Minutes of the November 19, 2014 Meeting of the
National Industrial Security Program Policy Advisory Committee (NISPPAC)

The NISPPAC held its 49th meeting on Wednesday, November 19, 2014, at 10:00 a.m. at the National Archives and Records Administration (NARA), 700 Pennsylvania Avenue, NW, Washington, DC 20408. John Fitzpatrick, Director, Information Security Oversight Office (ISOO) chaired the meeting. Minutes of this meeting were certified on January 27, 2015.

I. Welcome and Administrative Matters

After introductions, the Chair welcomed everyone and reminded them that NISPPAC meetings are recorded events and that minutes of the meeting will be provided at a later date. He then introduced two new industry representatives, Michelle Sutphin and Martin Strones, and noted that industry representatives are nominated by industry membership and subsequently appointed by the Chair to serve a four year term. After welcoming the new members, he asked Greg Pannoni, the Designated Federal Official (DFO), to review the Committee's old business. (See Attachment 1 for a list of those in attendance.)

II. Old Business

Mr. Pannoni noted that a listing of the four action items from the June 19, 2014, meeting was available in each member's packet (See Attachment 2). He noted that the first item was completed with the appointment of the two new industry members. He explained that the remaining items were taskings for the Personal Security Clearance Working Group (PCLWG), and that each would be covered in depth during today's meeting. He summarized them as a study of the e-adjudication process to determine if it can be made more effective for the adjudication of industry security clearances; an examination of a Joint Personnel Adjudication System (JPAS) anomaly depicting the number of open cases at the Defense Office of Hearings and Appeals (DOHA), followed by a report on efforts to eliminate this procedural inaccuracy; and an investigation of the security clearance validation process to determine if personnel being adjudicated for access to classified are in fact being subsequently accessed as required. The Chair noted that any actions generated as a result of today's discussions would be carried forward through the minutes to the appropriate working group to be reported at the next NISPPAC meeting.

III. Reports and Updates

The Chair began with a brief commentary of the historical purpose of the National Industrial Security Program (NISP), followed by an explanation of the program's future as made necessary by the passage of time and how the government is currently addressing the challenges of expanding missions within the framework of an ongoing industrial reliance and partnership. He explained that prior to the NISP, which was formalized in a 1993 Executive Order, there was diversity and conflicts in the ways government security requirements were implemented in industry; and that it was in the national interest to formally put an executive order and a program, in place, to address such matters in a much more consistent manner, to speak more singularly as the government, and to do that in a contractually observable way. He noted that the NISP was established, to bring the existing classified contracting programs of the government under a single umbrella; and to provide the major government agency NISP participants: the Department of Energy and the Nuclear Regulatory Commission doing the oversight of classified nuclear-related activity, the Department of Defense overseeing the contracting for both its own purposes, and on behalf of other government agencies; and the intelligence community servicing its needs with its constituent contractors. Continuing, the Chair noted that the NISP established a consistent set of guidelines regarding the way that government contracting with industry would go forward. He delineated that the words in the executive order that got to that idea are "a consistent, integrated industrial security program for the US government." He described the period of the inception of the NISP as difficult, but noted that over 20 years later, the NISPPAC still represents the commitment on the part of the government and industry together to have an open dialog about issues and to continually tend to the needs of both. The Chair noted that events that are occurring in government and national security arenas, in general, are impacting policies more broadly than those original activities that fell under the NISP umbrella. He described in detail activities in the areas of critical infrastructure protection, and cyber security, where unique partnerships, between the public and private sectors do not always follow the traditional NISP contracting methods. He noted that whether or not it's for a classified contract, security requirements are being addressed in both government contracts and policy that require both the government and its industry partners take different approaches to implementing security requirements. The Chair asserted that while the entire government effort around controlled unclassified information (CUI), by definition, does not fall under the NISP, the government is articulating safeguarding requirements that are analogous in many ways, to the kind of requirements that come through the classified environment. He noted that this has made the landscape much more complex, and that we cannot confine our point of view to just those issues that fall directly under the NISP umbrella. He offered that with critical infrastructure, cyber security, and CUI activities occurring in all of our mission areas, we cannot limit our discussions to only those of the NISP. The Chair acknowledged that the message from our industry representatives, that the government seems to speak in many voices has been received, and declared that his challenge was to pull together the principals in the NISP to address their concerns. He noted that industry had signaled a need to discuss how to better integrate security requirements in 2014 and beyond, which is not that dissimilar from what happened 20-odd years ago that led to the start the NISP. The Chair opined that there are ways that we can enhance the integration between NISP guidance and other policy requirements, and that ISOO is the place where that should happen. He advocated that when conversations emerge around cyber, critical-infrastructure, and information sharing; whether from the National Security Council or other venues, that it is done under the auspices of the NISP. The Chair noted that even if it doesn't look like a classified contract, the principles behind information protection, risk management and risk assessment all need to be the same, and if we need new tools to deal with these new requirements, then let us build them and keep everything as closely integrated as possible. He declared that his message to industry was, "we heard you" and that what we anticipate going forward, is a focused dialogue on their needs, and that if industry feels the NISP is fractured, then the first step is to determine how best to express what that impact is on them, and then figure out the solution to better integrating those security requirements. The Chair noted that when industry conveys its problem statement to the NISPPAC, that it is in a ready-to-listen mode, and ready to engage in those dialogues through the formal mechanisms of the NISP and the NISPPAC. The Chair suggested the establishment of a temporary or permanent working group under the NISPPAC to provide a focus on policy needs and integration efforts for the NISP as it goes forward. He suggested that a second track is to have a more focused dialogue on a formal NISP Operating Manual (NISPOM) revision to-do list beginning in 2015. He added that separate and apart from the conforming change activity that's been driven by other policy needs, this would be one where we take feedback, because any NISPOM revision must include a round of industry feedback. The Chair commented, that some of those in attendance were part of the original discussion that launched this idea that the NISP could be better integrated in the future, and that some, such as the NISP Cognizant Security Authorities (CSA), have heard this conversation over the last few weeks. Tony Ingenito, Industry, advised that industry was currently tracking 50-plus issues that are potentially leading to changes in security policy, and noted that industry was excited to move forward and formalize the process, and to look deep into the root-cause of some of these requirements. He mentioned that changes in the process for publishing the NISPOM revision continue to impact industry's ability to comply with changing requirements. Stan Sims, Director of Defense Security Service (DSS), echoed Mr. Ingenito's appreciation to the Chair for taking on this effort and noted the challenges in trying to work with government and industry to come up with a policy that is not problematic for us. He noted that DSS wants to be part of the discussion and called for patience from industry, as they try to work through these challenging activities and until such time that they can reset our policy and get it back on track. The Chair concluded noting that this forum and its working-groups will continue to provide updates and opportunities for dialogue about policy changes.

Valerie Heil, Office of the Undersecretary of Defense for Intelligence (OUSDI) provided the DoD update. She noted that NISPOM conforming change number two will levy requirements on cleared contractors to establish and maintain an insider-threat program, and that the document should be ready for publication by the summer of 2015. She noted that after the final DoD review, where there will be changes, time will be afforded for a final review and required concurrence by the other Cognizant Security Agencies before it is published. She provided an update on the NISPOM rewrite, noting the coordination process is expected to start in March or April of 2015, and that they will combine the prior actions from that the NISPOM Rewrite Working Group , with the changes from the two NISPOM conforming changes to form the baseline document. She indicated that OUSDI's goal is to work through the NISPPAC informal process, and have the NISPOM rewrite enter the DoD formal policy-issuance process by September 2015. She reiterated that, the final NISPOM rewrite will have to go into the Federal Register for public comment prior to its expected publication in FY17. Ms. Heil updated the Committee on the status of the DoD Acquisition, Technology and Logistics (AT&L) and the Chief Information Officer's (CIO) Procedures, Guidance and Instructions (PGI) relating to the Defense Federal Acquisition Regulation (DFAR) clause on safeguarding controlled unclassified technical information. She explained that representatives of both AT&L and CIO met with many of the industry associations to discuss their concerns over areas of the PGI or the DFAR clause that they thought were confusing. She noted that the PGI is expected to be published in December 2014, and will be linked to the DFAR clause. She noted that the PGI is guidance for contracting offices; however industry will also be able to view it.

Mr. Sims provided the DSS update, noting that as customary over the last few years, DSS hosted a government-stakeholder meeting on Monday November 17, 2014, and then one with our industry partners on November 18, 2014, in preparation for this meeting. He briefed that much of the discussion with both groups centered on the personnel security clearance management process, and that each group discussed governance, oversight, and then improvements to those processes. He noted that a prevailing topic was the Director of National Intelligence (DNI) memo from October 2014 regarding the reduction of personnel security clearances across government and industry, as well as DSS's efforts to oversee that process, and a pending DNI review and update on that oversight process. He explained that as a result of that memo, the DNI authorized DSS to conduct an assessment of industry clearances over the next couple of years, as part of our overall assessment process. Mr. Sims noted a discussion of a continuous evaluation process for government and industry, and updated attendees on DSS efforts in conjunction with on-going pilot programs. He opined that DSS's efforts were to manage the results of the pilot, minimize the impact on industry, and to keep industry updated as the pilot programs progressed.

Mr. Sims gave an update on the Office of the Designated Approval Authority (ODAA) Business Management System (OBMS) that automates the process for submitting system security plans to DSS for certification and accreditation, and validated that in January 2015, there will be a requirement to submit your systems security plans through the OBMS to be processed. Finally, Mr. Sims reported that efforts to automate the DD 254, "Contract Security Classification Specification", were progressing, and that through their partnership with the DoD AT&L, they will save on both time and costs in implementing the capability. He noted that testing would begin in December 2014 and suggested that by early summer the automated system will be available for use by both industry and government and will represent a huge win for the community at large.

Mr. Ingenito, Industry spokesperson, provided an update on Industry issues and concerns (see Attachment 3). He also welcomed Michelle Sutphin and Martin Strones to the NISPPAC and noted they will serve until 2018. He noted there will be two changes in our Memorandum of Understanding (MOU) Group Representation for the Aerospace Industries Association and the American Society for Industrial Security in January. He touched on the CUI program, and expressed appreciation for the efforts of ISOO, as the executive agent, and that industry looked forward to being able to review and comment on the National Institute of Standards and Technology (NIST) *Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal information Systems and Organizations*. Addressing the area of the insider threat, Mr. Ingenito, explained that industry was currently monitoring eight separate policy actions, and noted that industry looked forward to folding these issues into the working group that will be established on policy integration. Regarding cyber reporting requirements, he noted that industry continues to see requirements for implementing controls without a corresponding policy in place. He expressed concern that some of the data breaches that have happened to company networks could result in the potential loss of contracts with the government, and noted that industry as a whole is now starting to have some reservations about the requirements to report this data, if there's going to be retribution. He agreed with the Chair's comments regarding the fracturing of the NISP, and mentioned key areas, such as cyber, insider threat, and personnel security where we see some of the greatest policy inconsistencies. He explained that industry wants everyone to understand that when there's a policy change, that there is also a potential security-cost increase that goes with it. He noted that when there is a change that's going to implement more stringent and costly security processes, that industry needs lead time to be able to budget for it before having to implement it. Mr. Ingenito informed the Committee that he attended the last Personnel Security Clearance (PCL) Working Group, meeting and was pleased with the progress that’s being made, regarding the review and updates to the e-adjudication business rules, and in the updated federal investigative standards, and will work to ensure these efforts can help us in the future. Additionally, he opined that the Certification and Accreditation (C&A) Working Group was doing good work, and noted that industry was working with DSS to develop a guidance that will be published on the Microsoft XP operating system end of life, and its impact on testing equipment, and on how we’re going to move forward with a policy. Mr. Ingenito addressed conforming change number two, and noted that industry continues to support its implementation. Regarding the DD254 database, he noted that industry has 25 beta testers ready to assist in its initial implementation, and that they are waiting on DSS to put them to work. Mr. Ingenito noted that industry had been seeing a lot of inconsistent application of policy coming out of the special access program (SAP) environment, and that some policy activity, as a result of the Joint SAP Implementation Guide and Risk Management Framework, and the two-person integrity policy, requires industry to request that the SAP working group be reconvened so that we can truly work these issues in a more direct and timely manner, rather than just trying to work issues through the MOU Group process. The Chair agreed, and took an action for ISOO to reconvene the SAP working group, and refocus their efforts at these issues of concern.

David Best, ISOO, introduced the PCL Working Group report (see Attachment 4) and reminded members of the three action items from the June NISPPAC meeting, that were mentioned earlier in the meeting. He advised members that the performance metrics for DoD, DNI, DOE, and NRC, as well as the DSS Personnel Security Management Office (PSMO) were provided for their review, and highlighted items from the PSMO metrics, that showed the electronic fingerprinting submission rate is now at 94%, up from 30% this time last year, and that overdue periodic reinvestigations (PR) are at 8,550 as of October 2014, down from a little over 30,000 in June 2014. Mr. Best noted that two working group meetings were held since the June NISPPAC meeting to work the following action items: (1) study the e-adjudication process to see if it can be made more effective for the process of clearing industry personnel; (2) address ways to fix the erroneous data in JPAS that shows over 10,000 cases in the DOHA inventory, and how to bring that number down over time; and (3) review the security-clearance validation process, and see if those being adjudicated for access to classified are, in fact, being accessed as required. Regarding, the review of the e-adjudication process, Mr. Best, noted that the group recommended a raise in the adjudicative thresholds of the Office of Personnel Management (OPM) business rules, so more industry clearances can be done through the e-adjudication process. In response to the issue of the erroneous reporting of open cases at DOHA, Mr. Best opined that Carl Klein, Chief of Personnel Security at OUSDI, suggested the initiation of a new data-quality initiative (DQI) that will change the file notations in JPAS to “pending adjudication", thus eliminating any reference to DOHA. In addressing the issue raised regarding the Office of the DNI (ODNI) reporting of the variance between the number of people with adjudicated clearances and the number of those actually granted access to classified information, Mr. Best noted that the group observed that the variance, in part, could be attributed to the DoD IT credentialing process use of the investigation process for classified information to grant an IT credential. He noted this action results in issues regarding paying for investigations for a security clearance and not using it for other purposes.

Steve DeMarco, DoD Central Adjudication Facility (DoDCAF) reported (see Attachment 5) that the DoDCAF transformation is continuing since its consolidation into one entity in October 2012. He noted that the timeliness of industry investigations is up, and that the DoDCAF adjudicates initials cases on average in 35 days, and PRs in 58 days. He explained that they were exceeding Intelligence Reform and Terrorism Protection Act (IRTPA) and DoD-mandated timelines, because they were working the oldest cases first, in order to eliminate their backlog of cases, and that for every backlog case that is adjudicated that's more than 365 days old, that 20 new cases must be adjudicated, to offset one older case by 19 days. He noted that the DoDCAF puts a lot of effort and time and resources into eliminating the backlog cases, which has resulted in longer adjudicative timelines. Mr. DeMarco noted that the industry case inventory was trending down, with a backlog of 6,300 cases, and that in January of 2014 they had 14,500 cases in backlog, which had now been reduced by 72% to fewer than 4,100 cases. He noted their goal was to eliminate the backlog by the end of FY15. In response to the action item regarding JPAS erroneously reflecting cases pending at DOHA, Mr. DeMarco explained that the DODCAF stopped indicating that an investigation status was pending at DOHA about 18 months ago. He advised that anything prior to that still reflects the case as pending at DOHA. He noted that they are working with the Defense Manpower Data Center (DMDC) to determine the scope of the problem and then determine the requirements for a DQI within JPAS to fix the problem. He concluded noting that the PCLWG, in partnership with DSS, DOHA, and OSDI, are working to ensure that we get the right information reflected accurately in JPAS. Mr. Pannoni asked if there was a way of identifying how many of that target group are actually PRs?, Mr. DeMarco explained that if clearance eligibility was granted by DOHA, that it was actually adjudicated by DOHA or has been a denial or revocation, and that going back and clean up all the other DOHA comments requires a different initiative. The Chair questioned if the referred to DOHA notation may or may not indicate the presence of serious issues. Mr. DeMarco replied that all the cases still need to be reviewed physically to determine the seriousness of any issues, and that most of the due process cases referred to DOHA involve credit issues, which are normally easily mitigated once they are updated. Leonard Moss, Industry, commented that the fact that it says the case is at DOHA creates problems, so changing the language is the best course of action unless you know there is a reason for a suspension. Mr. DeMarco noted that there is a separate criterion in place for an interim suspension, which is worked in partnership with DSS, and that criterion, asks if it is in the best interest of the national security to remove that person from access temporarily until the issues can be resolved? He noted that either the CAF or DSS will initiate the action as appropriate. The Chair commented that there are not expectations around cases that are denied or revoked in how they are processed, but what should be done is to follow this dialogue through to say all of those cases that used to be labeled "DOHA" are now understandable through the DoD CAF's normal reporting mechanism, and here's where all of them are, and note that anything that's still at DOHA is in the procedural process which is different from being in the adjudication process. He noted that its completely reasonable asking who DOHA is accountable to, and what information can be shared here, and if there are transparency requirements for DOHA reporting. The Chair stated that he wanted to make sure we're clear that we're asking two different questions, and opined that the establishment of the DoD CAF provided both the opportunity to make the process clearer, and that being in transition meant we had to be a little patient while they get to this point. Vince Jarvie, Industry, asked if the trend line for initial industry clearances is going down or up. Mr. DeMarco responded that the trends were going down slightly and Mr. Sims added that the volume of submissions was also down, due primarily to the budgetary environment.

Christie Wilder, ODNI, updated the Committee (See attachment 6) regarding the memos that were issued in the last year that asked agencies to validate their employees with a security clearance and access. She noted that the Security Executive Agent (SEA) observed a 3.1% reduction in those agencies that provided responses. She explained that it wasn't necessarily a reduction so much as a validation that those people with access to classified information had a need to know and were in access. She noted that the memo accelerated several initiatives that were already under way to clean up the repositories and other systems that are used to validate that the people with access still needed that access, and that overall there was a 5.3% reduction as of October 1, 2014. She mentioned that another initiative that required a reduction of the PR backlog was still underway. She noted that the first memo tasked agencies to come up with a risk-based approach, and to develop some criteria to assess which investigations need to be worked first. She noted that now agencies are required to report on a quarterly basis what their out-of-scope population is, and then the number of out-of-scope PRs that have been initiated each quarter, and in doing so we want to see the number of out-of-scope PRs decrease, and the number initiated increase, until they somewhere meet in the middle, and hopefully clear that backlog. Ms. Wilder advised that in the past, timeliness had always been the hot-topic issue that we focused on, now several new challenges such as quality of background investigations, reciprocity, and metrics on how we assess the revocation process, are now in the forefront. She noted that going forward they would to keep an eye on reciprocity metrics, because the 2014 Intelligence Authorization Act, requires ODNI to collect reciprocity metrics over the next three years, and then submit an annual report to the Congress and President. She advised that a memo requesting agencies to provide reciprocity metrics is in coordination, and is due out in December 2014, and that ODNI wants to start collecting that data in January 2015. Next she spoke to the quality of background investigations, noting that the SEA had partnered with OPM, the suitability executive agent, to come out with quality standards and metrics, as well as a tool that agencies could use to assess quality, indicating that in FY16 they would start collecting metrics from the agencies on the quality of background investigations. She updated the Committee on reporting required under the Intelligence Authorization Act regarding security clearance determinations, and noted that the numbers for this year, which had been briefed to the DNI, show a decrease across the government in eligibility of 12.3% and 5.3% for those in access. Ms. Wilder explained that the reason why there are people that are eligible for a clearance but not in access, is because there are many people that are investigated and adjudicated and given access and then no longer need it, and because of reciprocity, we keep their eligibility status active and keep them in the repository, so when we collect the numbers for this data call, we measure those people as well. She noted that it was more cost effective to maintain those individuals in a repository, in case they need access in the future, rather than having to reinvestigate and re-adjudicate them. In addition, she explained that there are people in sensitive positions that are investigated and adjudicated to the same level of those that are in access, but who actually never need access, and are considered to be eligible because, if they needed access, we could read them in on a moment's notice. Mr. Sims added that management of your personnel security clearance database is critical in determining access versus eligibility, because at the moment you take someone out of access, the two-year clock starts, and that it does take awareness on the part of security managers in both the government and industry to properly manage the process. Lisa

Loss, OPM, spoke regarding assessment standards, noting that OPM is very close to issuing the document that specifies the standards and that an assessment tool will be developed for use by the agencies, so they can start applying the new standards to investigations, as soon as it is out. Ms. Wilder noted that what was found was that many agencies had a different definition of what made up a quality investigation, and that this will help clarify most of the issues. The Chair noted that this was Ms. Wilder's last appearance before the NISPPAC, where she has been representing the SEA and ODNI, and acknowledged her contributions to the Committee. The Chair then introduced her replacement, Gary Novotny, ODNI.

Tracy Brown, DSS, presented the report of the Certification and Accreditation Working group (C&AWG), (See attachment 7) and advised the Committee that for this fiscal year, the group is working to collect information on the compliance tools that are currently being used by the other CSAs, and that the intent of the project is to assess and leverage any similar processes so we can establish consistency in the way that we perform system validations. Additionally, she advised that they were looking at ways to improve the tracking and approval of changes to the ODAA Process Manual. She noted that information about this proposed change management process was in their packages. Regarding DSS-specific C&A metrics, Ms. Brown noted that they were issuing Interim Approvals To Operate (IATO) in an average of 21 days and issuing straight to approval to operate (SATO) in 26 days. She advised that the working group expressed concern that timelines have been trending upward since July 2014, but noted that the increase was attributable to the fact that during that same timeframe DSS was rolling out OBMS. She explained that while they are in transition, they would still receive email submissions, while they process the plans being submitted through OBMS. She noted that industry was using OBMS for about 40% of the submissions, and that their goal was to get the other 60% using the system by January 2015. Ms. Brown identified the key takeaways were: (1) ODAA had done a good job in processing system security plans in a timely fashion; (2) they were still seeing the same common deficiencies, with the plans missing required attachments, and containing numerous errors; (3) during on-site validation visits they were still seeing security-relevant objects that were not being locked down; and (4) ODAA was continuing to move forward in the processing of more SATOs where practical, and to improve the consistency and to minimize the risk in industry. Mr. Moss asked if they were aware of the challenges that people are having with OBMS. Ms. Brown responded that there were some challenges with our call center's response to issues, and that they were working with their technical team to improve training, and turnaround time. She advised that contacting the call center was the first step, and if you continue to see the same problem to report it using the ODAA mailbox, and by informing the local ISSP. Mr. Sims commented that as they roll out new systems we are always going to have challenges, and noted that the biggest issue was that the ISSMs never got confirmation that their plans were submitted, and that caused some complications, since people couldn't verify their plan had been accepted. He explained that a team was brought in from across the DSS regions and with their support contractor, had worked out all the issues. Mr. Sims noted that another big challenge was getting OBMS users to set up accounts, and to make sure that their PKIs are accepted, so that their certificates and credentials will be verified. He noted that there was nothing to hold up a company from submitting their plans through the OBMS system except setting up an account. Mr. Sims reminded members that as of 1 January 2015, all plans must be submitted through OBMS.

The Chair then updated the Committee on the status of the CUI program (see Attachment 8). He described it as an effort to standardize the instructions and practices around what CUI is, and how to define that information more clearly. He advised members that they can go to the CUI registry on Archives.gov/CUI, and explore the categories and subcategories of information that, under some regulation, law, or government-wide policy, require control. He noted that under the CUI regime, once the new federal regulation is approved, there will be a single set of instructions, guidance, and directions about how agencies should control information that is in the CUI registry. The Chair explained that the first part of the three-part plan for implementing CUI is the federal regulation (32 CFR Part 2002) that is currently in the OMB's interagency review process, and which will go through the Federal Register for public review and comment in 2015. The Chair stated the objectives are to clearly articulate what the requirements are and to set expectations that anybody reading this rule will understand, and that he would let the NISPPAC know when it is released. He noted that normally a new rule will go through at least two rounds of public review and comment, and he estimated that we'll have a federal rule in effect in the middle of or near the end of FY15. The Chair explained that the second of the three-part plan was the release of the NIST special publication which will provide the IT requirements for any non-federal system that handles CUI. He noted that the third part of the CUI plan was to publish a clause in the Federal Acquisition Regulation (FAR) that would be employable in all contracts that involve CUI requirements, and would apply the handling practices that will be in the federal rule throughout federal contracting. The Chair advised that ISOO was keeping the FAR Council principals and the Office of Federal Procurement Policy involved in the process of drafting of the federal rule. He summarized; noting that both the CFR and the NIST special publication should be published in late FY15, and then we would see the CUI FAR clause, and its public review and comment period in about a year. The Chair spoke specifically regarding NIST special publications, noting that they are normally applied through some other regulatory form, which in this case it would be the CUI FAR clause that would apply it to the specific contracting situation. He advised that the initial public draft of *NIST Special Publication 800-171* that was just released would have a 60-day period for public comment, after which we'll review the comments and put the final version out. He noted that now is the time for organizations, trade associations, and any others who desire to provide comments. The Chair reiterated that the federal rule will require that CUI systems be protected at the moderate level with confidentiality controls from the NIST Risk Management Framework, and that these are articulated in a series of NIST publications that apply to federal agencies through FISMA and that they won't apply to contracts unless they are applied through the CUI contract clause. He explained that the special publication translates the existing NIST guidance, that establishes the specific controls on information and information systems, and informs users of non-federal systems how they will demonstrate compliance. The Chair emphasized that the new special publication is intended to articulate a means for companies to utilize compensatory controls, to validate that they meet the objective of identification and authentication, but in a way which differs slightly from the federal guidance but still meets its' objectives. The Chair commented that that's the flexibility which is understood by all the federal partners to be necessary for something to be implementable in the non-federal space, and so the intent of that document is to provide greater flexibility than is in the Defense FARS (DFARS), and when it is successfully enacted, then parts of that DFARS rule would be removed. Mr. Sims asked what the mechanism would be that would determine that the contractor community was in compliance with all requirements. The Chair responded that one way to understand the scope of this effort is that under the FAR umbrella there are 350,000 entities that contract with the US government that actually have work that this clause could apply to. He noted that under that context, the responsibility to verify compliance would fall under the government contracting authority, and that this would be part of the FAR rule, and would use the General Services Administration's System for Award Management (SAM), that regulates, collects, and provides information about contracting activity, to those 350,000 entities, through the government contracting community. He explained that SAM would be the repository for any contractually required material and then, it is up to the Government Contracting Authority (GCA) to determine the verification mechanism, which would include a self-certification, and a follow-up, just like any aspect of the FAR is subject to review and validation by the GCA. The Chair indicated that this is the starting position, and while we do not know how many of those 350,000 contracting entities will be actively engaged with CUI designated information, we do estimate that it is going to be the majority, and that the mechanism raises questions that we are going to have to work through in the regulatory process. He envisioned that from its starting position a company will assert and certify its total compliance for the CUI program, and to the degree that it relates to NISP oversight, DSS would have a role. He opined that this is a very broad application of a federal rule, meaning the CUI FAR rule and all that it will entail: such as marking requirements, dissemination controls, and whatever is in the final version of the NIST document. He advised that while we do not know what the impact will be, with regards to NISP-specific concerns, we do need to keep our eyes open about it, and noted that while the NISP CSAs have had discussions around all of these “fracturing of the NISP” concerns, this is one issue that’s certainly bigger than cleared NISP contractors. The Chair encouraged members to review SP 800-171, and advised that when we need similar public comment for the CFR and the CUI federal rule, we will alert you.

The Chair announced the opportunity for anyone to raise an issue that we haven’t discussed, and polled those both present and those teleconferencing if they had any additional issues to raise to the Committee. He noted that the next NISPPAC meeting is scheduled for March 18, 2015, at the National Archives, and while our summer meeting is scheduled for July 15, 2015, we have been asked to have that meeting as an event with the NCMS seminar on June 22, 2015 at the Bellagio Resort in Las Vegas. The Chair informed the members that in order to make a thoughtful decision regarding that request, we will be sending out a survey within the next few days, to see if we can support a meeting at that location. He noted that the last meeting of 2015 will be on November18, 2015 at the National Archives. He adjourned the meeting at 1155 after thanking everybody for attending.

Attachment #1

Attachment 1

NISPPAC MEETING ATTENDEES/ABSENTEES

The following individuals were present at the November 19, 2014, NISPPAC meeting:

John Fitzpatrick,	Information Security Oversight Office	Chairman
Greg Pannoni,	Information Security Oversight Office	DFO/Presenter
Stan Sims	Defense Security Service	Member/Presenter
Kimberly Baugher	Department of State	Member
Jeff Moon	National Security Agency	Member
Anna Harrison	Department of Justice	Member
Kathy Healy	National Aeronautics & Space Administration	Member
Anthony Ingenito	Industry	Member
William Davidson	Industry	Member
Richard Graham	Industry	Member
Phillip Robinson	Industry	Member
Steve Kipp	Industry	Member
Martin Strones	Industry	Member
Michelle Sutphin	Industry	Member
Jeffery Bearor	Department of the Navy	Member
Brent Younger	Department of the Air Force	Member
Tim Davis	Department of Defense	Member
Rick Hohman	Office of the Director of National Intelligence	Alternate
Kisha Braxton	Department of Commerce	Alternate
Anthony B. Smith	Department of Homeland Security	Alternate
Mark Pekrul	Department of Energy	Alternate
Jason Rubin	Department of the Army	Alternate
Valerie Heil	Department of Defense	Alternate/Presenter
Valerie Kerben	Nuclear Regulatory Commission	Alternate
George Ladner	Central Intelligence Agency	Alternate
Christy Wilder	Office of the Director of National Intelligence	Presenter
Lisa Loss	Office of Personnel Management	Presenter
Steven DeMarco	Department of Defense	Presenter
Tracy Brown	Defense Security Service	Presenter
Keith Minard	Defense Security Service	Attendee
Glenn Clay	Department of the Navy	Attendee
Denis Brady	Nuclear Regulatory Commission	Attendee
Gary Novotny	Office of the Director of National Intelligence	Attendee
Alegra Woodard	Information Security Oversight Office	Attendee
Evan Coren	Information Security Oversight Office	Attendee
Chris Forrest	Department of Defense	Attendee
Kathy Branch	Department of Defense	Attendee
Priscilla Matos	Department of Defense	Attendee
R.B. Peele	Department of Defense	Attendee
Lisa Gearhart	Defense Security Service	Attendee

Christine Beauregard	Defense Security Service	Attendee
Laura Hickman	Defense Security Service	Attendee
Brandon Esher	Defense Security Service	Attendee
Anne Marie Galligan	Department of Energy	Attendee
Kastytis Miller	Central Intelligence Agency	Attendee
Jay Buffington	Defense Security Service	Attendee
Karen Duprey	Industry/ MOU Representative	Attendee
Mark Rush	Industry/ MOU Representative	Attendee
Kirk Poulsen	Industry/ MOU Representative	Attendee
Leonard Moss, Jr.	Industry/ MOU Representative	Attendee
Mike Witt	Industry/ MOU Representative	Attendee
Dan McGarvey	Industry/ MOU Representative	Attendee
Jim Shamess	Industry/ MOU Representative	Attendee
Scott Conway	Industry	Attendee
Mike Witt	Industry	Attendee
Mitch Lawrence	Industry	Attendee
Dianne Raynor	Industry	Attendee
Maurice Jones	Industry	Attendee
Quinton Wilkes	Industry	Attendee
Rhonda Peyton	Industry	Attendee
Debbie Young	Industry	Attendee
Gussie Scardina	Industry	Attendee
Vince Jarvie	Industry	Attendee
Richard Knight	Industry	Attendee
Maurice Jones	Industry	Attendee
David Best	Information Security Oversight Office	Staff
Michael Manning	Information Security Oversight Office	Staff
Robert Tringali	Information Security Oversight Office	Staff
Joseph Taylor	Information Security Oversight Office	Staff

Attachment #2

.

Action Items from 11/19/2014 NISPPAC Meetings

ISOO will

1) Establish a NISPPAC Working Group, that will focus on security policy issues that require coordination due to their potential impact on NISP interactions, and which can enhance the integration between NISP guidance and other guidance in the government.

2) Reconvene the NISPPAC's Ad-hoc Special Access Program (SAP) Working Group to refocus on issues such as: the inconsistent application of policy, two person integrity, 8570 Certification , and the status of policy development and implementation.

Attachment #3

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

Industry

19 November 2014

Outline

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

National Industrial Security Program

Policy Advisory Committee Industry Members

Members	Company	Term Expires
Rick Graham	Huntington Ingalls Industries	2015
Steve Kipp	L3 Communications	2015
J.C. Dodson	BAE Systems	2016
Tony Ingenito	Northrop Grumman Corp.	2016
Bill Davidson	KeyPoint Government Solutions	2017
Phil Robinson	CGI Federal	2017
Michelle Sutphin	American Systems Corp.	2018
Martin Strones	Strones Enterprises	2018

National Industrial Security Program

Industry MOU Members

AIA *	J.C. Dodson
ASIS *	Jim Shamess
CSSWG	Mark Rush
ISWG	Karen Duprey
NCMS	Leonard Moss
NDIA	Mike Witt
Tech America	Kirk Poulsen

* Change in MOU Rep in Jan 2015

Security Policy Update

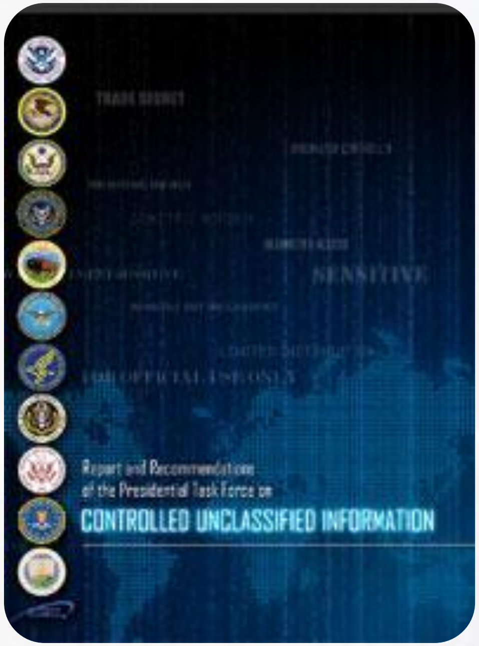
Executive Order #13556

EO # 13556

Controlled Unclassified Information (CUI)

4 NOV 2010

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



Report and Recommendations of the Presidential Task Force on CONTROLLED UNCLASSIFIED INFORMATION

- Next Steps
  - Monitor development of marking, safeguarding, dissemination and IT Security policy
  - CUI rules and User Agency comments being worked. Expecting update to be circulated prior to Federal Registry posting
  - NIST CUI standards developed (SP 800-171). Expect posting 18 Nov. for public comment.
  - Begin working with FAR Council on specific CUI clause.

Security Policy Update

Executive Order #13587

EO # 13587

Structural Reforms to improve security of classified networks

7 OCT 2011

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

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

INSIDER THREAT

- Directing structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks
  - Integrating Information Security, Personnel Security and System Security
- Need consistent requirement across all the User Agencies relating to implementation SOPs.
- Monitoring eight separate policy/directive actions across the government and providing input where possible.
  - Fractured implementation guidance being received via agency/command levels.

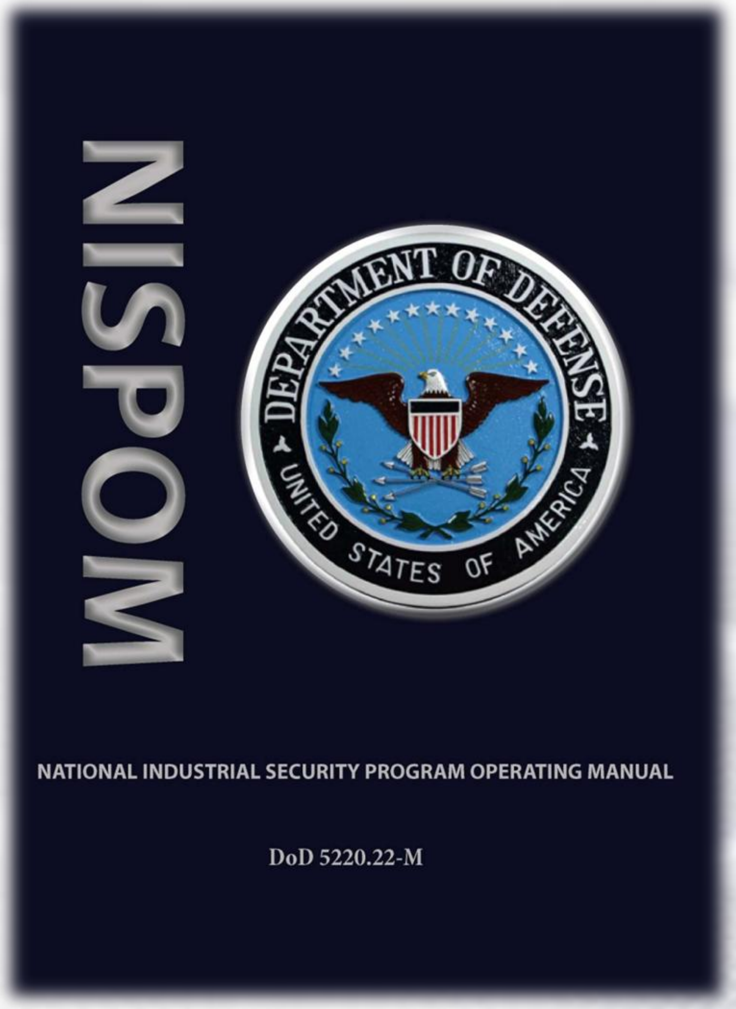
Security Policy Update

IT Security

- Defense Federal Acquisition Regulation Supplement (DFARS) Unclassified IT Security
  - Establishes security measures for IT across the Defense Industrial Base (DIB)
  - Greater emphasis on network security and IT incident reporting
  - Share threats and vulnerabilities throughout DIB
- IMPACT
  - Other government agencies moving forward with imposing IT Security measures and requirements
    - Controls are being interpreted differently by various programs and agencies, this creates multiple/duplicative approval tracks for industry.
    - Concerns developing with retribution and potential contract losses.

Security Policy Update

Industrial Security Policy Modernization



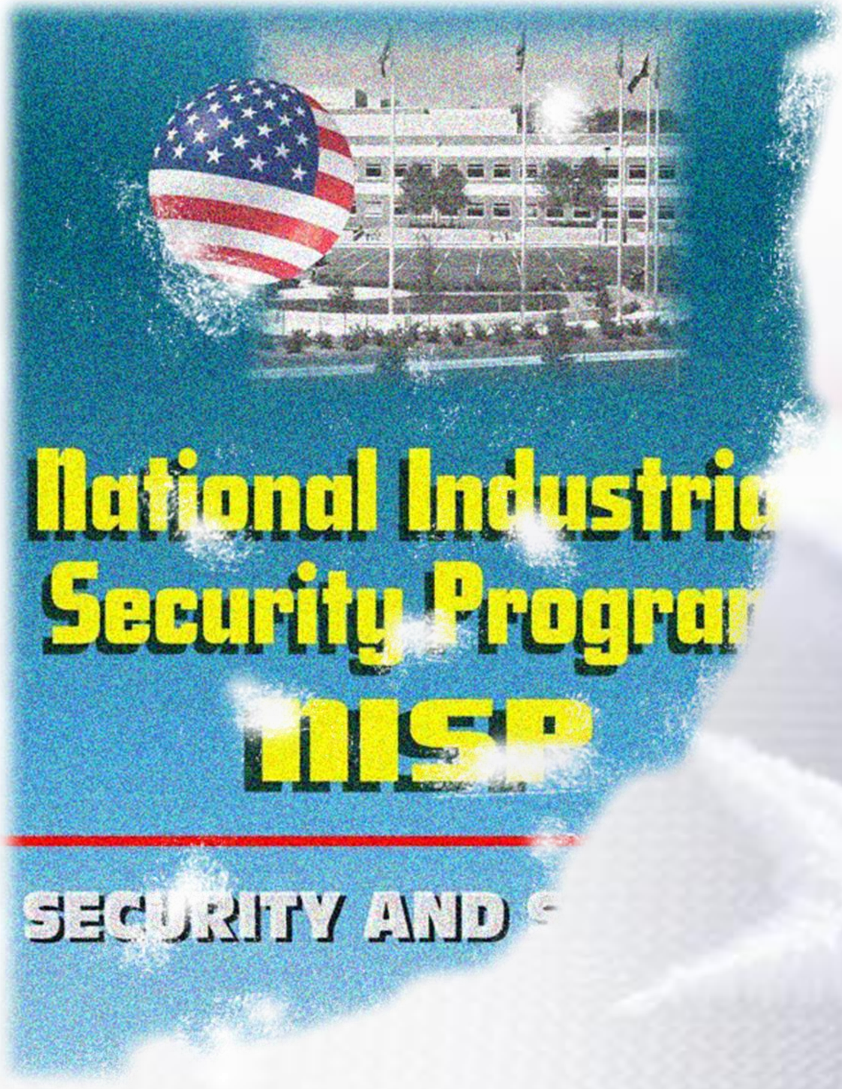
NISPOM

NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL

DoD 5220.22-M

- National Industrial Security Program Operating Manual revision and update
  - Industry provided comments on draft Jun/July 2010
- Department of Defense Special Access Program Manual development
- Industrial Security Regulation, Volume II update
- Special Access Program (SAP) Supplement being eliminated
- IMPACT
  - Industry working under a series of interim directions
  - Strong industry coordination for this interim direction is inconsistent
  - Delay of single, integrated policy is leading to differing interpretation of interim direction by user agencies

Fracturing of the NISP



- National & world events have stimulated reactions for policy changes and enhanced directives to counter potential vulnerabilities
  - Key areas include Cyber Security, Insider Threat and PERSEC.
- Process for directive/policy development and promulgation has become cumbersome and complicated.
  - Multiple years in most cases.
- Complications and delays have resulted in fractured lower level organization implementing a singular focused plan.
  - Inconsistency among guidance received.
- Driving increased cost for implementation and not flowing changes thru contract channels
- Tracking in excess of 50 initiatives
- Establish formal NISPPAC Working Group to address root cause and solutions

National Industrial Security Program

Policy Advisory Committee Working Groups

- Personnel Security
  - Working group moving out to address areas of concern.
    - E-adjudication business rules. Ensure aligned with new Federal Investigative Standards
    - DOHA SOR Process. Definitively ID true caseload and aging of those cases.
    - Security clearance validation.
    - Risk in adjudication backlog. Sequestration recovery plan making progress
    - USIS investigation case load. Reassigned and 33% have closed.
- Automated Information System Certification and Accreditation
  - Provided DSS & OSD suggested XP End of Life guidance to mitigate the impacts across existing programs, including testing equipment. Need to get guidance published
  - Engage IC and SAP C&A Communities relating to CC #2 (Note: will push the C&A process to CSA provided guidance. Engaging industry in the guide development).

National Industrial Security Program

Policy Advisory Committee Working Groups (cont.)

- Ad-hoc
  - NISPOM Rewrite Working Group
    - Awaiting further actions relating to NISPOM and Conforming Change #2. Now looking at 3rd Qt FY15 timeframe
  - NISP Contractor Classification System (NCCS) – Automated DD254 system
    - Expected to participate in beta test with 25 Industry testers
  - Development of National Industrial Security System (NISS)
    - Participated on the system requirements phase and standing by for further development meetings.
- ISOO sponsored Ad-hoc SAP Working Group
  - Numerous situations with inconsistent guidance and implementation of changes relating to JSIG (RMF) and TPI.
  - Requesting to formalize this working group.

Attachment #4

Personnel Security Working Group (PCLWG) Report

- NISPPAC action items from 6/19/2014 meeting: (See attachment 2 in folder)

- OPM Performance metrics data from DoD, DOE, NRC, as well as the PSMO update are in folders and will be posted with NISPPAC minutes. Highlights:

  - PSMO reports:
    - e-fingerprinting submission rate now at 94%, and
    - Overdue PRs at 8,550 (10/14) down from 30,154 (6/14).

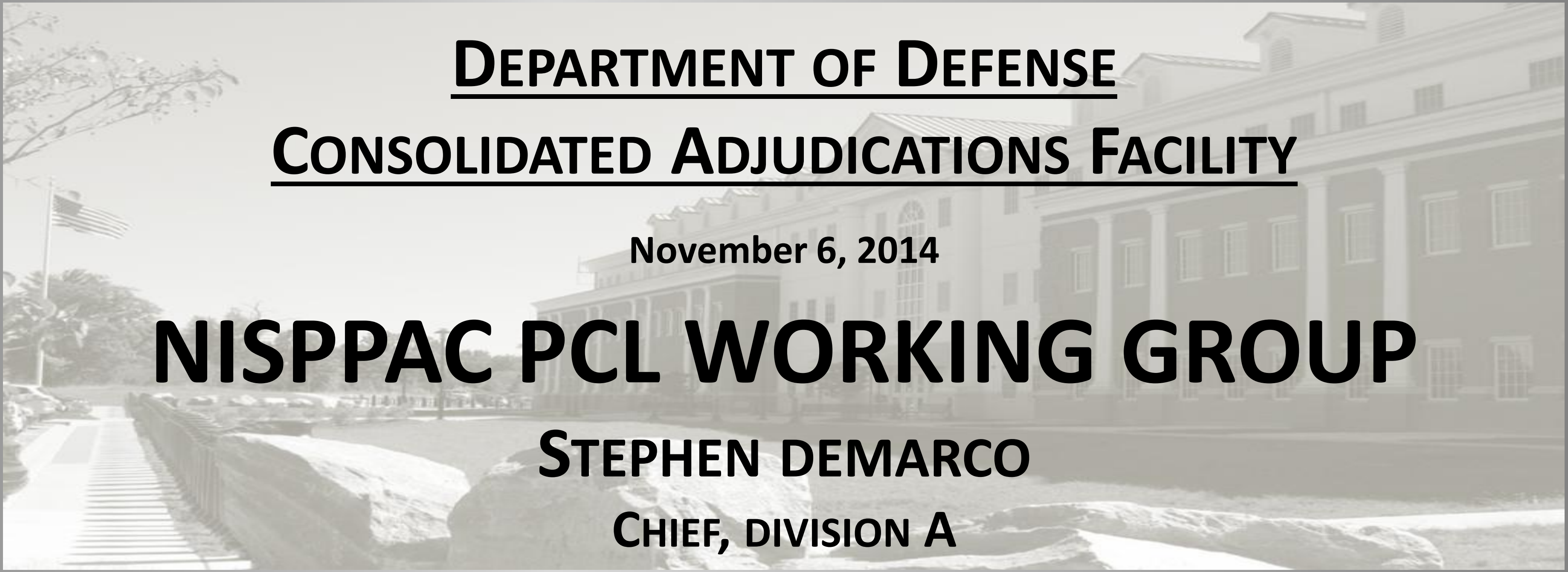
- Meetings held on 8/26/2014 and November 6, 2014. Highlights included:

  - Recommendation to raise threshold on business rules for e-adjudication, (OUSDI and DODCAF working with OPM and ODNI to effect changes).

  - OUSDI (Personnel) agreed to initiate a “data quality initiative” that would identify case files marked “at DOHA” and then change the notation to “Pending Adjudication”.

  - Review of security clearance validation process concluded that the use of the wrong process for DoD Credentialing has resulted in resource issues that impact both time and cost that should be devoted to security clearances for industry.

Attachment #5



Department of Defense

Consolidated Adjudications Facility

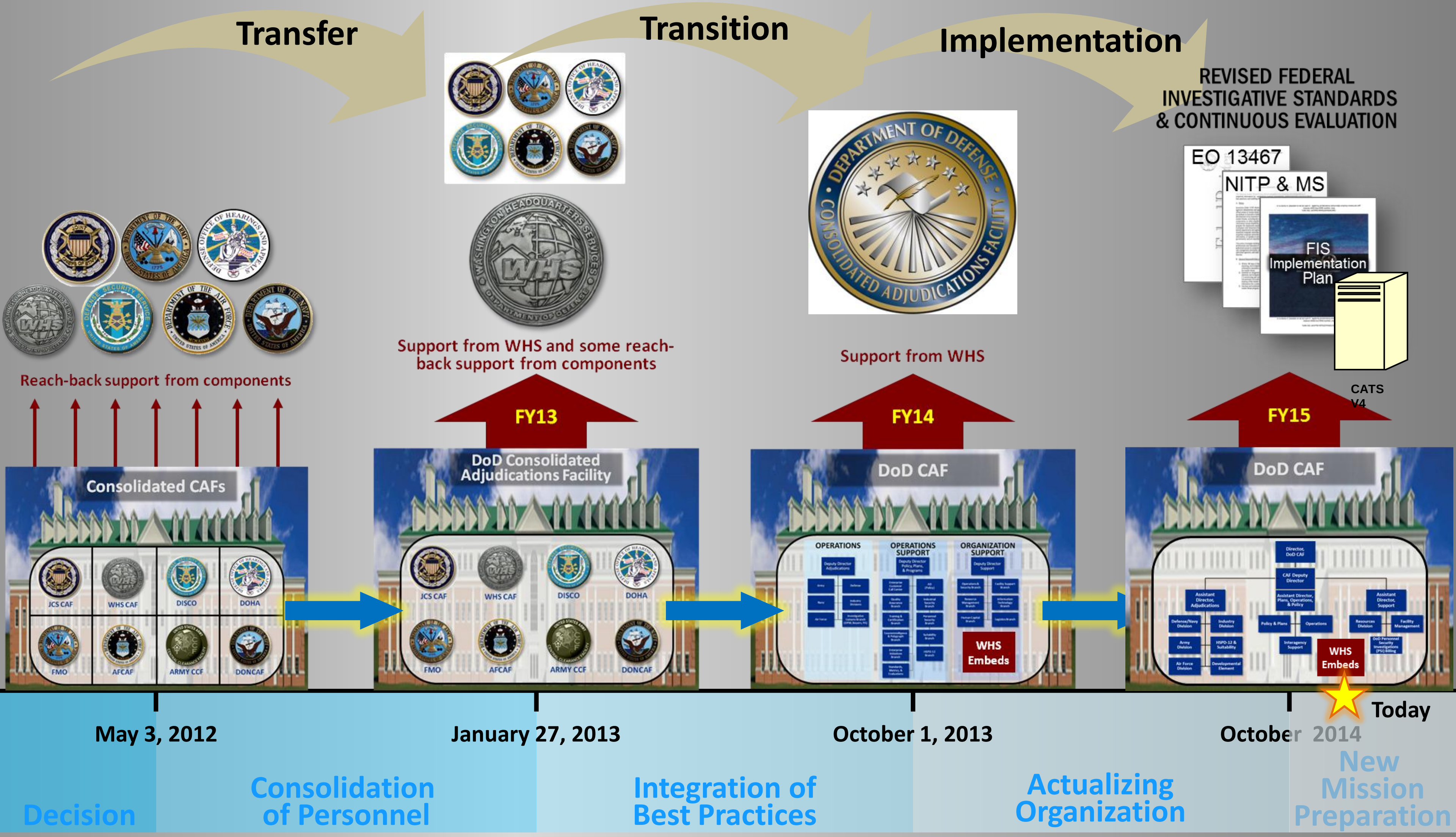
November 6, 2014

NISPPAC PCL WORKING GROUP

Stephen demarco

Chief, division A

DoD CAF Transformation



Transfer

Transition

Implementation

REVISED FEDERAL INVESTIGATIVE STANDARDS & CONTINUOUS EVALUATION

EO 13467

NITP & MS

FIS Implementation Plan

CATS V4

Reach-back support from components

Support from WHS and some reach-back support from components

Support from WHS

FY13

FY14

FY15

Consolidated CAFs

DoD Consolidated Adjudications Facility

DoD CAF

DoD CAF

JCS CAF
WHS CAF
DISCO
DOHA
FMO
AFCAF
ARMY CCF
DONCAF
OPERATIONS
OPERATIONS SUPPORT
ORGANIZATION SUPPORT
Deputy Director Adjudications
Army
Defense
Navy
Industry Divisions
Air Force
Investigation Liaison Branch (OPM, Reports, PS)
Deputy Director Policy, Plans, & Programs
Enterprise Customer Call Center
AIS (Policy)
Quality Assurance Branch
Industrial Security Branch
Training & Certification Branch
Personnel Security Branch
Counterintelligence & Polygraph Branch
Suitability Branch
Enterprise Initiatives Branch
HSPD-12 Branch
Standards, Metrics, & Evaluations
Deputy Director Support
Operations & Security Branch
Facility Support Branch
Resource Management Branch
Information Technology Branch
Human Capital Branch
Logistics Branch
WHS Embeds
Director, DoD CAF
CAF Deputy Director
Assistant Director, Adjudications
Assistant Director, Plans, Operations, & Policy
Assistant Director, Support
Defense/Navy Division
Industry Division
Army Division
HSPD-12 & Suitability
Air Force Division
Developmental Element
Policy & Plans
Operations
Interagency Support
Resources Division
Facility Management
DoD Personnel Security Investigations (PSI) Billing
WHS Embeds

May 3, 2012

January 27, 2013

October 1, 2013

October 2014

Today

Decision

Consolidation of Personnel

Integration of Best Practices

Actualizing Organization

New Mission Preparation

Federal "End-to-end" Timeliness for Initial Clearances (September 14)

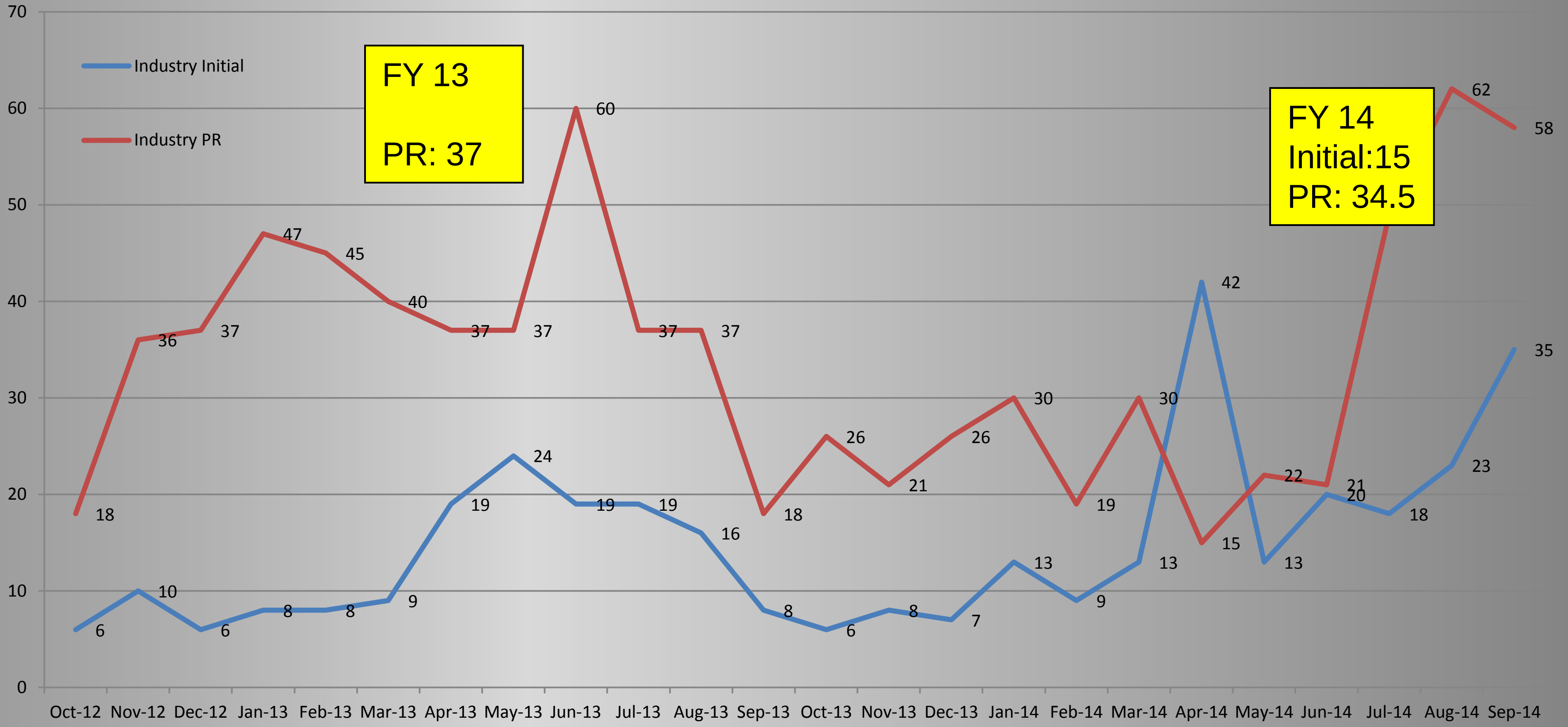
All Agencies	60 days
Defense	57 days
Army	51 days
Navy	45 days
Air Force	51 days
Industry	97 days
Homeland Security	129 days
Energy	77 days
DHHS	130 days
Justice	111 days
OPM	58 days
Transportation	61 days
Interior	100 days
NRC	92 days
Treasury	103 days
VA	82 days
Agriculture	83 days
Commerce	68 days
NASA	70 days
GSA	103 days
NARA	
EPA	65 days
SSA	n/a days
HUD	n/a days
Labor	151 days
FCC	126 days
Education	359 days
NSF	107 days

- IRTPA "end-to-end" Objective ≤ 60 days

- DoD CAF Specific Timelines:
  - Initial (All Types) – Adjudicated in 4 of 20 days
  - SSBI-PRs – Adjudicated in 15 of 30 days

- Industry Specific Timelines:
  - Initial (All Types) – Adjudicated in 35 of 20 days
  - SSBI-PRs – Adjudicated in 58 of 30 days

Industry
Intelligence Reform and Terrorism Prevention Act Performance



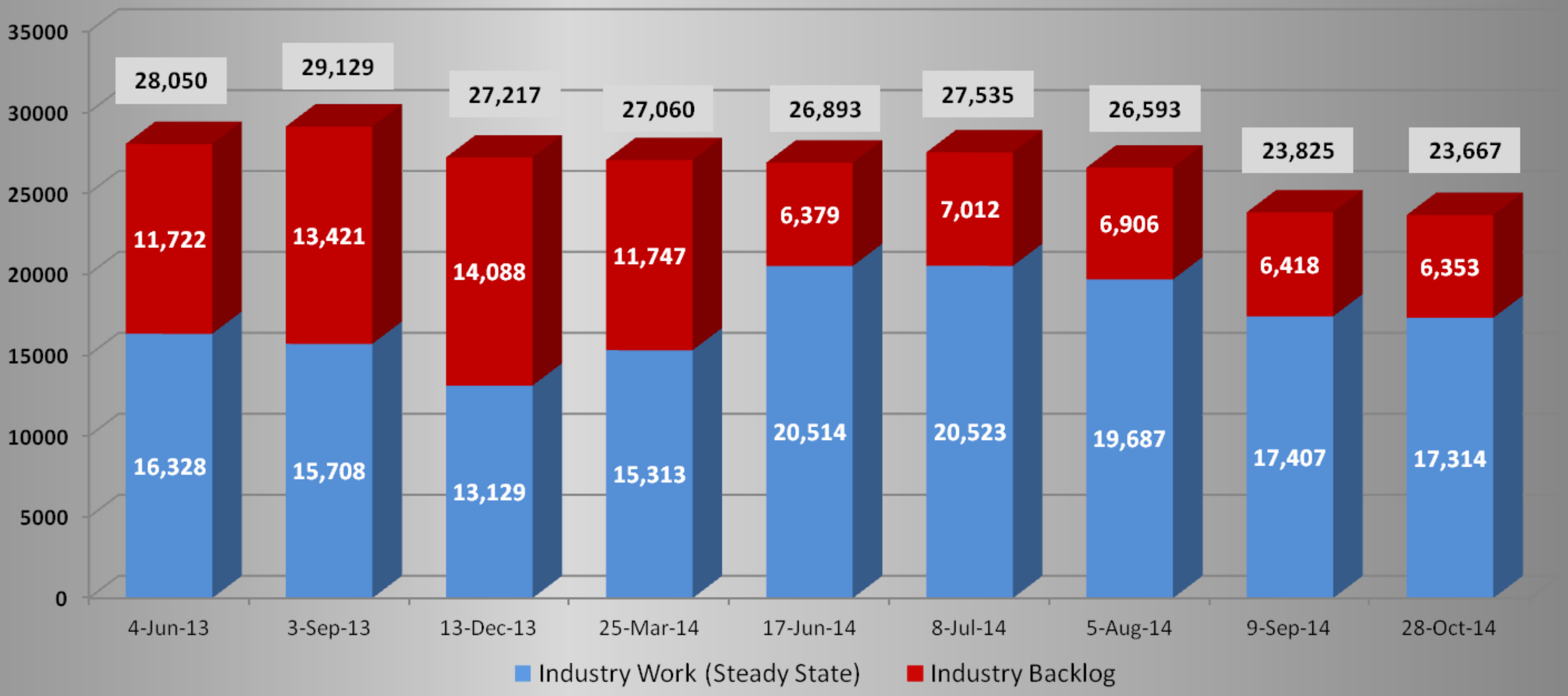
FY 13

PR: 37

FY 14
Initial:15
PR: 34.5

- •Timeliness to fluctuate/increase in FY15 until IND backlog eliminated
- •Overall DoD CAF timeliness also edged up in FY14 as backlogs addressed
- •FY14 4Q IND ingest increased by ~25% ; likely due to increased DSS funding for PRs

Pending Industrial Workload



* Additional ~5,000 JPAS IRs >20 days

- **Backlog likely to endure into late-2015:**
  - **Deploy single OPS system (CATS) in FY15 will affect production**
  - **FY 14/15 CE pilots to increase overall CAF workload**

Month	NISP Backlog	Annual NISP Receipt	Backlog % of Total NISP
October 13	13,515		8.1%
October 14	6,353		3.1%
	-7,162	~ 200,000	

Attachment #6

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Industry Performance Metrics

ONCIX/Special Security Directorate

LEADING INTELLIGENCE INTEGRATION

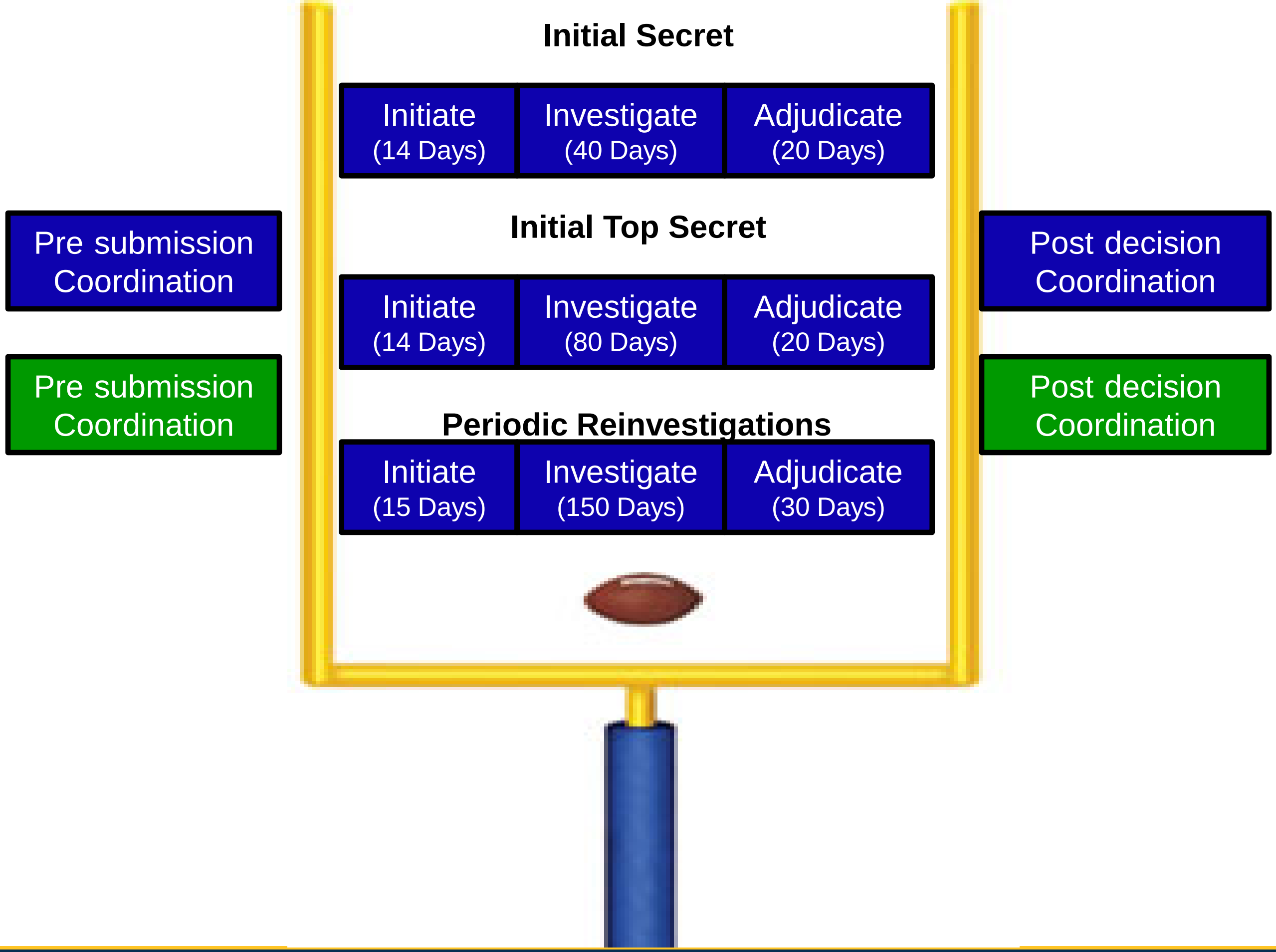
PCL Working Group
28 May 2014

Performance Accountability Council(PAC) Security Clearance Methodology

- Timeliness data on the following slides reflects USG performance on Contractor cases

- 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



Pre submission Coordination

Pre submission Coordination

Initial Secret

Initiate (14 Days) | Investigate (40 Days) | Adjudicate (20 Days)

Initial Top Secret

Initiate (14 Days) | Investigate (80 Days) | Adjudicate (20 Days)

Periodic Reinvestigations

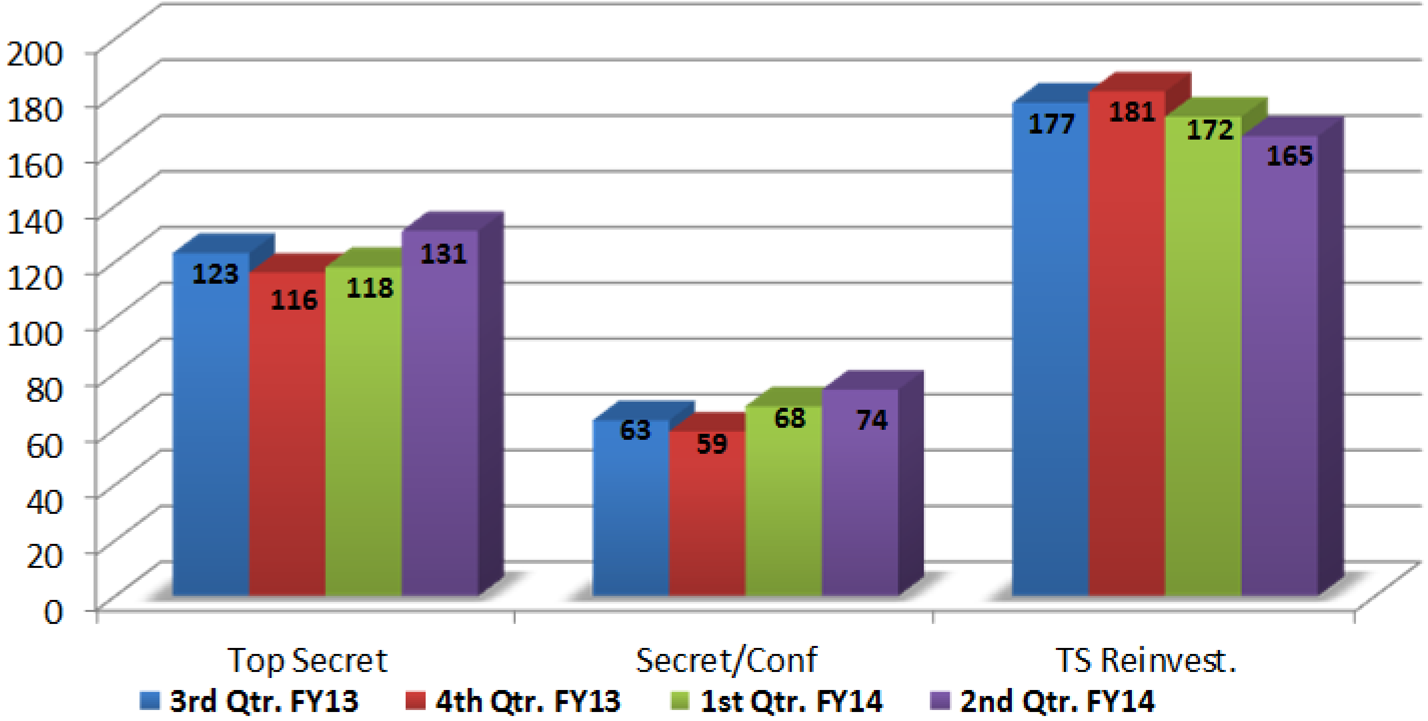
Initiate (15 Days) | Investigate (150 Days) | Adjudicate (30 Days)

Post decision Coordination

Post decision Coordination

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

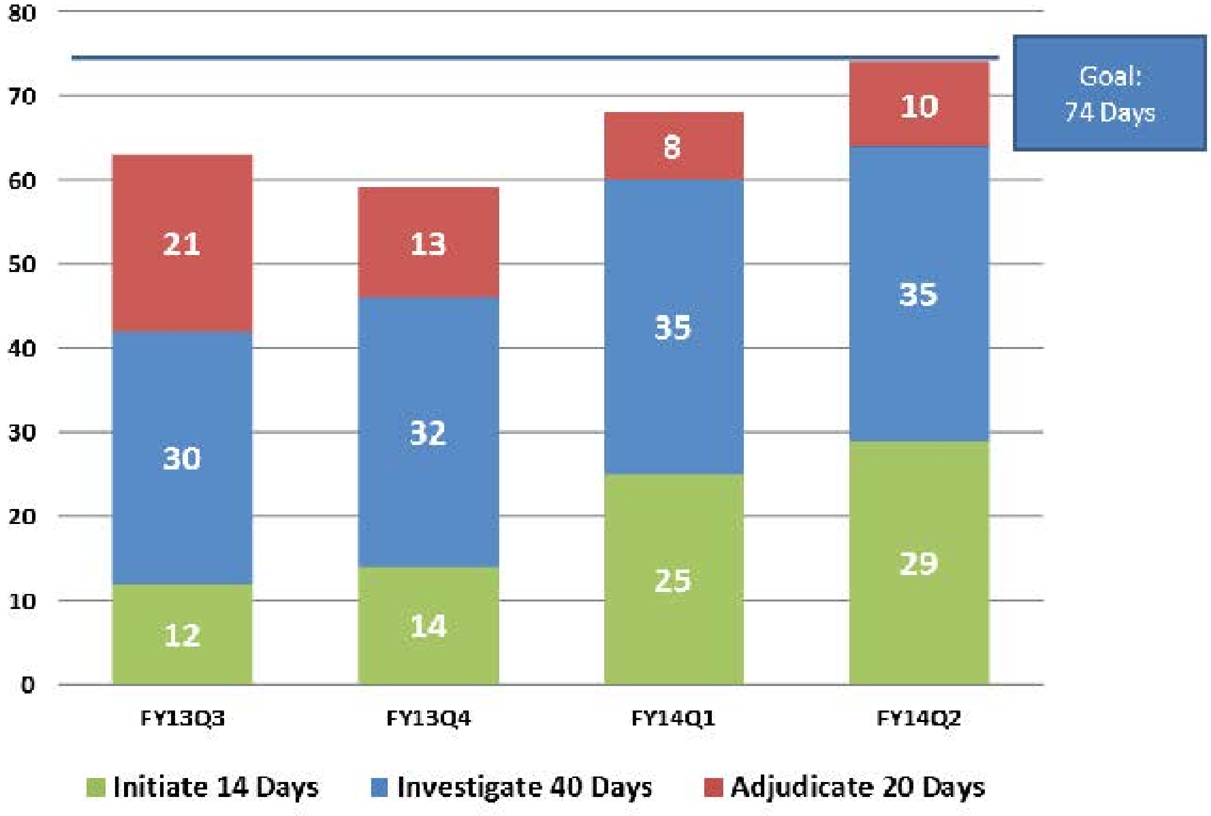
Average Days of Fastest 90% of Reported Clearance Decisions Made



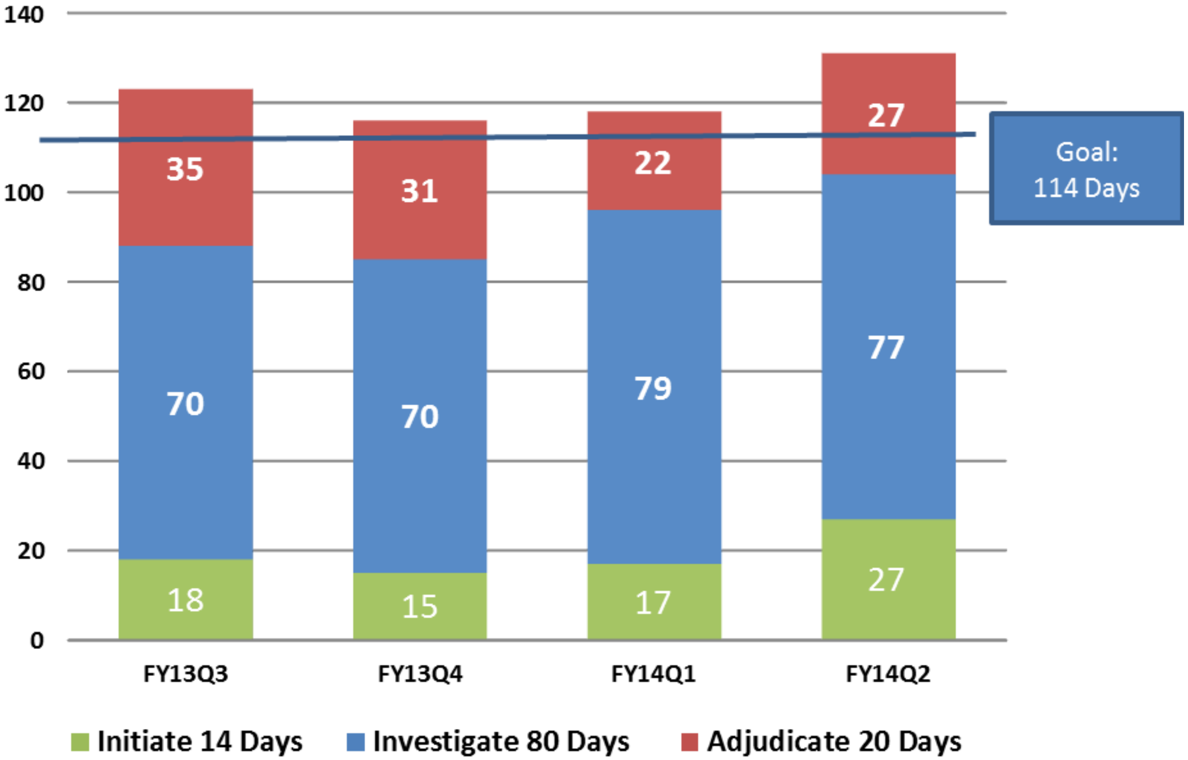
	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 3rd Q FY13	8,883	20,981	12,385
Adjudication actions taken – 4th Q FY13	9,268	20,165	18,807
Adjudication actions taken – 1st Q FY14	5,802	13,858	12,918
Adjudication actions taken – 2nd Q FY14	6,306	17,594	15,363

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

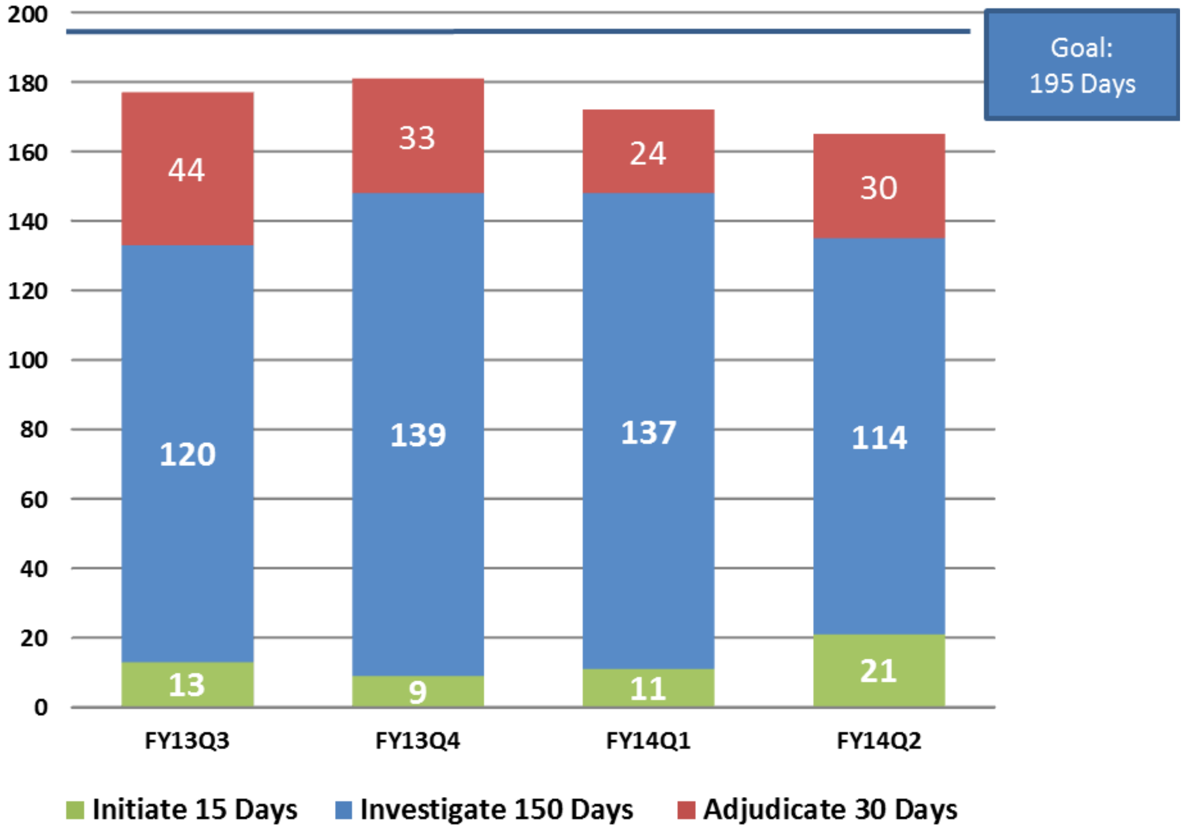
IC and DoD Industry Secret Clearances



IC and DoD Industry Top Secret Clearances



IC and DoD Industry Periodic Reinvestigations



2012 Intelligence Authorization Act Report on Security Clearance Determinations

Format used in 2012:

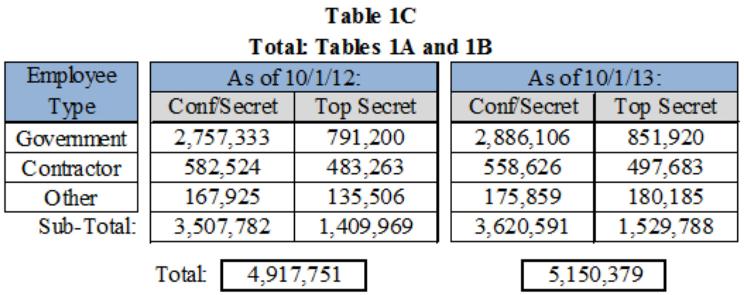


Table 1C
Total: Tables 1A and 1B

Employee Type	As of 10/1/12:		As of 10/1/13:	
	Conf/Secret	Top Secret	Conf/Secret	Top Secret
Government	2,757,333	791,200	2,886,106	851,920
Contractor	582,524	483,263	558,626	497,683
Other	167,925	135,506	175,859	180,185
Sub-Total:	3,507,782	1,409,969	3,620,591	1,529,788
Total:	4,917,751		5,150,379	

Further detail in 2013:

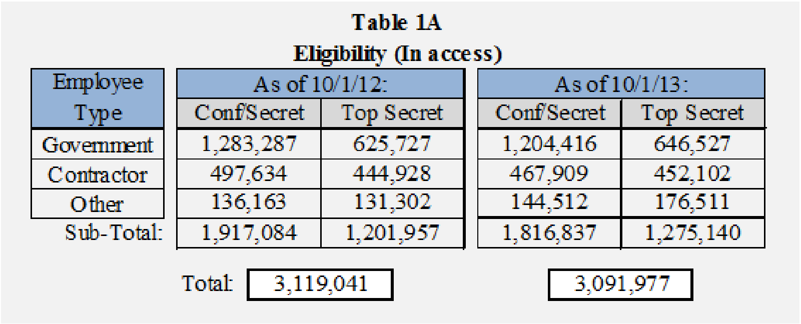


Table 1A
Eligibility (In access)

Employee Type	As of 10/1/12:		As of 10/1/13:	
	Conf/Secret	Top Secret	Conf/Secret	Top Secret
Government	1,283,287	625,727	1,204,416	646,527
Contractor	497,634	444,928	467,909	452,102
Other	136,163	131,302	144,512	176,511
Sub-Total:	1,917,084	1,201,957	1,816,837	1,275,140
Total:	3,119,041		3,091,977	

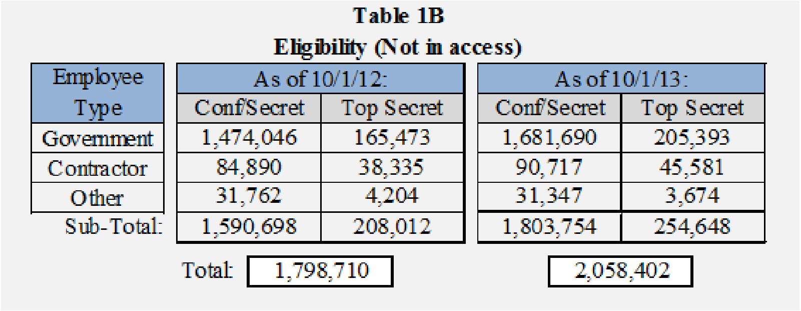


Table 1B
Eligibility (Not in access)

Employee Type	As of 10/1/12:		As of 10/1/13:	
	Conf/Secret	Top Secret	Conf/Secret	Top Secret
Government	1,474,046	165,473	1,681,690	205,393
Contractor	84,890	38,335	90,717	45,581
Other	31,762	4,204	31,347	3,674
Sub-Total:	1,590,698	208,012	1,803,754	254,648
Total:	1,798,710		2,058,402	

Contact information:
Christy Wilder
571-204-6502 (W)
93-58834 (S)

Attachment #7

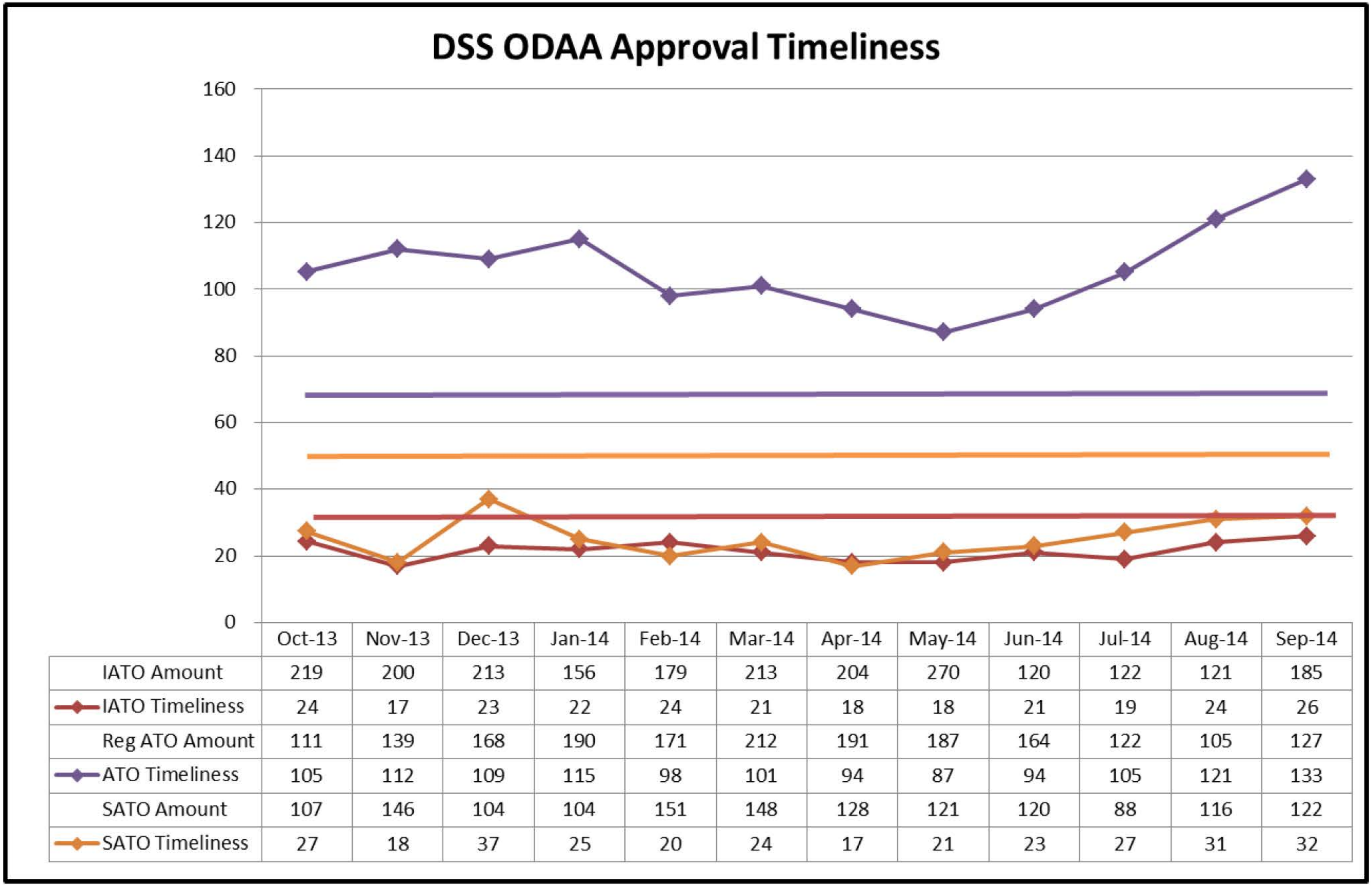
NISPPAC C&A Working Group Update for the Committee

November 2014

Working Group Initiatives

- Validation Tools Currently Under Evaluation
- Evaluate Change Management Process for the ODAA Process Manual

ISFO – ODAA



	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14	May-14	Jun-14	Jul-14	Aug-14	Sep-14
IATO Amount	219	200	213	156	179	213	204	270	120	122	121	185
◆ IATO Timeliness	24	17	23	22	24	21	18	18	21	19	24	26
Reg ATO Amount	111	139	168	190	171	212	191	187	164	122	105	127
◆ ATO Timeliness	105	112	109	115	98	101	94	87	94	105	121	133
SATO Amount	107	146	104	104	151	148	128	121	120	88	116	122
◆ SATO Timeliness	27	18	37	25	20	24	17	21	23	27	31	32

Takeaways:

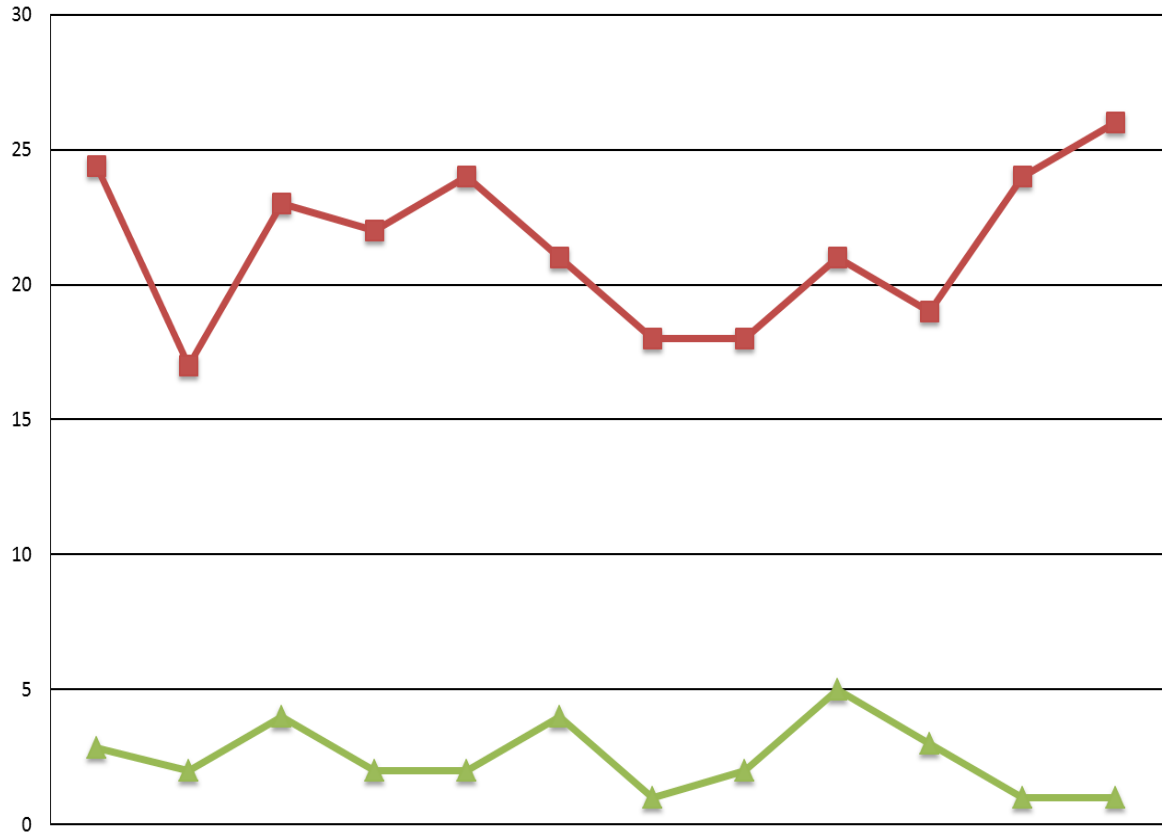
- Security Plans are Being Processed and Reviewed in a Timely Manner
  - Most Common Deficiencies in SSPs Include Missing Attachments and Documentation Errors
- Onsite Validations are Being Completed in a Timely Manner
  - Most Common Vulnerabilities Identified During System Validation Include Auditing Controls, Configuration Management, Not Protecting Security Relevant Objects
- More Straight to ATO (Where Practical) to Reduce Risk and Increase Efficiency

Back-Up Slides

NISPPAC C&A Working Group

Sept 2014

Security Plan Review Results from Aug 2013- Sept 2014



	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14	May-14	Jun-14	Jul-14	Aug-14	Sep-14
Total IATOs	219	200	213	156	179	213	204	270	120	122	121	185
▲ Industry Response Time to DSS Questions, Comments	3	2	4	2	2	4	1	2	5	3	1	1
# Second IATOs	21	14	19	13	5	9	5	8	4	4	10	11
■ Time from DSS Receipt of plans to Granting of IATOs	24	17	23	22	24	21	18	18	21	19	24	26

3974 SSPs were reviewed

22202 IATOs were issued

Avg. 21 days to issue an IATO

1455 SATO were processed

25 days to issue a SATO.

976 of the SSPs (25%) required some level of correction

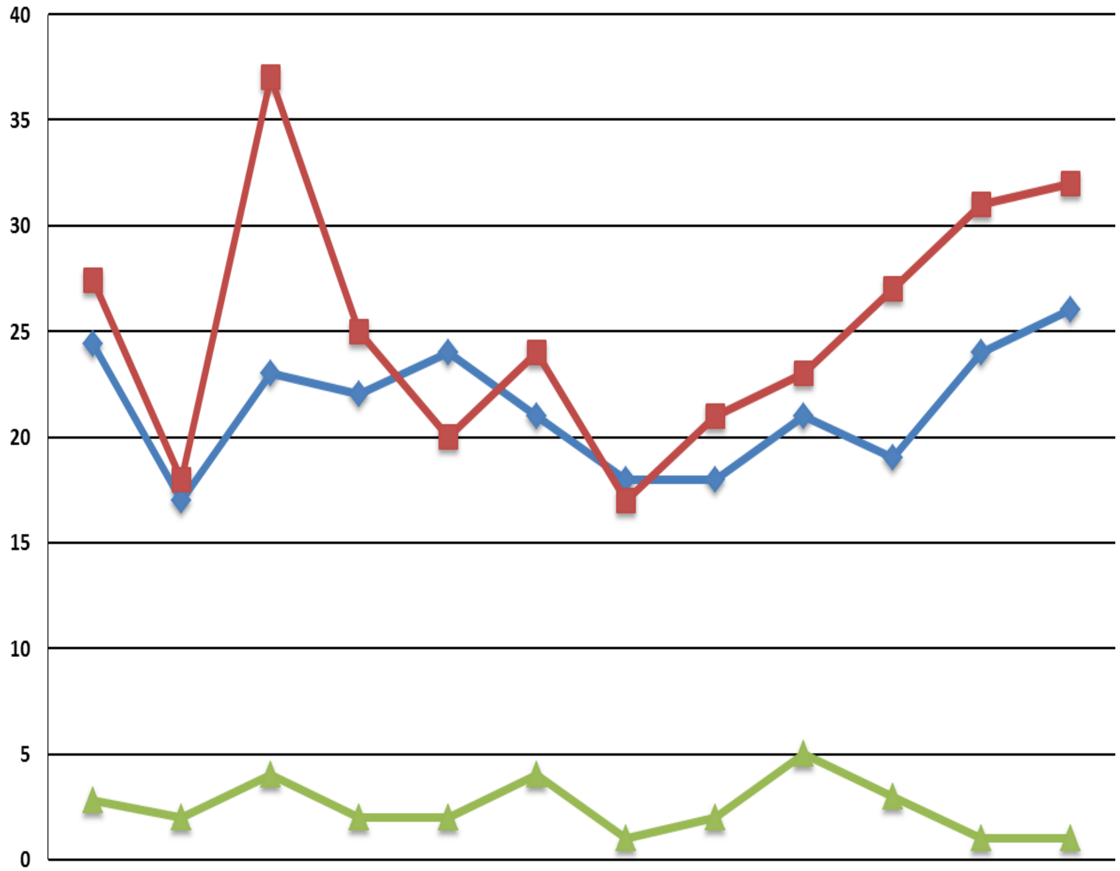
- 635 of the SSPs (16%) were granted IATO with corrections required.

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

- 252 of the SSPs (6%) were reviewed and denied IATO. (resubmitted after corrections)

- 65 of the SSPs (2%) were not submitted in accordance with requirements and were rejected. (resubmitted after corrections)

Security Plan Review Results from Aug 2013- Sept 2014



	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14	May-14	Jun-14	Jul-14	Aug-14	Sep-14
◆ Time from DSS Reciept of plans to Granting of IATOs	24	17	23	22	24	21	18	18	21	19	24	26
■ Time from DSS Reciept of plans to Granting of SATOs	27	18	37	25	20	24	17	21	23	27	31	32
▲ Industry Response Time to DSS Questions, Comments	3	2	4	2	2	4	1	2	5	3	1	1
Second IATOs	21	14	19	13	5	9	5	8	4	4	10	11

3974 System security plans (SSPs) were accepted and reviewed during the preceding 12 months.

2202 Interim approvals to operate (IATOs) were issued during the preceding 12 month period, it took an average of 21 days to issue an IATO after a plan was submitted.

1455 “Straight to ATO (SATO)” were processed during the preceding 12 months, it took an average of 25 days to issue the ATO.

976 of the SSPs (25%) required some level of correction prior to conducting the onsite validation.

635 of the SSPs (16%) were granted IATO with corrections required.

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

Denials: 252 of the SSPs (6%) were received and reviewed, but denied IATO until corrections were made to the plan.

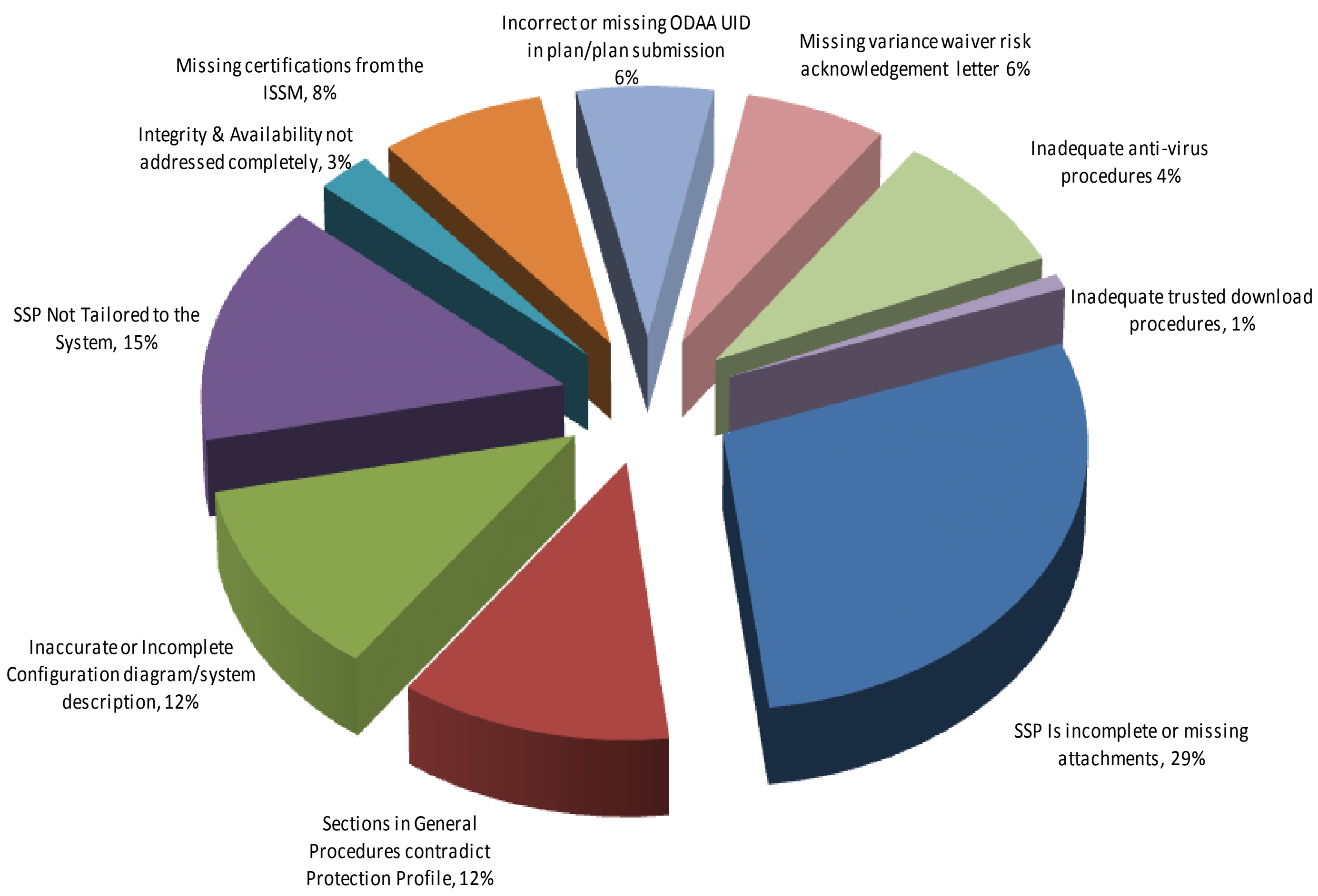
Rejections: 65 of the SSPs (2%) were not submitted in accordance with requirements and were not entered into the ODAA process. These SSPs were returned to the ISSM with guidance for submitting properly and processed upon resubmission.

Last Months Snapshot: September 2014

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

122 SATOs were granted with an average turnaround time of 32 days

Common Deficiencies in Security Plans from Aug 2013- Sept 2014



	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14	May-14	Jun-14	Jul-14	Aug-14	Sep-14
# Deficiencies	178	148	137	197	146	178	179	258	154	102	69	86
# Plans w/ Deficiencies	101	83	90	76	89	92	90	140	87	64	56	73
# Plans Reviewed	364	376	338	282	357	396	363	431	275	228	247	317
Avg Deficiency per Plan	0.49	0.39	0.41	0.70	0.41	0.45	0.49	0.60	0.56	0.45	0.28	0.27
Denials	29	19	16	17	22	31	28	30	26	14	10	10
Rejections	9	11	5	5	5	4	3	10	9	4	0	0

Top 10 Deficiencies

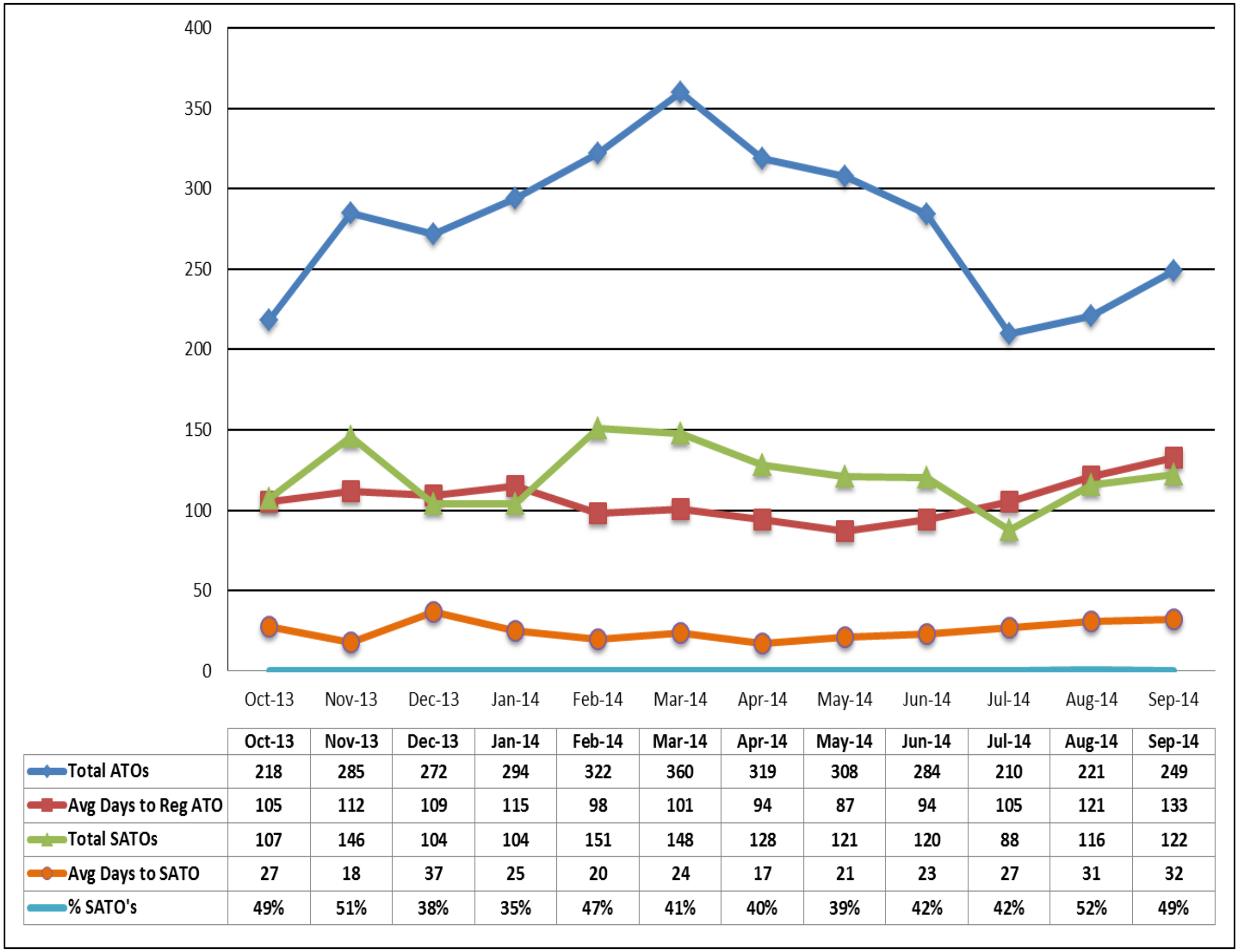
1. SSP Is incomplete or missing attachments
2. SSP Not Tailored to the System
3. Inaccurate or Incomplete Configuration diagram or system description
4. Sections in General Procedures contradict Protection Profile
5. Missing certifications from the ISSM
6. Missing variance waiver risk acknowledgement letter
7. Incorrect or missing ODAA UID in plan submission
8. Inadequate anti-virus procedures
9. Integrity & Availability not addressed completely
10. Inadequate trusted download procedures

NISPPAC C&A Working Group

Sept 2014

On Site Review Results from Aug 2013- Sept 2014

Performance: Metrics reflect excellent performance across the C&A program nationwide. Improvements have been made in the number of systems processed straight ATO and reducing the number of days systems operate on an IATO when compared to six months ago. We are averaging over 44% of all ATOs being straight to ATO.



	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14	May-14	Jun-14	Jul-14	Aug-14	Sep-14
Total ATOs	218	285	272	294	322	360	319	308	284	210	221	249
Avg Days to Reg ATO	105	112	109	115	98	101	94	87	94	105	121	133
Total SATOs	107	146	104	104	151	148	128	121	120	88	116	122
Avg Days to SATO	27	18	37	25	20	24	17	21	23	27	31	32
% SATO's	49%	51%	38%	35%	47%	41%	40%	39%	42%	42%	52%	49%

3187 completed validation visits we completed during the preceding 12 months

1887 systems were processed from IATO to ATO status during the preceding 12 months, it took 105 days on average to process a system from IATO to ATO

1445 systems were processed Straight to ATO status during the preceding 12 months, it took 25 days on average to process a system Straight to ATO

Across the 12 months, (44%) of ATOs were for systems processed Straight to ATO

2356 systems (74%) had no vulnerabilities identified.

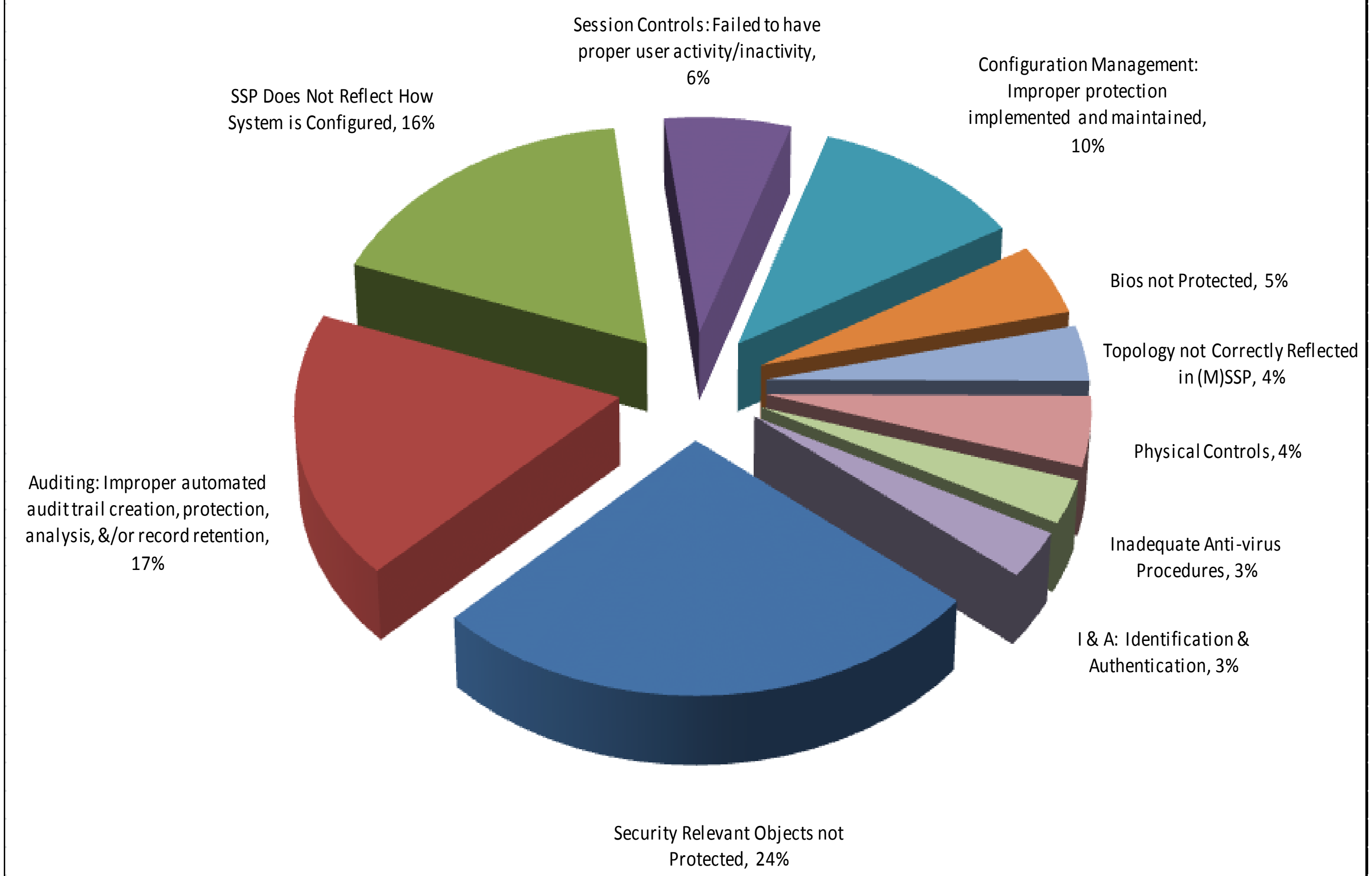
763 systems (24%) had minor vulnerabilities identified that were corrected while onsite.

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

Last Months Snapshot: Sept 2014
127 ATOs were granted with an average turnaround time of 133 days

122 SATOs were granted with an average turnaround time of 32 days

Common Vulnerabilities found during System Validations from Aug 2013- Sept 2014



	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14	May-14	Jun-14	Jul-14	Aug-14	Sep-14
# Vulnerabilities	133	66	86	102	114	133	96	76	114	77	53	81
# Onsites w/ vulnerabilities	74	45	70	70	78	90	81	62	84	52	59	64
# Onsites	204	267	263	283	309	342	295	301	260	212	211	238
Avg Vulnerability per Onsite	0.65	0.25	0.33	0.36	0.37	0.39	0.33	0.25	0.44	0.36	0.25	0.34

Top 10 Vulnerabilities

1. Security Relevant Objects not protected.
2. Auditing: Improper automated audit trail creation, protection, analysis, &/or record retention
3. SSP does not reflect how the system is configured
4. Inadequate configuration management
5. Improper session controls: Failure to have proper user activity/inactivity, logon, system attempts enabled.
6. Bios not protected
7. Topology not correctly reflected in (M)SSP
8. Physical security controls
9. Inadequate Anti-virus procedures
10. Identification & authentication controls

Attachment #8

Three-Part Plan

- Purpose – to standardize the requirements for CUI both within the Federal Government and when such information resides in nonfederal information systems and organizations.
- Three-parts:
  - Incorporating uniform CUI policies and practices into the Code of Federal Regulations
  - Using NIST Special Publication to define requirements to protect the Confidentiality of CUI in the nonfederal environment
  - Developing a standard Federal Acquisition Regulation to protect CUI in the contractor community

NIST Special Publication 800-171

- ISOO collaborated with NIST on developing the draft NIST Special Publication
- Available for comment until January 16, 2015 at http://csrc.nist.gov/publications/PubsDrafts.html#800-171
- Purpose – to provide Federal agencies with recommended requirements for protecting the Confidentiality of CUI when such information resides in nonfederal information systems and organizations.
  - **The security requirements apply only to components of nonfederal information systems that process, store, or transmit CUI.**

Security Requirements

- Basic and derived security requirements obtained from the FIPS 200 and NIST SP 800-53 – and then tailored appropriately to eliminate requirements that are:
  - Primarily the responsibility of the Federal Government (uniquely Federal requirements).
  - Related primarily to availability.
  - Assumed to be routinely satisfied by nonfederal organizations without any further specification.