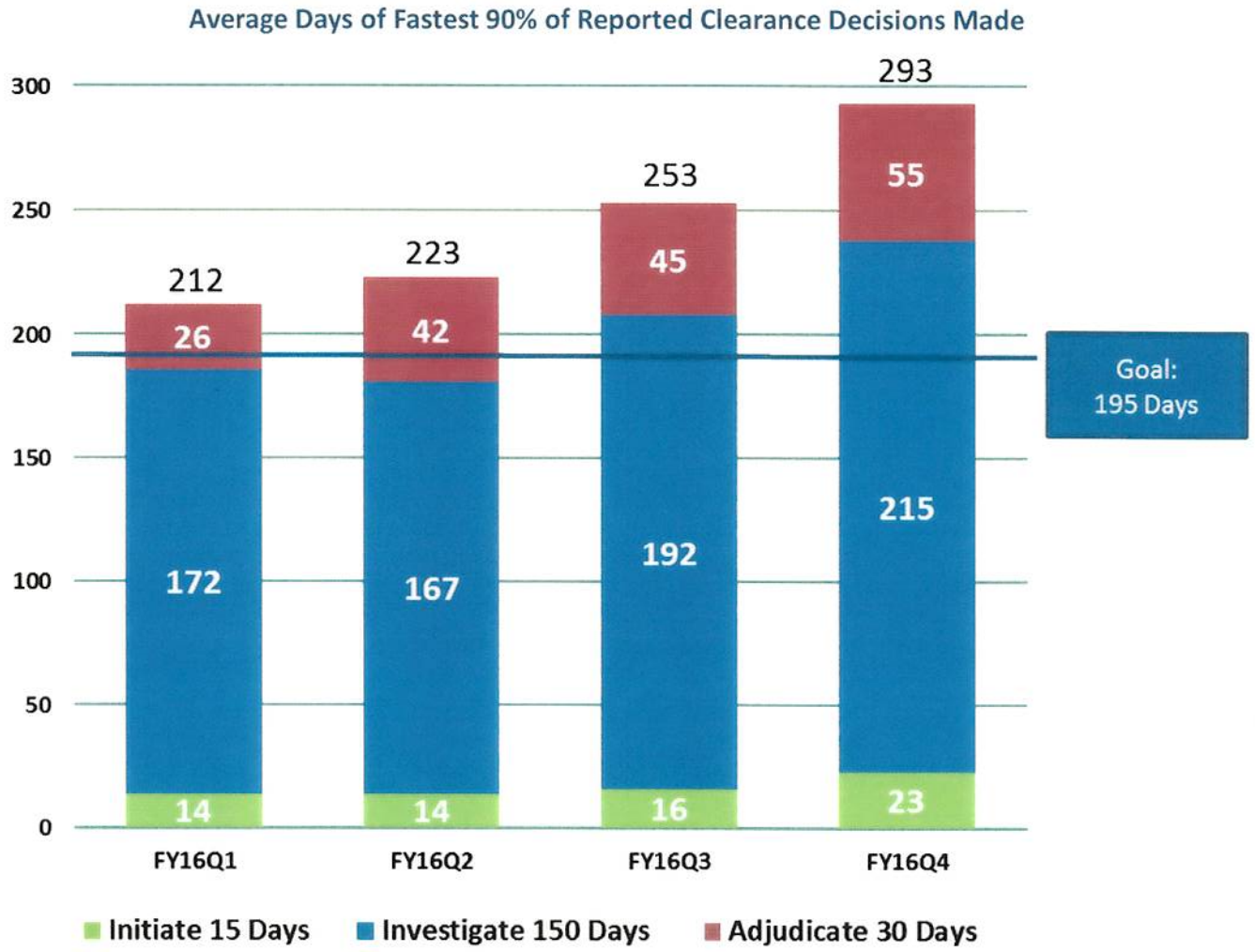


IC and DoD Industry - Top Secret Clearances

Average Days of Fastest 90% of Reported Clearance Decisions Made



IC and DoD Industry - Periodic Reinvestigations



Other Security Executive Agent Initiatives

- e-Adjudication Business Rules for Tier 3 and Tier 3 Reinvestigations approved and distributed
  - DoD currently implementing in a phased approach
- Quality Assessment Standards and Implementation Plan
- Quality Assessment Reporting Tool
  - ODNI received Authorization to Operate on 27 October 2016
  - ODNI Launched tool on 9 November 2016
  - Collection of government-wide quality standards will begin

Questions?

- Gary Novotny
  Chief, Security Oversight Branch
  NCSC/SSD/PSG
  Phone: 301-243-0462
  Email: Garymn@dni.gov
- Diane Rinaldo
  Metrics POC
  Phone: 301-243-0464
  Email: SecEAmetrics@dni.gov
- General Inquiries
  Email: SecEA@dni.gov

Attachment #12

NISPPAC Information Systems Authorization Working Group

A. Purpose

Promote community (CSA/CSO, industry, ISOO, SAP, Intel, etc.) coordination in the development and refinement of processes used in assessing and authorizing classified information systems which are consistent throughout the NISP and where applicable aligned with federal requirements.

A. Scope

The WG shall:

- Recommend standardized metrics used for measuring the timeliness of processes with the purpose of identifying and reporting goal satisfaction and process improvement areas.
- Develop and review proposed changes to processes, tools, templates, etc. to facilitate community accepted standards, best practices, consistency, and reciprocity across the NISP.
- Review and provide comment to policy revisions and changes as they are related to NISP information systems processes.
- Assist in the development and release of training material as they relate to the above for the NISP community.

Attachment #13

Defense Security Service

C&A Working Group Update

November 2016

DSS Risk Management Framework (RMF) Transition Update

- **DSS Assessment and Authorization Process Manual (DAAPM)**
  - DAAPM released August 25, 2016
  - Phased Implementation for Stand-alones effective October 3, 2016
  - DSS will re-assess the RMF transition plan in the December/January timeframe
- **System Security Plan (SSP) Template**
  - DSS delivered an improved streamlined SSP Template to working group for coordination
  - After working group review, the revised SSP template will be released to the Community

DSS Industrial Operations (IO) Preparedness for RMF

- Outreach to Industry (2016)
  - 70+ RMF briefings conducted throughout the country to industry partners (NCMS; ISAC; Corporate security events).

- ISSP Training (2016)
  - HQ DSS conducted (2) RMF Training workshops specific to the ISSP roles and responsibilities hosted at CDSE.
    - Capital & Southern Region 13-15 September
    - Northern & Western Region 20-22 September

ISSM Training and Preparedness for RMF Transition Cont.

- **DSS Resources located www.dss.mil/rmf**
  - Getting Started with RMF Job Aid
  - System Security Plan Template
  - System Security Plan Appendices Template
  - Technical Assessment Guide Windows 7
  - Technical Assessment Guide Windows 10
  - Technical Assessment Guide Windows Server 2012
  - Technical Assessment Guide Red Hat Enterprise Linux 6
  - Getting Started with SCAP Compliance Checker and STIG Viewer Job Aid
  - SCAP Compliance Checker
  - DISA STIG Viewer
  - ISSM Tool Kit (available at http://www.cdse.edu/toolkits/issm/index.php)

ISSM Training and Preparedness for RMF Transition Cont.

- **The following RMF Courses are located at www.cdse.edu**
  - Introduction to RMF (CS124.16)
    - http://www.cdse.edu/catalog/elearning/CS124-signup.html
  - Continuous Monitoring (CS200.16)
    - http://www.cdse.edu/catalog/elearning/CS200.html
  - Categorization of the System (CS102.16)
    - http://www.cdse.edu/catalog/elearning/CS102.html
  - Selecting Security Controls (CS103.16)
    - http://www.cdse.edu/catalog/elearning/CS103.html
  - Implementing Security Controls (CS104.16)
    - http://www.cdse.edu/catalog/elearning/CS104.html
  - Assessing Security Controls (CS105.16)
    - http://www.cdse.edu/catalog/elearning/CS105.html
  - Authorizing Systems (CS106.16)
    - http://www.cdse.edu/catalog/elearning/CS106.html
  - Monitoring Security Controls (CS107.16)
    - http://www.cdse.edu/catalog/elearning/CS107.html
  - RMF Overview - Recorded Webinar
    - http://www.cdse.edu/catalog/webinars/webinar-archives.html

DSS CDSE RMF Training Metrics FY16

Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

CDSE Consolidated Metrics Report - Summary by Activity

October 01, 2015 - September 30, 2016

Summary by Activity (STEPP)

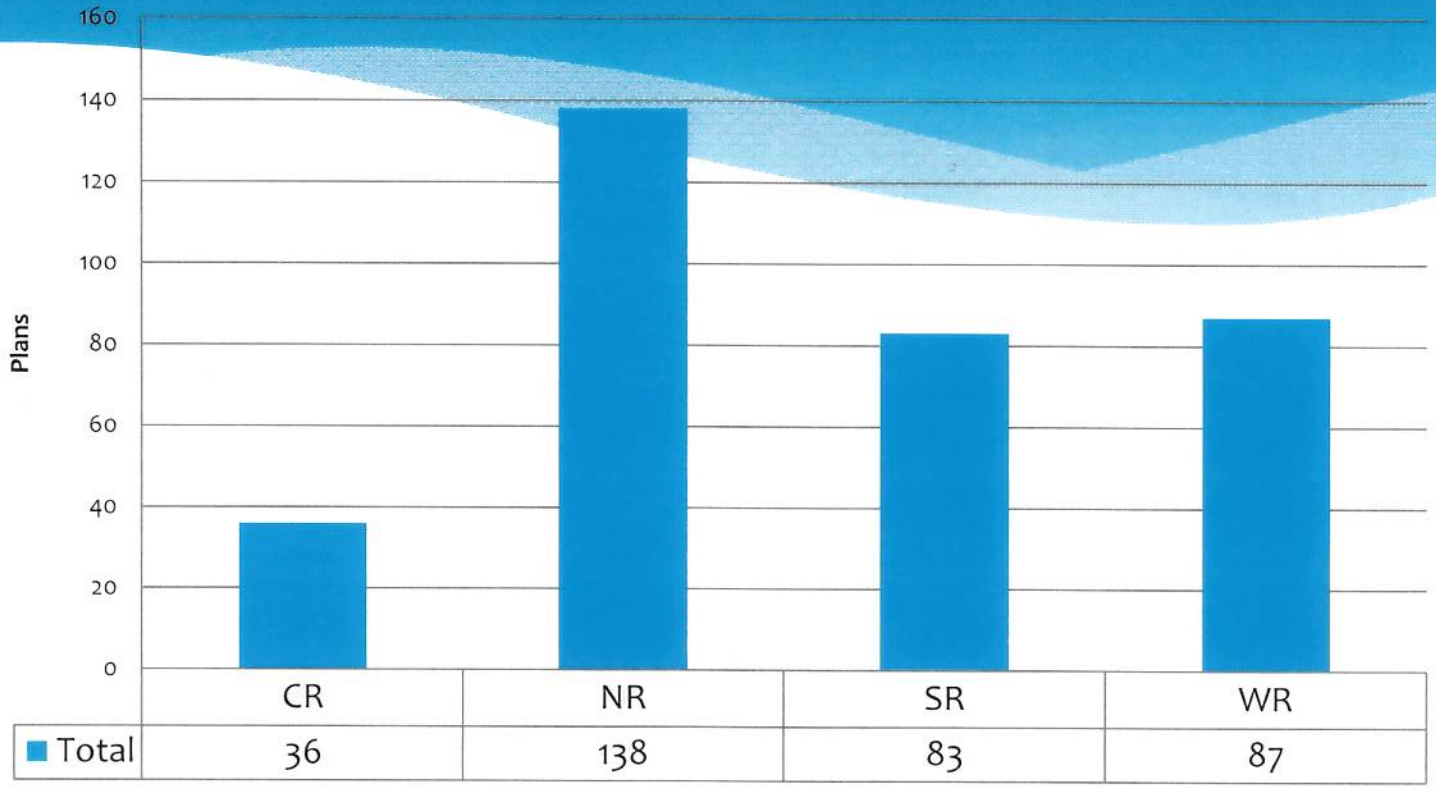
ACTIVITY NAME	ACTIVITY TYPE	DISCIPLINE	Industry
CONTINUOUS MONITORING COURSE	COURSE	CYBERSECURITY	295
INTRODUCTION TO THE RISK MANAGEMENT FRAMEWORK (RMF) COURSE	COURSE	CYBERSECURITY	427
RISK MANAGEMENT FRAMEWORK (RMF) STEP 1: CATEGORIZATION OF THE SYSTEM	COURSE	CYBERSECURITY	530
RISK MANAGEMENT FRAMEWORK (RMF) STEP 2: SELECTING SECURITY CONTROLS	COURSE	CYBERSECURITY	461
RISK MANAGEMENT FRAMEWORK (RMF) STEP 3: IMPLEMENTING SECURITY CONTROLS	COURSE	CYBERSECURITY	435
RISK MANAGEMENT FRAMEWORK (RMF) STEP 4: ASSESSING SECURITY CONTROLS	COURSE	CYBERSECURITY	408
RISK MANAGEMENT FRAMEWORK (RMF) STEP 5: AUTHORIZING SYSTEMS	COURSE	CYBERSECURITY	391
RISK MANAGEMENT FRAMEWORK (RMF) STEP 6: MONITOR SECURITY CONTROLS	COURSE	CYBERSECURITY	375

DSS FY 17 Training Products
(CDSE to develop)

- Introduction to RMF under NISP
- RMF Walk Through under the NISP
- Configuring Systems for RMF under the NISP

BACKUP SLIDE

Systems Expiring Within 90 Days



	CR	NR	SR	WR
Total	36	138	83	87

Total Plans Expiring within 90 Days for All Regions: 344

*** Data as of 2016OCT31****

Attachment #14

U.S. NRC Classified Contractor Information Systems Authorizations

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NISPPAC Information Systems Authorization Working Group - NRC

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- NRC maintains two separate Industrial Security Programs under the NISP
  - One program for NRC cleared contractor companies
  - One program for NRC Licensee and Licensee contractor companies
- NRC has a Memorandum of Understanding (MOU) with Department of Energy (DOE) for DOE to perform Certification and Accreditation (C&A) and reviews of NRC Licensee/Licensee contractor classified networks
  - Same accreditation and review process for NRC as for DOE
  - NRC has 10 classified Licensee networks accredited by DOE
- No NRC cleared contractor companies require classified IT systems at their facility.
  - NRC is working with DOE to modify the current MOU allowing DOE to perform C&A functions for NRC cleared contractors (non-Licensee), like the one in place for NRC Licensees, in the event the need arises

Attachment #15

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

Industry

10 November 2016

Agenda

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

National Industrial Security Program

Policy Advisory Committee Industry Members

Members	Company	Term Expires
Bill Davidson	KeyPoint Government Solutions	2017
Phil Robinson	SSL MDA Holdings, Inc.	2017
Michelle Sutphin	BAE Systems	2018
Martin Strones	Strones Enterprises	2018
Dennis Keith	Harris Corp	2019
Quinton Wilkes	L3 Communications	2019
Robert Harney	Northrop Grumman	2020
Kirk Poulsen	Leidos	2020

National Industrial Security Program

Industry MOU Members

Industry Association	Chairperson
AIA	J.C. Dodson
ASIS	Dan McGarvey
CSSWG	Brian Mackey
ISWG	Marc Ryan
NCMS	Dennis Arriaga
NDIA	Mitch Lawrence
Tech America/PSC	Kirk Poulsen

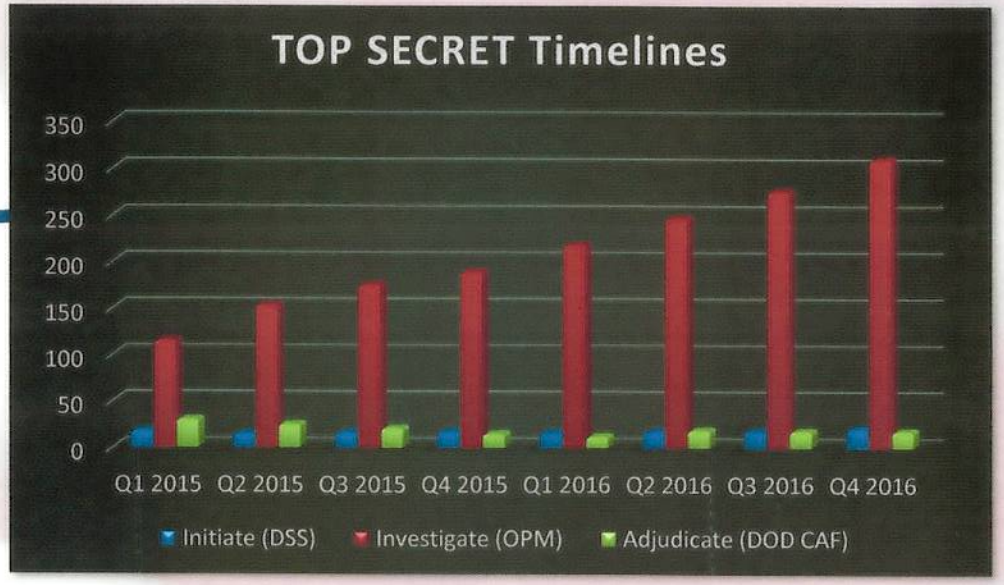
Impacts of Policy Changes - Overview

- 2017 will be a year of change with Insider Threat, CUI, RMF, JVS, and NCCS. Industry and USG both need increased fidelity on the costs of NISP implementation before additional reforms and new regulations are considered.
- The growing backlog of personnel security investigations and long lead time for meaningful reform to take hold will place national security at risk as both the USG and industry struggle to deliver responsive solutions from a tightening cleared labor market.
- Industry will be responsive to new initiatives, more efficiently so if included in preparatory phrases where the intended outcomes of new initiatives are determined.

New Business

Clearance Timelines

- National Background Investigations Bureau (NBIB)
  - Industry will be awaiting updates on the progress of the NBIB to include an update on the status of the hiring and training of the additional 400 investigators
- FBI manual name checks 28,000 backlog – Not needed for interim. But a challenge for closing cases in a timely manner.
- Concern regarding funding shortfall with DSS in FY17
- Push for an ODNI Memo to Components (similar to OUSD, Robert Andrews Memo 7/31/2006) indicating eligibilities do not expire with a link from the DSS website to OUSDI web.
- Industry will be struggling with retention and recruitment of cleared personnel as well as increasing salaries as clearance timelines escalate



- CDC employee base and national security is being placed at risk; workforce churn, increased competition intra-industry for cleared personnel, efforts to work at lower levels of classification and loss of qualified scientific and technical candidates outside of the DIB as they select other employment options

New Business

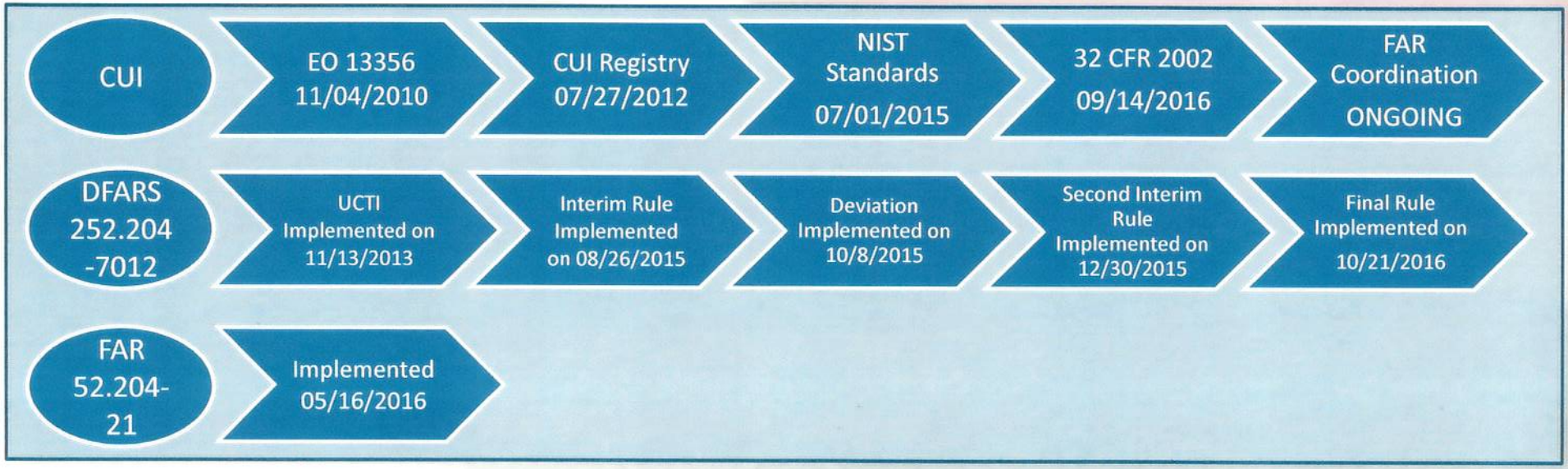
Department of Commerce and DSS Survey

- Industry was concerned with the scope of this questionnaire and the lack of coordination/discussion to understand the impact it will have on our thinly stretched FSOs and support teams.
- ISOO, Commerce, DSS & Industry meetings held to address concerns.
- Boeing, L3 and Harris working with Government as Beta testers for Industry MFOs, Lockheed will be soon
- Industry will be eagerly anticipating communication back from Boeing/L3/LHM as to how the process has been working.
- Our hope is a more flexible and efficient approach will be given for MFOs.

New Business

CUI, CDI, & Federal Contract Information

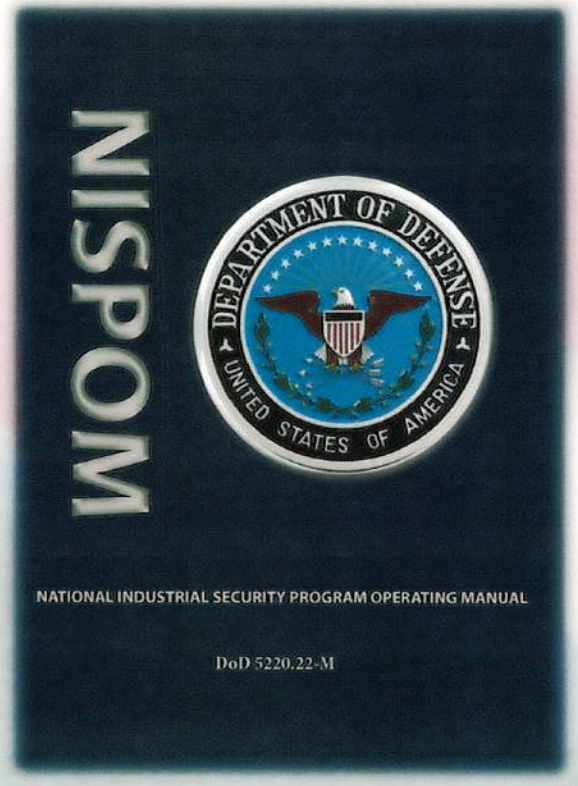
- Working towards compliance with NIST 800-171 by December 2017
- Large companies will incur a huge cost to upgrade networks; smaller companies will lack in-house expertise
- Proper marking of information and guidance from government will be key



Security Policy Update

Industrial Security Policy Modernization

- National Industrial Security Program Operating Manual revision and update
  - 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.
- 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 JAFAN and NISPPOM SAP Supplement upon publication of all the above.
  - AF SAPCO officially rescinds JAFANs
- *AF and NAVY releasing separate implementation guides for each volume late 16-early 17.*
- *Numerous Cyber Security Policies remain a challenge for SAP Community*
  - *RMF/JSIG, Win 10 Implementation, Data at Rest, DFAR requirements, Monitoring Tools, Cyber Workforce*
- SEADs Under Development and Review; Industry unable to review due to being FOUO. Industry input into SEAD development would be seen as optimal and timely given state of personnel security process transition.
  - SEAD 3: Minimum Reporting Requirements
  - SEAD 4: Adjudicative Backlogs



National Industrial Security Program

Policy Advisory Committee Working Groups

- Personnel Security: General
  - E-adjudication business rules being aligned with new Federal Investigative Standards. New FIS expected decrease in e-adjudication across the board.
  - DOHA SOR Process. Definitively ID true caseload and aging of those cases.
  - Interim Clearance impacts due to policy change on granting interim eligibility for industry (4 days to 30 or more)
  - Expecting backlog to continue growing based on OPM Breach, new FIS, and DSS funding challenges

National Industrial Security Program

Policy Advisory Committee Working Groups (cont.)

- Personnel Security: Applications
  - NISP Contractor Classification System (NCCS)
    - What is plan for deployment and account administration?
    - Industry need to plan for training of security, contracts and PM's. Projected live date is December.
    - Currently one POC at DSS to set up accounts. What is the long term plan and will this be incorporated into the Knowledge Center?
    - SAM will override ISFD in terms of legal entity names and may invalidate CAGE codes.
  - Defense Information System for Security (DISS) and Joint Verification System (JVS)
    - Projected go live December for components, March for Industry
    - Concern regarding the mirroring of JPAS and JVS while transitioning to Industry
    - Industry Advocate for the Governance Review Board for DISS change requests
    - JVS does not send eligibility notification, this is a NISPOM requirement for industry
    - Template needed in csv format for developers of SIMs, Access Commander and ISMSi to be able to import
    - No formal training for this system has been developed to date (training needed for all stakeholders)
  - Development of National Industrial Security System (NISS)
    - Participated on the system requirements phase and standing by for further development meetings.

National Industrial Security Program

Policy Advisory Committee Working Groups

- Insider Threat Working Group
  - OUSDI, DSS & Industry collaborated on Insider Threat ISL (published 25 May).
  - Need consistent requirement across all the User Agencies relating to implementation SOPs. Great start with the CIA publishing implementation guidance that mirrored the NISPOM requirements.
  - Industry will be curious to learn what DSS will be looking at when evaluating at an the Enterprise vs. Local levels of an Insider Threat Program.
- Information Systems Authorization Working Group (Formerly C&A WG)
  - Working group focus is on incorporating the Risk Management Framework (RMF) into future process manual updates.
  - Currently commenting on the new RMF Template