NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

SUMMARY MINUTES OF THE MEETING

The NISPPAC held its 40th meeting on Wednesday, November 16, 2011, at 10:00 a.m. in the Archivist's Reception Room at the National Archives and Records Administration, 700 Pennsylvania Avenue, NW, Washington, DC 20408. John Fitzpatrick, Director, Information Security Oversight Office (ISOO), chaired the meeting, which was open to the public. The following minutes were finalized and certified on January 13, 2012.

The following members or alternates were present:

- John Fitzpatrick, Chair
- Daniel McGarvey (Department of the Air Force)
- Booker Bland (Department of the Army)
- Stephen Lewis (Department of Defense)
- Richard Hohman (Office of the Director of National Intelligence)
- Stan Sims (Defense Security Service)
- Drew Winneberger (Defense Security Service)
- Richard Donovan (Department of Energy)
- George Ladner (Central Intelligence Agency)

Christal Fulton (Department of Homeland Security)
Dennis Hanratty (National Security Agency)
Derrick Broussard (Department of the Navy)
Kimberly Baugher (Department of State)
Rosalind Baybutt (Industry)
Scott Conway (Industry)
Shawn Daley (Industry)
Richard Graham (Industry)
Steven Kipp (Industry)
Frederick Riccardi (Industry)
Marshall Sanders (Industry)
Michael Witt (Industry)

I. Welcome, Introductions, and Administrative Matters

Mr. Fitzpatrick introduced himself as the new Chair and welcomed two new industry representatives, Steve Kipp and Rick Graham, thanking them for their willingness to serve. He thanked and acknowledged the service of Sheri Escobar and Christopher Beals of industry whose terms expired. He reminded the attendees that a NISPPAC meeting is a recorded and public event. After having each Committee member introduce himself/herself, the Chair asked Greg Pannoni, ISOO and the NISPPAC Designated Federal Official, to review old business.

II. Old Business

Mr. Pannoni described the first action item from the last meeting to form an ad-hoc working group to focus on issues affecting small and medium-sized companies. To that end, ISOO hosted a meeting on July 28, 2011, and discussed some of these issues, particularly those concerned with rejections of security clearances and system security plans. Future meetings of both the Personnel Security Clearance and the Certification & Accreditation Working Groups

will continue to focus on these areas. Next, he described a request from the Department of Defense (DoD) for an accounting of the number of remaining industry-operated non-GSA approved security containers, and stated that DoD would provide an update during this meeting. He then reviewed a request for ISOO to coordinate a presentation on "The Governance of the Insider Threat." He mentioned that the month of October 2011 saw the issuance of Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," designed to improve the security of classified networks as well as the responsible sharing and safeguarding of classified information. Further, that the new order focuses on, among other things, classified information systems, and prescribes minimum standards and guidance for the implementation of policy governing insider threat programs. He posited that the Chair would briefly describe governing aspects of this order, and in a future NISPPAC meeting, would summarize guidance related to ongoing developments in the insider threat program. Next, Mr. Pannoni alluded to a report on trends relating to a decline in the submission of Phased Periodic Reinvestigations (PPR), and stated that representatives of the Security and Suitability Executive Agent's (SEA), PPR Working Group would provide an update on continuing efforts to ensure consistency in the application of the PPR process. Finally, he described the last action item concerning the formation of an ad-hoc working group to address how appropriate threat data may be expeditiously disseminated to National Industrial Security Program (NISP) facilities. He explained that ISOO had subsequently hosted a July 28, 2011 meeting to address these issues and to identify the pathway ahead. He also announced that DoD, in support of this initiative, will host an all-day Threat Information Workshop at the Collaboration Center in Quantico, VA on December 1, 2011. Finally, he called for working group updates, and began with Randy Riley of the Defense Security Service (DSS).

III. Working Group Updates

A) Certification & Accreditation Working Group (CAWG) Report

Mr. Riley presented an update (Attachment #1) of recent activity of the CAWG. He defined the primary function of the Working Group as an examination of the processes for certifying and accrediting information systems. He explained that DSS is the Designated Approval Authority (DAA) and the Cognizant Security Authority (CSA) on behalf of industry, and as such is responsible for accrediting information systems. He emphasized several key points with regard to DAA's responsibilities in the certification and accreditation process, most notably that the process ensures that information system security controls are in place to limit the risk of compromising national security information, that they provide a structure to efficiently and effectively manage a certification and accreditation process, and that the process ensures adherence to national industrial security standards.

Mr. Riley noted that the systems metrics data, covering the period October 2010 through September 2011, reflects continued improvement in the timelines for issuing Interim Approval to Operate (IATO) and Approval to Operate (ATO) certificates. With regard to System Security Plan (SSP) review metrics, the data continues to reflect that one third or more of all plans required changes prior to the on-site review, and about one fourth of the systems required some

level of modification during the on-site verification process. The metrics identify the discrepancies by facility category, which focuses attention on where problems are most frequently occurring. The findings suggest that a large percentage of these discrepancies are more prevalent in smaller companies. These observations reflect systemic problems within industry that must be addressed both by the NISPPAC and the government in order to minimize the number of rejections and to reduce the number of denials to an absolute minimum.

Tim McQuiggan, Industry, inquired, in view of the fact that a 34 percent error rate is unacceptable, if there might be a way that companies at headquarters level could be apprised of their own data, so that if there are systemic issues within their organizations, they could begin to address them. Mr. Riley responded that such assistance could certainly be provided, perhaps even at the Commercial and Government Entity (CAGE) code level. He suggested that the Working Group would discuss this issue and develop the particulars of precisely what information should be provided. Stan Sims, DSS, pledged that the concept would certainly receive serious consideration and that DSS would report back to the NISPPAC with the feasibility and scope of analysis by which the information might be provided. Mr. Riley added that the DAA would require that point of contact details be sent to the ODAA mailbox from all those corporate entities wanting this information.

Mr. Riley explained the differences between a denial and a rejection in the IATO process, defining a denial as acceptance of an SSP into the process, reviewing it, and then denying issuance of accreditation, often due to such conditions as incorrect documentation, while a rejection indicates that an SSP was so weak that it couldn't even be entered into the process, perhaps for such a condition as failure to attach the plan. Thus, DAA's primary goals are to reduce the number of denials and eliminate rejections. Further, industry is working efficiently to turn around the denials quickly, as this is often accomplished in two or three days.

Next, Mr. Riley presented data concerning the on-site system validation which reflected that approximately two percent of the systems reviewed had significant problems that prevented immediate issuance of an ATO. He described DAA's efforts in moving systems from IATO to ATO status noting that the number of days to achieve ATO status has been significantly reduced.

There followed a discussion of tracking initial issuance and/or second issuance of an IATO. Although these numbers are on a decidedly downward trend, DAA remains interested in identifying and reducing them, especially the second IATO, because system accreditation cannot occur while it exists. Tony Ingenito, National Classification Management Society (NCMS), inquired as to whether this process had been automated. Mr. Riley explained that the process elements for doing so were still in development, but expected to be completed by the end of FY 2012. The plan is based on an online system wherein the facility Information System Security Manager can submit the SSP without using e-mail. Once this action is completed, the plan's steps can be tracked, so that everyone involved in the process knows the exact condition of the plan's development at each stage.

The Chair then challenged the membership to take advantage of the work done by the various working groups, as their efforts enable both government and industry representatives to refine

discussion on each of the topics and to raise new concerns. He placed special emphasis on the NISPPAC's need to work harmoniously with Congress, the Office of Management and Budget (OMB), and the intelligence community as each addresses continuous streamlining of the personal security clearance process. He then introduced the Personnel Security Clearance Working Group and asked that its representatives update the timeliness metrics for industry investigations.

B) Personnel Security Clearance Working Group (PSCWG) Report

Representing the PSCWG were Lisa Loss, Office of Personnel Management (OPM), and Helmut Hawkins, DSS. Ms. Loss's metrics presentation showed continued reductions at all levels in both investigation and adjudication times for FY 2011 (Attachment #2). The Chair articulated that because the system does not always account for 100 percent of completed adjudication data, there is a gap between investigations completed and adjudications reported. Therefore the metrics can only reflect statistical accuracy to the degree that the information is reported to the system. The Chair requested that the Working Group evaluate how to close this gap so that we can realize full confidence in the comprehensive nature of the data.

Mr. Hawkins then reported metrics on pending initial investigations and renewals (periodic reinvestigations), both of which achieved completion time improvements (Attachment #3). He followed with a depiction of the Defense Industrial Security Clearance Office's (DISCO) workload for the FY, and noted that these updated metrics more accurately reflect suspended cases that DISCO has that pertain to supplemental investigations, special investigations, pending subject interviews, and reopening of other categories. Thus, the adjudication cannot be completed until the additional required information is provided.

Next, Mr. Hawkins briefed on industry cases pending at OPM, showing an FY reduction of roughly three percent, followed by an illustration of the rejection rates at both DISCO and OPM. DISCO's rejection rate was approximately ten percent of all investigations submitted; OPM's rejection rate was approximately five percent. He noted that one of the chief factors causing an OPM rejection was the non-receipt of fingerprint cards within the 30-day allotment which was decreased to 14 days, effective October, 2011. However he noted that a 14-day cutoff has long been the standard for all government agencies except for DoD, to include the NISP. Thus the 14-day allotment is now being applied for everyone except for overseas investigations. Several meeting participants were unaware of this change and expressed concern that since the 30-day cutoff already results in numerous rejections, there is likely to be a further increase. Ms. Loss explained that knowledge of the change was provided through the Background Investigations Stakeholder Group (BISG), was posted on their website, and tracks back to the Performance Measurement and Management Subcommittee that had sought to establish a standard of 14 days for the end-to-end process since it established the metrics. The Chair suggested that the Working Group, along with representatives from OPM, the Undersecretary of Defense for Intelligence (OUSD(I)), and DSS, consult on this matter to determine the ultimate impact, and perhaps pursue the development of an improved migration plan to meet the standard.

Mr. Sims suggested that since DoD has a 2013 timeline to establish the transfer to electronic fingerprints, and more than 70 percent of the rejections are due to fingerprints not matching the investigative file, it would seem that we could adjust a change in that policy to coincide with the requirement for the electronic fingerprint process. The Chair suggested that we first understand the impact of such a change prior to proceeding to the next steps, and that we remain within the concerns of the NISPPAC, which is to understand and report that impact to the decision-makers. Further, he noted that as some of us have been the interlocutors for big customer and big service providers negotiations, we must ensure that we be attentive, respectful, and informative to that process, because if there is going to be a significant impact and if there is another path to better performance, we should surface that to those with this high level of interest.

Mr. Hawkins next discussed DISCO case rejections by facility category, and noted that 81.4 percent originate from the smaller facilities. He advised that 51 percent of all DISCO rejections result from either missing employment information or inaccurate information on finances. He added that every DISCO rejection results in an additional 25 to 30 days, and that every OPM rejection results in an additional 60 days for case completion.

Finally, Mr. Hawkins' described the primary reasons for OPM rejections, namely missing fingerprint cards and certification/release issues. He noted that 91 percent of all OPM rejections come from one or both of these two categories. In response to the Chair's plea for an explanation of the nature of certification/release issues, Laura Hickman, DISCO, described the primary problem as missing certifications and/or unreadable signatures on release data. Finally, the Chair suggested that the Working Group include other investigative and adjudicative information, such as the Defense Office of Hearings and Appeals (DOHA) statistics.

C) Performance Accountability Council (PAC) Report

The Chair called for a report from the Performance Accountability Council's (PAC) working group on Phased Periodic Reinvestigations (PPR) to address the processes in place to affect their use and impact on clearances submitted under the NISP. He introduced Christy Wilder, Office of the Director of National Security (ODNI), and re-introduced Ms. Loss.

Ms. Loss informed the Committee that a PPR working group has been established to make recommendations to the SEA for government-wide policy regarding at what point a PPR should convert to a full Single-Scope Background Investigation (SSBI)-PR. In 2005, OPM met with the BISG, and established a set of "triggers" (essentially thresholds) that indicate the presence of security issues necessitating the expansion of the investigation to a full SSBI-PR. However, enough concerns about the validity of some triggers has since arisen that there have been two revisions. Further, when OPM began working with the SEA, a new SF 86 that would meet the reform deliverables already committed to Congress was needed as well as standardization of PPR triggers for the entire investigative community.

Ms. Wilder then described how the ODNI's SEA Advisory Committee (SEAAC), composed of virtually all government agencies who maintain a personnel security program, OPM, the Defense Personnel Security Research Center (PERSEREC), and DOHA, formed a Working Group to re-

evaluate and recommend triggers for PPR conversions (Attachment #4). As a result of the Working Group's efforts, the SEA intends to issue a government-wide policy, perhaps as early as February 2012, which, pending implementation of the revised Federal Investigative Standard (FIS), will be used by all Investigative Service Providers (ISP). The updated product is ready to go out for a 30-day comment period, and all agencies who participate in the SEAAC and the BISG will be asked to provide suggestions and/or recommendations. Ms. Wilder reminded the Committee that the implementation date for the revised FIS is December 2013.

IV. New Business

A) Executive Order (E.O.) 13587

The Chair presented a brief recap of the causes that provoked action, followed by a description of the current executive branch posture, with regard to insider threat activity (Attachment #5). He began with a summary of the Fall 2010 events that led to realization of the need for a unified response to the problems inherent in the unauthorized disclosure of classified information, proceeded to the formation by the National Security Staff (NSS) of an interagency committee to review the policies and practices for the handling of classified information, and concluded with an overview of E.O. 13587. He characterized this order as the beginning of a formal national response to the heightened activity caused by the WikiLeaks disclosures, which very carefully provides a governance structure for future policy and standardization to follow.

He next explained how NSS and OMB launched a number of activities, among which was a policy process to create the "to-do" lists for government. He described how the E.O. provides a new governance structure for improved security of our networks, while continuing emphasis on the sharing of classified information. He stressed that these are companion goals, and that they each received significant emphasis throughout the process. He then defined the guiding principles governing proposed reforms: reinforcement of the importance of responsible information sharing, ensuring that policies, processes, technical security solutions, oversight, and organizational cultures match information sharing and safeguarding requirements, emphasizing consistent guidance and implementation across the entire federal government, recognizing the importance of shared risk and shared responsibility, and continuing to respect the privacy, civil rights, and civil liberties of the American people. This was all accomplished with the establishment of some decision-making bodies and some guidance-providing bodies.

He then described the uppermost of these bodies, the Senior Information Sharing and Safeguarding Steering Committee. This committee has overall responsibility for fully coordinating interagency efforts and ensuring that departments and agencies are held accountable for the implementation of information sharing and safeguarding policy and standards. (The Chair serves on this committee.) In addition, staff support for this committee comes from the newly created Classified Information Sharing and Safeguarding Office (CISSO), which is administered within the ODNI's program manager for Information Sharing Environment. CISSO is, a small staff function created to organize the work of the steering committee and to ensure proper activity coordination, namely DoD and NSA who jointly are the Executive Agent for Safeguarding Classified Information on Computer Networks.

The new E.O. has also created an Insider Threat Task Force (ITTF), co-chaired by the Attorney General and the Director of National Intelligence (DNI). Its mission is to bring together the practitioners to create national policy affecting improvements in identification from within organizations and systems users who have access to classified information, and a better characterization of the threat that they may represent to that information and to those systems. In practice, the task force is co-chaired by the National Counterintelligence Executive (NCIX) and the Federal Bureau of Investigation (FBI), and is supported with detailees and assignees from across its membership. Further, the new E.O. tasks the ITTF to establish national policy on insider threat. The Chair correlated this activity with the objectives of the NISPPAC, in that it represents the interweaving of existing requirements for personnel security and information systems security, and will place increased emphasis on consistency, network-monitoring tools, and how these might trigger indicators that can be used to better protect classified information.

The E.O. emphasizes that agencies have the primary responsibility for sharing and safeguarding classified information. It leverages but does not change existing policy structure for classified information. Similar to E.O. 13526, it requires the designation of a senior agency official who will be responsible for the implementation of the national policy on insider threat and the safeguarding of classified information on computer networks. All of this activity is coordinated and overseen by the steering committee and reports through the CISSO, placing renewed emphasis on existing requirements for agencies to self-inspect.

The Chair noted that even though there is not yet an impact on policy or specific requirements governing industry participants in the NISP, there will be specific guidance forthcoming. As policies begin to emerge, they will be promulgated through the NISPOM. Since these policies involve elements of both personnel security clearance processes and the safeguarding of network processes that the NISPPAC already participates in, there will be actions for the NISPPAC as this process matures. For example, the reporting of personal foreign travel and personal foreign contacts today may evolve to performing those tasks perhaps in a different way or through a new process. What is less clear is the way that this policy will connect to classified enclaves operated on contractor-owned versus government-owned networks. Currently, the emphasis in the steering committee is on how to characterize and improve these capabilities on government-owned networks. To the extent that industry has users on those networks, those users will fall under the same umbrella as anybody else. Certainly there will be increased capabilities, but to the degree that it may require additional capabilities to be borne on contractor-owned networks that operate within these classified security domains, that's the space to watch and one of the primary reasons that we're opening a dialogue on this topic today. So, perhaps the initial critical question is at what point the voice of industry is needed in this policy development process. Finally the Chair asked to be kept informed of any questions, in particular on anything Committee members may have already heard about this, in terms of it levying requirements or other work. The Chair then asked Steve Lewis, OUSD(I) to provide the DoD update.

B) DoD Update

Mr. Lewis gave the Executive Agent's (EA) report on the NISP, and addressed the status of the NISPOM re-write. He informed the Committee that within two days of E.O. 13587 being issued,

DoD was receiving questions as to its applicability to industry. He assured the Committee that as the implementing directives are written for this E.O., the Committee will closely evaluate them, because E.O. 12829, as amended, "National Industrial Security Program" requires similar security controls for industry to those applicable to government. Indeed, a keystone of E.O. 13587 is the Committee on National Security Systems (CNSS) process for identifying security controls in the information systems environment. The proposed revisions to Chapter 8 of the NISPOM make a similar reference to CNSS. Therefore, it's understood that as new federal policy is developed, that will translate into new NISPOM requirements.

Regarding the NISPOM re-write, Mr. Lewis stated that later that day OUSD(I) would forward to the NISPOM working group members an adjudicated comments matrix. This distribution will not include Chapter 10 because of the extreme volume of comments on that chapter, nor Appendix D, which is the NISPOM supplement, because there are still a few issues on which to complete our work. In addition, we'll be asking for "fall-on-your-sword-" type comments by December 2nd. These fall into the category of, "we agreed to do something in the working group process and we didn't do it." Also, violations of law and/or of government-wide regulation are the types of things that would be reclama comments. He provided that the Working Group did not always agree as they moved through this process, one that required over a year to complete, but we attained a much-improved product. For example, in Chapter 5, Section 3, "Storage and Storage Equipment," we have provided an additional option for industry for the open storage of classified information, which is similar to options available to government agencies. He further explained that DSS has prepared an Industrial Security Letter (ISL) which allows for immediate implementation of those provisions for the approval of open storage areas, and that after coordinating the ISL with the other Cognizant Security Agencies (CSA) it will be distributed to the NISPPAC members. In addition, Chapter 8, "Information System Security," has been significantly improved. It has been streamlined, rendered much more flexible, and equipped with a measure of control and opportunity for industry to input into the process.

Mr. Lewis then moved to a brief description of several DoD initiatives as a result of mandated requirements. First, he addressed the issue of the Congressionally-directed action on security containers, and he reminded the Committee that DoD must submit a report to Congress in January, 2012 on the status of industry's discontinuing the use of non-GSA approved containers for the storage of classified information. He described the progress to date using 2009 baseline numbers in which industry had almost 13,000 non-GSA approved containers storing classified, contrasting that with the latest available numbers as reduced to 4,700, or roughly a 60-plus percent reduction. He added that DoD believes that this number has since been further reduced, and that there is every indication that contractors will achieve the October 1, 2012 deadline for eliminating all remaining non–GSA approved containers.

Next, Mr. Lewis presented brief reports on several ongoing DoD/NISP activities. First, he reminded the Committee that DoD was continuing to develop a Special Access Program (SAP) security manual. He emphasized that the goal of this initiative is that once issued within DoD we will propose that it become the national level standard for contractors, that is, a "NISPSAP" manual. Then, he reported on DoD„s progress towards updating its activities' security policies, briefly describing two volumes of the DoD NISP manual in various stages of coordination. One,

which will replace the 1985 industrial security regulation, contains the security requirements for government activities and is close to being formally coordinated. The other is the Foreign Ownership Control and Influence (FOCI) procedures for government activities, which will implement the existing directive-type memorandum, but on a more permanent basis. Finally, he described some new requirements levied on DoD activities concerning the tracking of National Interest Determinations (NID). He explained that this guidance requires that each DoD activity designate an individual authorized to provide coordinated positions on FOCI and NID matters to respond to a DSS NID notification requirement within 30 days. That is, activities must provide a NID, submit a proposed NID, pending concurrence from another activity, or make the determination to deny the NID. Thus, companies cleared under special security agreements will at least receive a definitive answer. Also, the memorandum requires that DSS track the NID process monthly. To that end, DoD received the first report from DSS yesterday.

Brad Groters, public visitor, inquired as to the projected timeline for finalization of the revised NISPOM, and when it will be posted in the *Federal Register*. Mr. Lewis responded that December 2nd is the suspense date for final comments from the NISPPAC members, and we will then follow with final changes. Therefore, within 60 days it will go to both a DoD coordination, and concurrently, coordination with the other CSAs.

C) DSS Update

The Chair recognized Mr. Sims, who introduced Jim Kren as the new Deputy Director, DSS. Mr. Sims then reported that both DoD and industry stakeholders had already consulted on most of the DSS implementation that Mr. Lewis described and that all had had clear, frank and productive discussions, and are committed to a collaborative approach for addressing these issues. He reiterated that in terms of the NID process, a lot of guidance has been issued to DoD participants, and that when included in the NISPOM, it will apply to all other government agencies that DoD provides industrial security services. He explained that DSS guidance complies with both the 30-day and 60-day NID national policy requirements, and that both DoD and other agencies who currently have outdated NIDs requests must address them within a specified time period to comply with those same regulations. Then, we'll place an internal control on monitoring all with outstanding NID requests, and subsequently provide a report to senior leadership of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD(AT&L)) for the industry piece, and the OUSD(I) for the security piece, thus permitting precise tracking of NID compliance. Also, he stated that DSS will coordinate with both the National Security Agency (NSA) and the NCIX to ensure that all DoD and other agencies have a workable procedure for processing NIDs. Therefore, he encouraged any government agency that is unclear about this procedure and/or their responsibilities to contact DSS through Drew Winneberger, or its website.

Mr. Sims then spoke of a restructuring of the DSS/Industry partnership that he has overseen in the 11 months since he became the Director. He is encouraged by the enthusiastic support and positive feedback from industry partners, and expects that this year's NISP will yield even greater results.

Next, Mr. Sims reported that DSS has recently completed the annual trends document targeting US technologies that the NISP requires be provided to industry. He added that there are both unclassified and classified versions. The classified version can be accessed through the Secret Internet Protocol Router Network (SIPRNet), or by contacting DSS. He added that senior leadership might benefit greatly from the contents of the report, and that, if requested, DSS would provide a briefing to NISPPAC member entities. He stressed that the document reflects the very real need for all stakeholders to be more vigilant in this arena, as our industrial base is being attacked every day, with perhaps even greater force, than on our battlefields.

Finally, Mr. Sims repeated his heartfelt thanks for the support of all in behalf of the Wounded Warrior program. He acknowledged that industry leadership has dedicated much time and energy accessing the website in order to locate the wounded warriors, and then proactively finding employment for these heroes. He recognized Tracy Kindle, DSS's frontrunner in this initiative, and recommended that interested industry and/or government personnel continue to contact him for assistance.

D) Combined Industry Presentation

The Chair introduced Scott Conway who provided the industry update (Attachment #6). He recognized the Memorandum of Understanding (MOU) membership and noted that Randy Foster was retiring and being replaced by Mark Rush, who would represent the Contractor Special Security Working Group. He then mentioned that industry would like to see the PSCWG continue and perhaps even be enhanced. He explained that industry was given a briefing on Public Key Infrastructure- (PKI) enabling JPAS. They are concerned that roughly 6,500 JPAS users are not PKI-enabled, and understand that the Working Group will address that issue. He acknowledged the PPR update today, but wondered where the clearance reform process is going. He expressed thanks that the DISCO relocation has been completed and also expressed his appreciation for the report by the PSCWG. He found most useful the update on the NISPOM revision and especially its reported increased flexibility, but expressed concern that the new Chapter 8 does not become so onerous that industry can't operate. However, the working relationship between DoD/DSS and industry seems to be on such a solid footing that he feels they will accomplish the task with joint satisfaction. He expressed appreciation for the update on processing metrics. Further, he described industry's desire to see the appointment of a Special Access Program working group to examine finding less complex ways of accomplishing some common tasks, such as foreign travel, etc. He explained that there have been some initial discussions with the OUSD(I) on this idea and that they were supportive of the concept.

He also reported that industry has discussed information sharing and threats and remains concerned with how they can receive real-time information, either from a Counterterrorism or a Counterintelligence perspective. That is, are there, or are there not, threats to industry? And if so, can we learn about them more quickly and more authoritatively?

Mr. Conway noted that industry has not yet broached the subject of Controlled Unclassified Information (CUI), and is concerned with how it is going to impact them. He also wonders how the initiatives prescribed in E.O. 13587 will affect industry. In addition, he explained that

industry had discussed the proposed requirement from the National Defense Act for some type of company official to certify the security program, but that they are looking forward to understanding how this will be represented in the new NISPOM. Both Mr. Sims and Mr. Lewis clarified that this concept is only a proposal and if approved, would have a certification similar to that made by the government security committee for certain companies operating under a FOCI agreement. They emphasized that this proposal is still pending congressional advice and consent.

Finally, Mr. Conway explained that most of the companies are just beginning to collect information related to the cost impact of data spills; the ultimate goal being to discover their potential damage to national security both from the perspective insider threat and the advanced persistent threat whenever information is being exposed on unclassified networks. The Chair then delineated some topics that should be included in the next NISPPAC meeting: continued discussions on clearance reform, a CUI update, with specific emphasis on the current status of the Defense Federal Acquisition Regulation Supplement, and a briefing by the ITTF on their plan of action with regard to policy development.

There followed a question from Kimberly Baugher, Department of State as to whether personnel whose JPAS accounts had been purged from the system for failure to access have now been restored. Mr. Lewis responded that such was indeed the policy of the Defense Manpower Data Center (DMDC), and Mr. Sims added that anyone whose account has been disabled due to the security risks inherent in inactivity could request and receive reinstatement. Mr. Sims was not certain how long it takes for an individual to be reinstated, but he will inquire, and he would also recommend to DMDC that they add a suggestion on their website that all account holders login periodically in order to avoid being disabled.

V. General Open Forum/Discussion

The Chair offered the public attendees the opportunity to speak or ask questions. Mr. Ingenito proffered workshop time and space at NCMS's next annual meeting for any NISPPAC working group. In addition, he suggested that it might be an excellent opportunity for both working group and small business personnel to discuss topics and subjects of interest to each. The Chair applauded the idea and suggested that working groups who would be meeting between now and then discuss the possibilities. George Ladner, Central Intelligence Agency (CIA), announced that Charles Phalen, CIA Director of Security, has retired and been replaced by Mary Rose McCaffrey.

VI. Closing Remarks and Adjournment

There being no other questions or points of information, the Chair announced the next two NISPPAC meetings as having been set for March 21, 2012 and July 11, 2012 respectfully, with the working groups typically meeting roughly six to eight weeks prior to the next meeting. The meeting was adjourned at 12:14 pm.

Summary of Action Items

1. ISOO will ensure that necessary investigative and adjudicative information and statistics from the ODNI and the Defense Office of Hearings and Appeals (DOHA) are provided to the PSCWG so it has an holistic picture of the clearance processes impacting industry.

2. ISOO will ensure the PSCWG, along with representatives from OPM, the Undersecretary of Defense for Intelligence (OUSD(I)), and DSS, determine the ultimate impact, and develop an improved migration plan to meet the OPM mandated 14 day standard for fingerprint submittal. Additionally, the PSCWG will evaluate how to close the gap between the number of investigations completed and the number of adjudications reported so full confidence can be gained in the comprehensive nature of such data

3. The CUI office will provide an update on recent developments regarding CUI implementation.

4. DoD will update the status of the changes to the Defense Federal Acquisition Regulation Supplement (DFARS), as well as update the status of the NISPOM rewrite.

5. The ITTF will present a briefing on their action plan to implement their portion of E.O. 13587.

6. ISOO will host an ad hoc working group on Special Access Programs.

7. .DSS agreed to inquire regarding the DMDC's policy for reinstating JPAS accounts that have been disabled because of account inactivity, as well as efforts to encourage DMDC to post their policy account usage on their website, so account holders can avoid having accounts disabled.

8. **DSS will report back to the CAWG and the NISPPAC with the feasibility and scope of analysis on how the aggregation of system security plan error data information might be provided to corporate level entities, so that if there are systemic issues within their organizations, they could begin to address them.**

ATTACHMENTS

Attachment #1- DAA C&A Presentation

Attachment #2- OPM PCL Presentation

Attachment #3- DISCO PCL Presentation

Attachment #4- Phased PR Presentation

Attachment # 5- Executive Order 13587 Presentation

Attachment # 6- Combined Industry Presentation

Attachment #1- DAA C&A Presentation

Defense Security Service

Industrial Security Field Operations (ISFO)

Office of the Designated Approving Authority (ODAA)

Oct 2011

Defense Security Service

Overview:

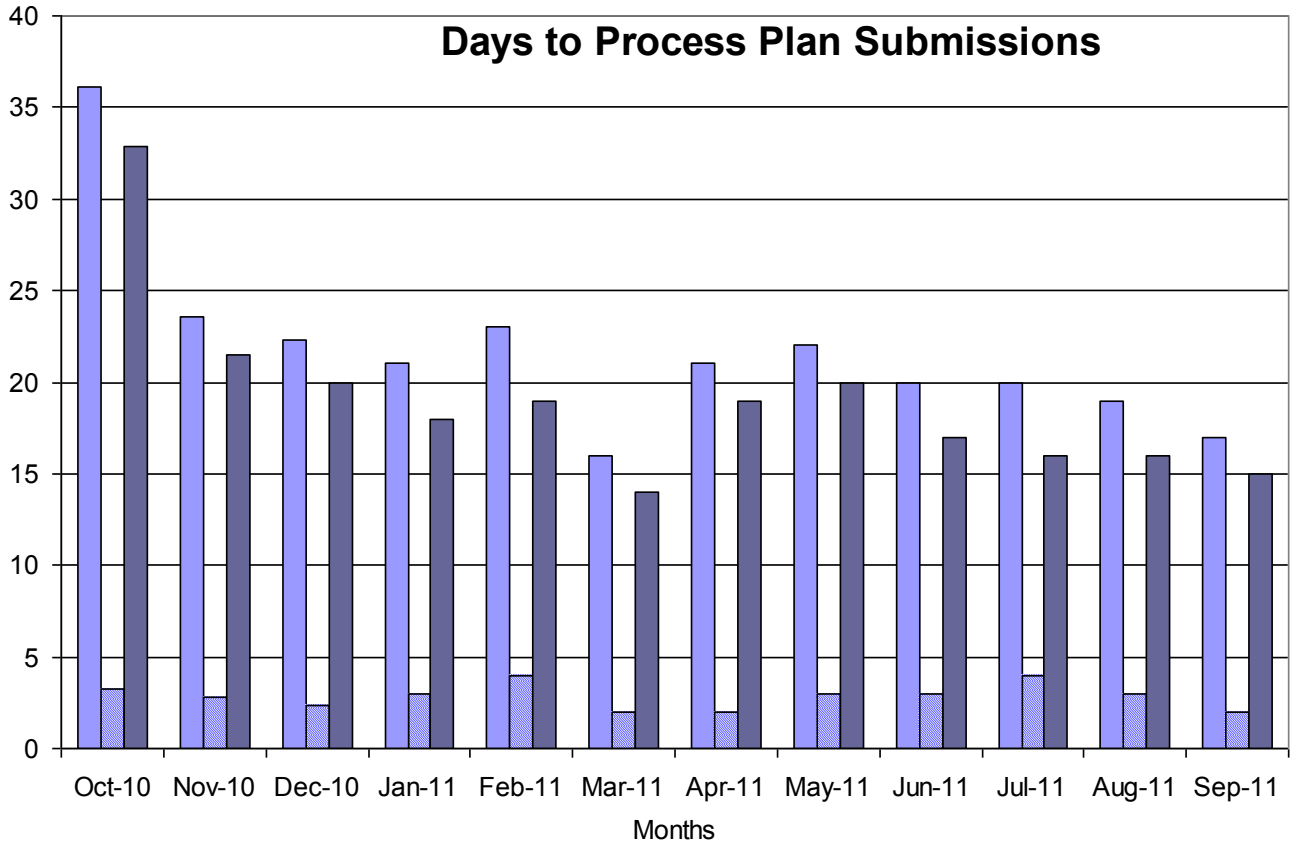
- Certification & Accreditation (C&A)
- ODAA Metrics
  - Timeliness and Consistency
  - Security Plan Review
  - Security Plan Review Errors
  - System Validation
  - Plan Submission Denials and Rejections
  - 2nd IATO Metrics

Defense Security Service

Certification & Accreditation

- DSS is the primary Government entity responsible for approving cleared contractor information systems to process classified data.
- Ensures information system security controls are in place to limit the risk of compromising national security information.
- Provides a system to efficiently and effectively manage a certification and accreditation process.
- **Ensures adherence to national industrial security standards.**

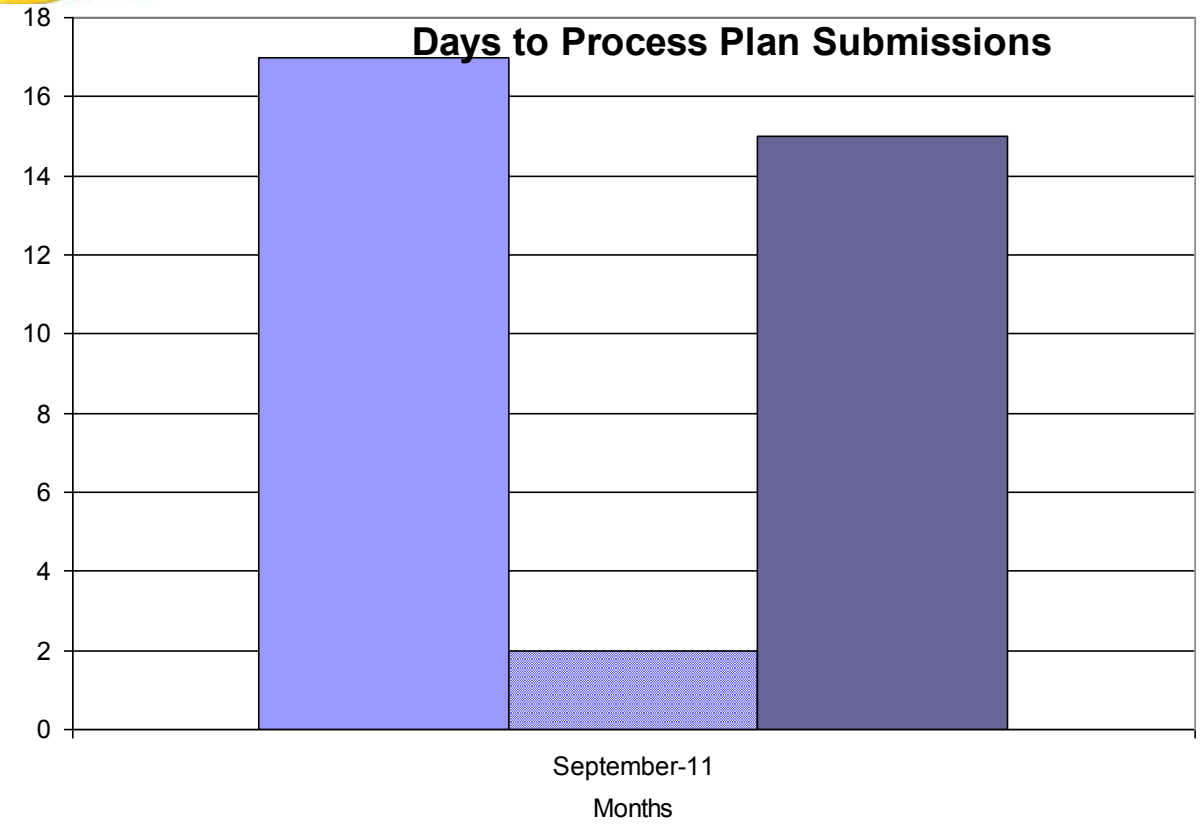
ODAA Improving Accreditation Timeliness and Consistency



(Oct 2010 – Sept 2011 Metrics)

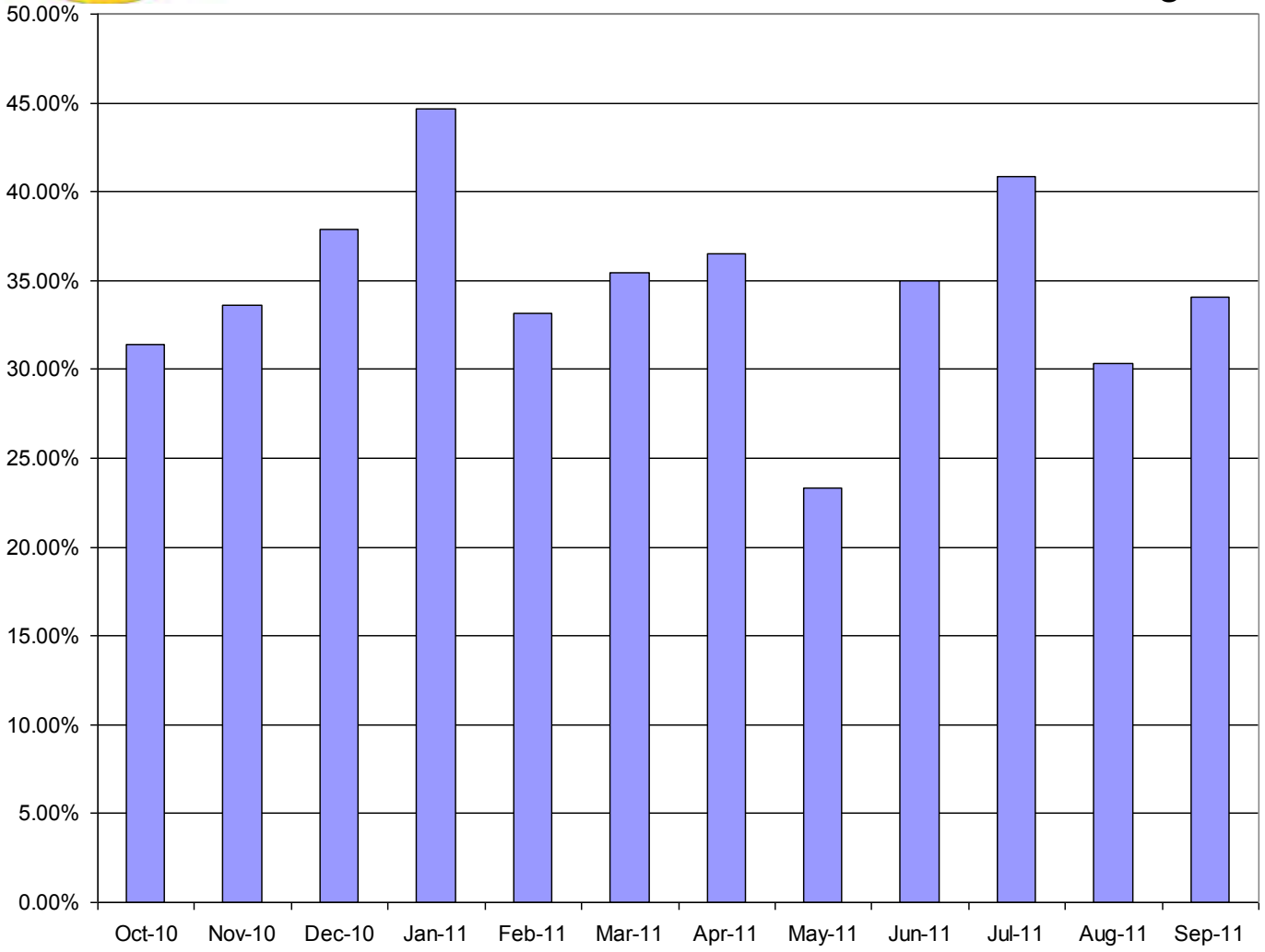
- The average number of days to issue an IATO for a system after plan submission was 22 Days
- The average number of days for a system under IATO to go to ATO status was 84

ODAA Improving Accreditation Timeliness and Consistency



- 327 IATOs granted
- The average number of days to issue an IATO after submission of a plan was 17 days

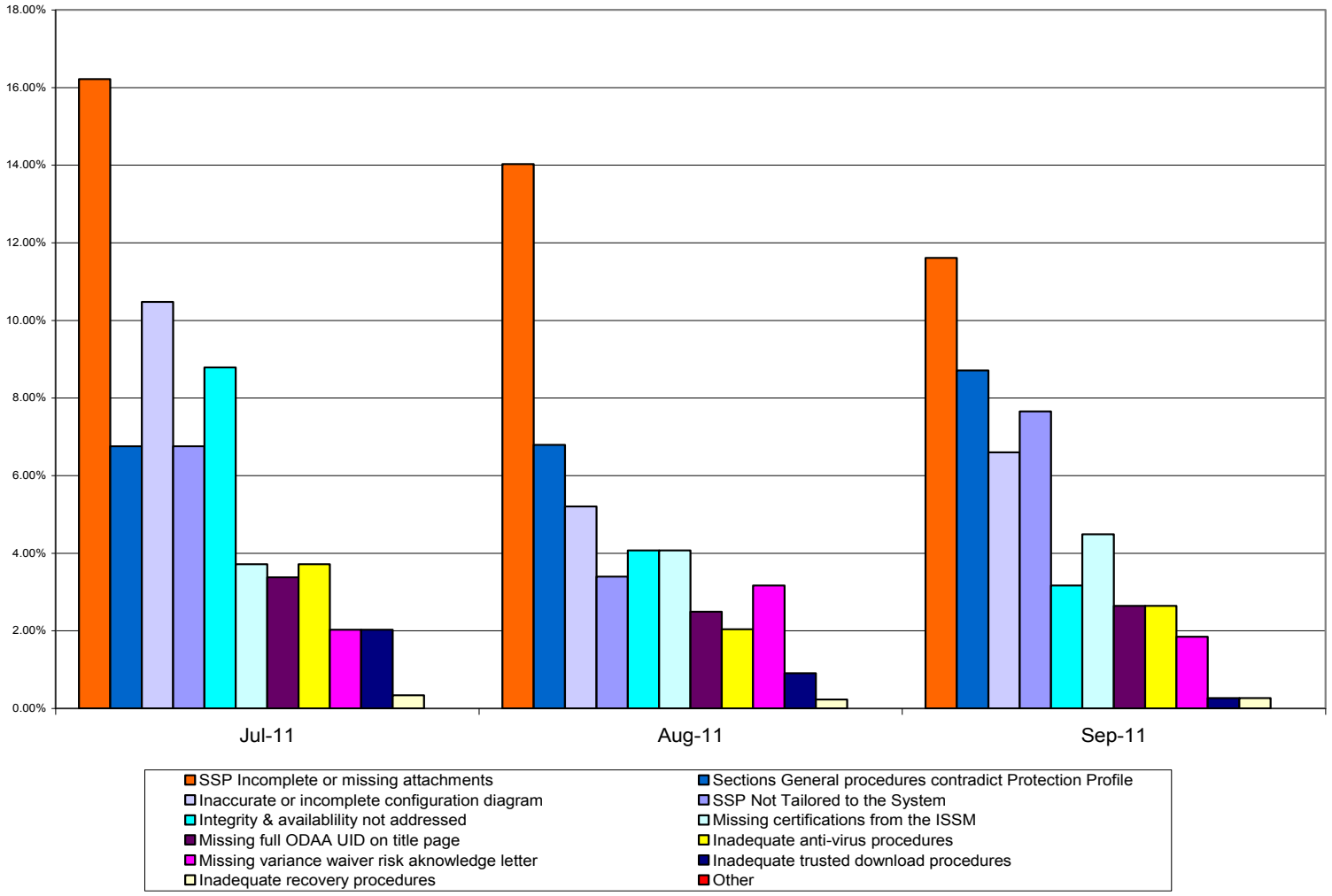
Security Plan Review Metrics



Oct 2010-Sept 2011

- Accepted/reviewed 5063 plans
- 34% of the plans submitted required corrections prior to the onsite validation for ATO
- 22%/1130 IATOs granted with corrections required
- 12%/611 IATOs denied due to plan corrections needed (processed after corrections made)

Security Plan Review Common Errors



Security Plan Review Common Errors by Facility Category

Month of September 2011

Number of Plans Submitted		39	87	47	70	136
	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
SSP Is incomplete or missing attachments	44	**7.69%**	8.05%	6.38%	**12.86%**	**16.18%**
Sections in General Procedures contradict Protection Profile	33	2.56%	**9.20%**	6.38%	**7.14%**	**11.76%**
SSP Not Tailored to the System	29	2.56%	**9.20%**	4.26%	**7.14%**	**9.56%**
Inaccurate or Incomplete Configuration diagram/system description	25	0.00%	**10.34%**	**2.13%**	1.43%	**10.29%**
Missing certifications from the ISSM	17	0.00%	**4.60%**	0.00%	**7.14%**	**5.88%**
Integrity & Availability not addressed completely	12	0.00%	**4.60%**	0.00%	**1.43%**	**5.15%**

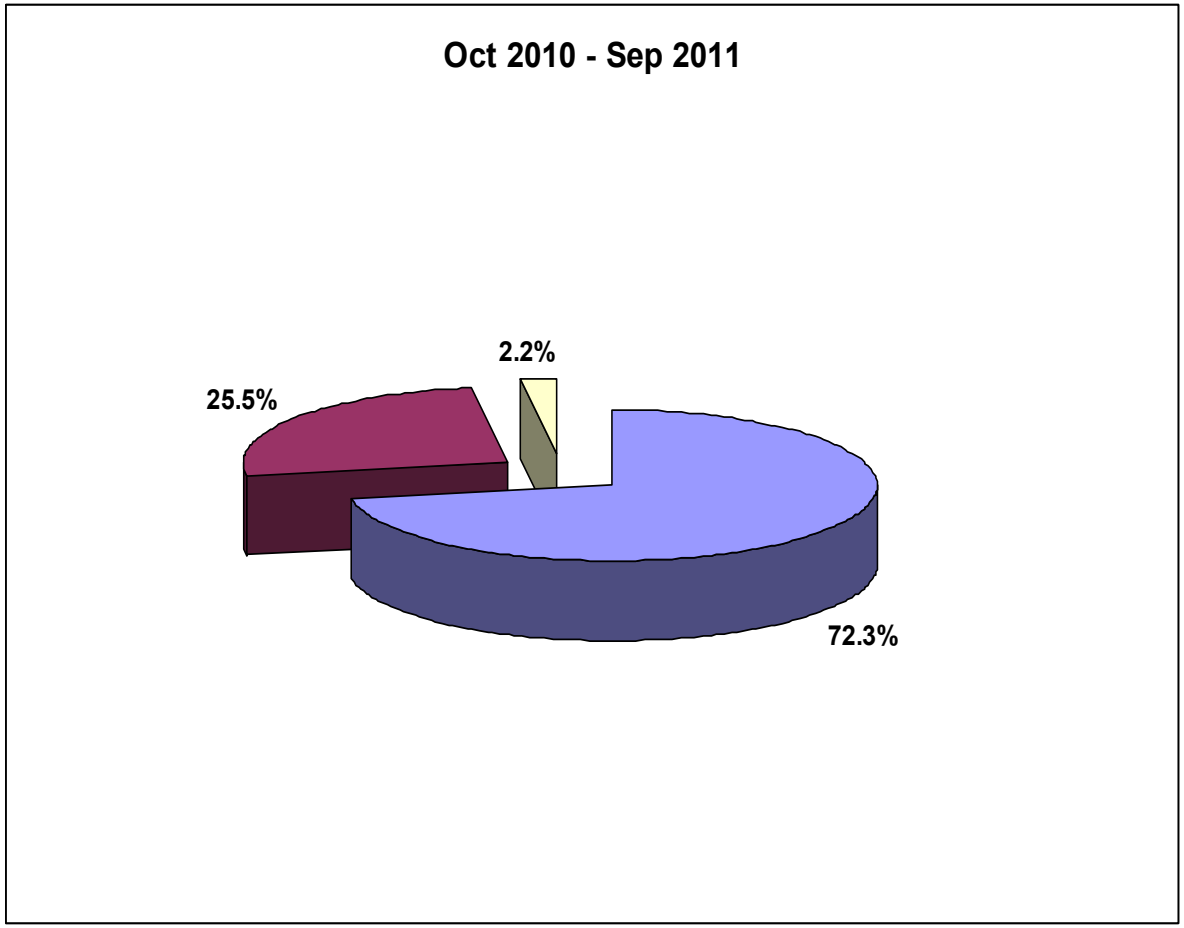
Security Plan Review Common Errors by Facility Category (cont'd)

Month of September 2011

	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Inadequate anti-virus procedures	10	0.00%	0.00%	**2.13%**	**4.29%**	**4.41%**
Missing full ODAA UID on Title Page	10	0.00%	0.00%	**12.77%**	**2.86%**	**1.47%**
Missing variance/waiver/risk acknowledgement letter	7	0.00%	**3.45%**	**4.26%**	**2.86%**	0.00%
Inadequate trusted download procedures	1	0.00%	0.00%	0.00%	0.00%	**0.74%**
Inadequate recovery procedures	1	0.00%	1.15%	0.00%	0.00%	0.00%
Other	0	0.00%	0.00%	0.00%	0.00%	0.00%
Total Errors %	**189**	**2.65%**	**23.28%**	**9.52%**	**17.46%**	**47.09%**
Total Errors	**189**	**5**	**44**	**18**	**33**	**89**

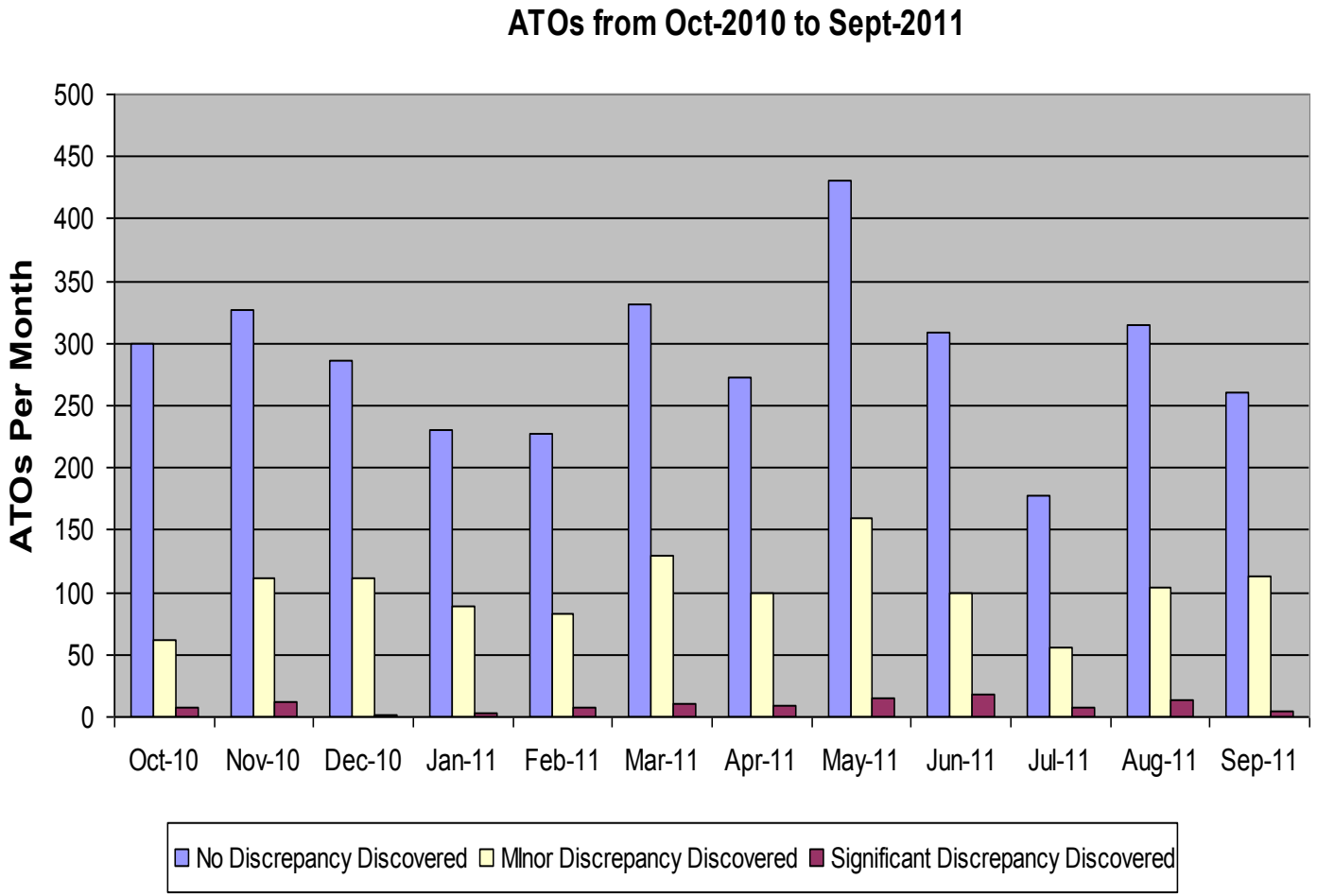
Onsite System Validation Metrics

27.7% of Systems Required Correction



- 3452 systems (72.3%) had no discrepancies identified during the onsite validation
- 1218 systems (25.5%) had minor discrepancies identified and corrected during the onsite validation
- 107 systems (2.2%) had significant discrepancies identified that could not be resolved (second validation visit required)

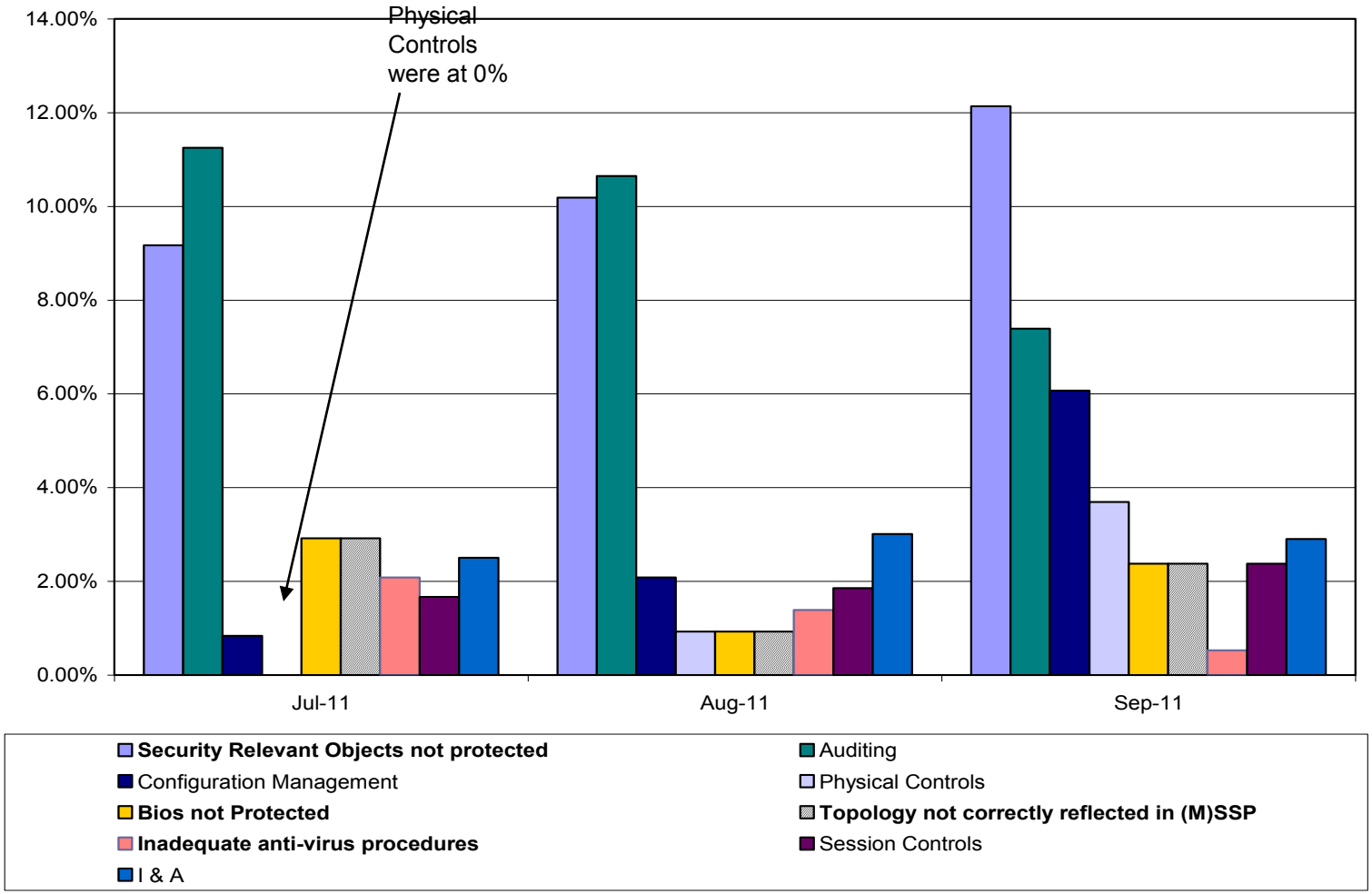
System Validation Metrics by Month



The average number of days for a system under IATO to go to ATO status was 84.

Common System Validation Discrepancies

Month of September 2011



System Validation Discrepancies by Facility Category

Month of September 2011

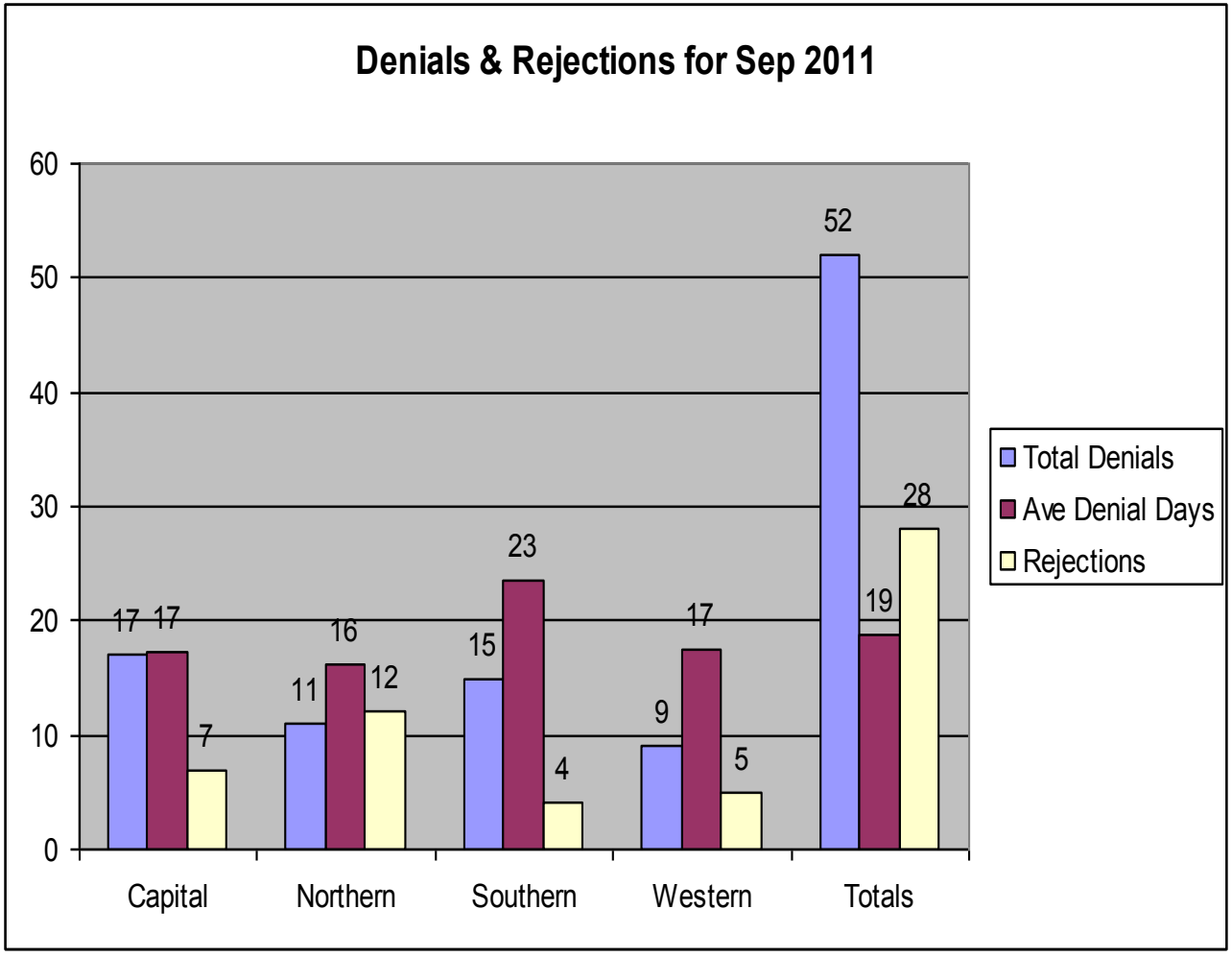
Systems Validated by Facility Category Sept 2011		32	62	27	75	178
	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Security Relevant Objects not protected	**46**	0.00%	6.45%	**10.71%**	**12.00%**	**16.57%**
Auditing	**28**	3.03%	3.23%	**3.57%**	**12.00%**	**8.29%**
Configuration Management	23	0.00%	0.00%	0.00%	**10.67%**	**8.29%**
Physical Controls	14	0.00%	0.00%	0.00%	**8.00%**	**4.42%**
I & A	11	0.00%	**3.23%**	0.00%	**8.00%**	**1.66%**
Bios not Protected	**9**	0.00%	0.00%	**3.57%**	**8.00%**	**1.10%**
Topology not correctly reflected in (M)SSP	**9**	0.00%	0.00%	**3.57%**	**8.00%**	**1.10%**
Session Controls	9	0.00%	1.61%	**3.57%**	**2.67%**	**2.76%**
SSP Does Not Reflect How the System is Configured	6	**3.03%**	0.00%	**3.57%**	**4.00%**	0.55%
RAL Not Provided	5	**12.12%**	**1.61%**	0.00%	0.00%	0.00%

System Validation Discrepancies by Facility Category (cont'd)

Month of September 2011

	Total	Facility Category AA %	Facility Category A %	Facility Category B %	Facility Category C %	Facility Category D %
Trusted Download Review	4	0.00%	0.00%	0.00%	**1.33%**	**1.66%**
Inadequate anti-virus procedures	2	0.00%	0.00%	0.00%	0.00%	**1.10%**
Root/Admin Account misconfigured	1	0.00%	0.00%	0.00%	0.00%	**0.55%**
Compilation	1	0.00%	0.00%	0.00%	0.00%	**0.55%**
POA&M not Implemented	0	0.00%	0.00%	0.00%	0.00%	0.00%
Other	**0**	0.00%	**0.00%**	**0.00%**	**0.00%**	**0.00%**
Different System Type	0	0.00%	0.00%	0.00%	0.00%	0.00%
All Users are Configured as Administrators	0	0.00%	0.00%	0.00%	0.00%	0.00%
NSP Not Provided/Referenced for a WAN Node	0	0.00%	0.00%	0.00%	0.00%	0.00%
PL Not Adequately Addressed	0	0.00%	0.00%	0.00%	0.00%	0.00%
Total Errors % Slide One and Two	**168**	**3.57%**	**5.95%**	**4.76%**	**33.33%**	**52.38%**
Total Errors # Slide One and Two	**168**	**6**	**10**	**8**	**56**	**88**

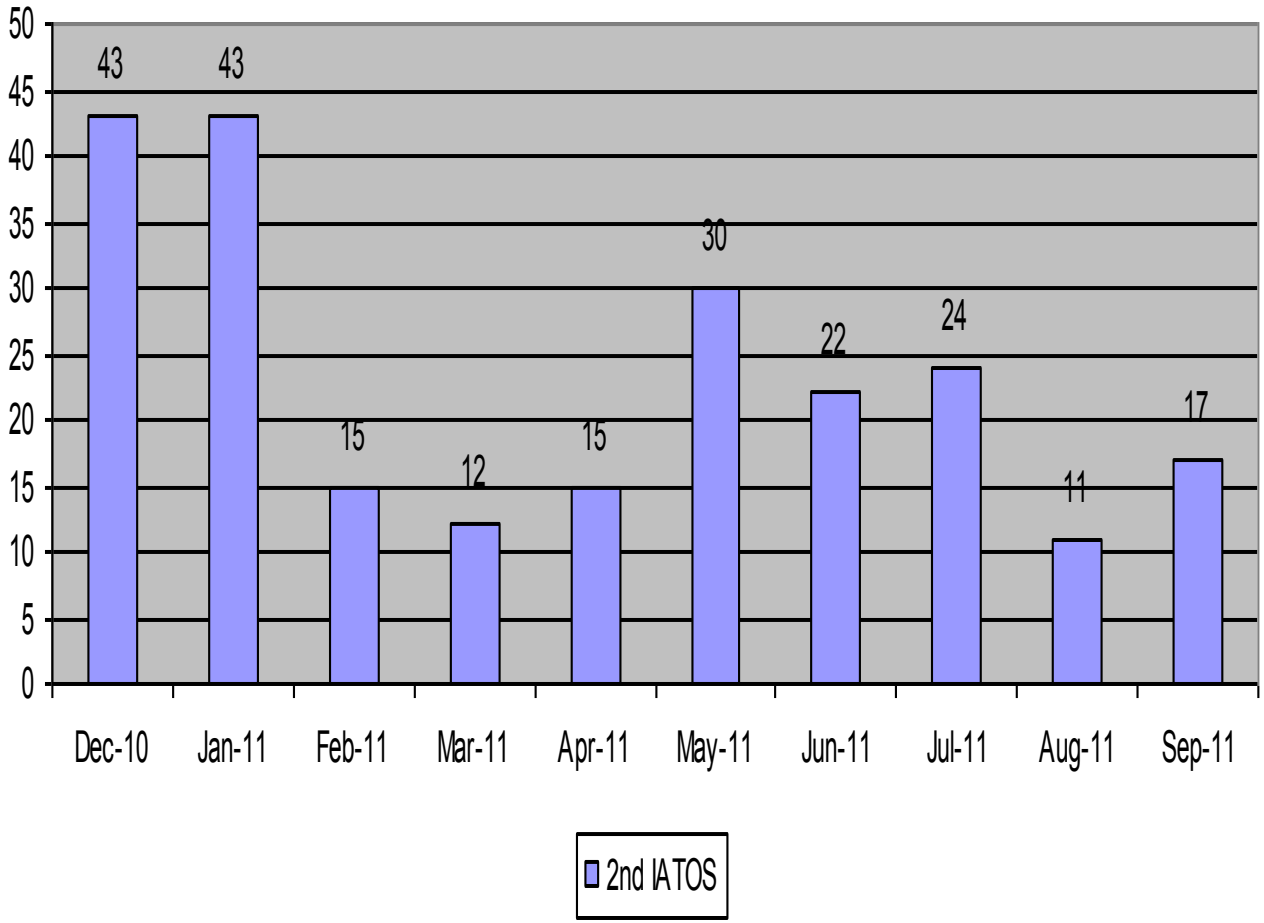
Plan Submission Denials & Rejections



- Denials - Plans were received and reviewed. An IATO could not be issued until corrections were made to the plans.

- Rejections - Plans not submitted in accordance with the ISFO Process Manual and not entered into the ODAA database. Plans are returned to the ISSM and must be resubmitted correctly for processing.

Second IATOs Issued



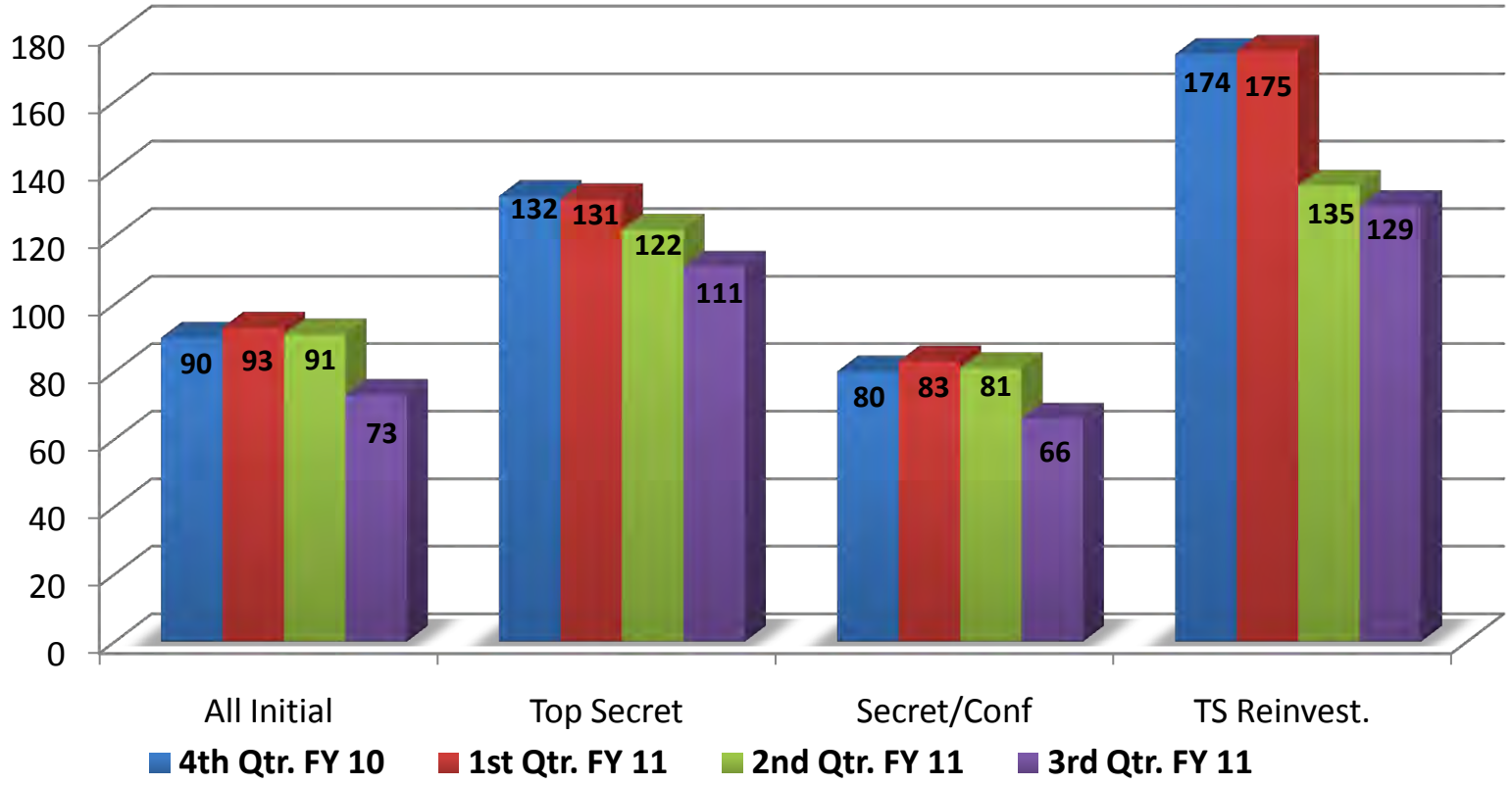
Most Common Reasons for Issuing Second IATOs

- Plan of Action and Milestone (POAM) items not addressed
- Corrections not made to systems or hardware
- HBSS Licensing, installation issues.
- Onsite rescheduled due to ISSP and/or ISSM availability

#2- OPM PCL Presentation

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

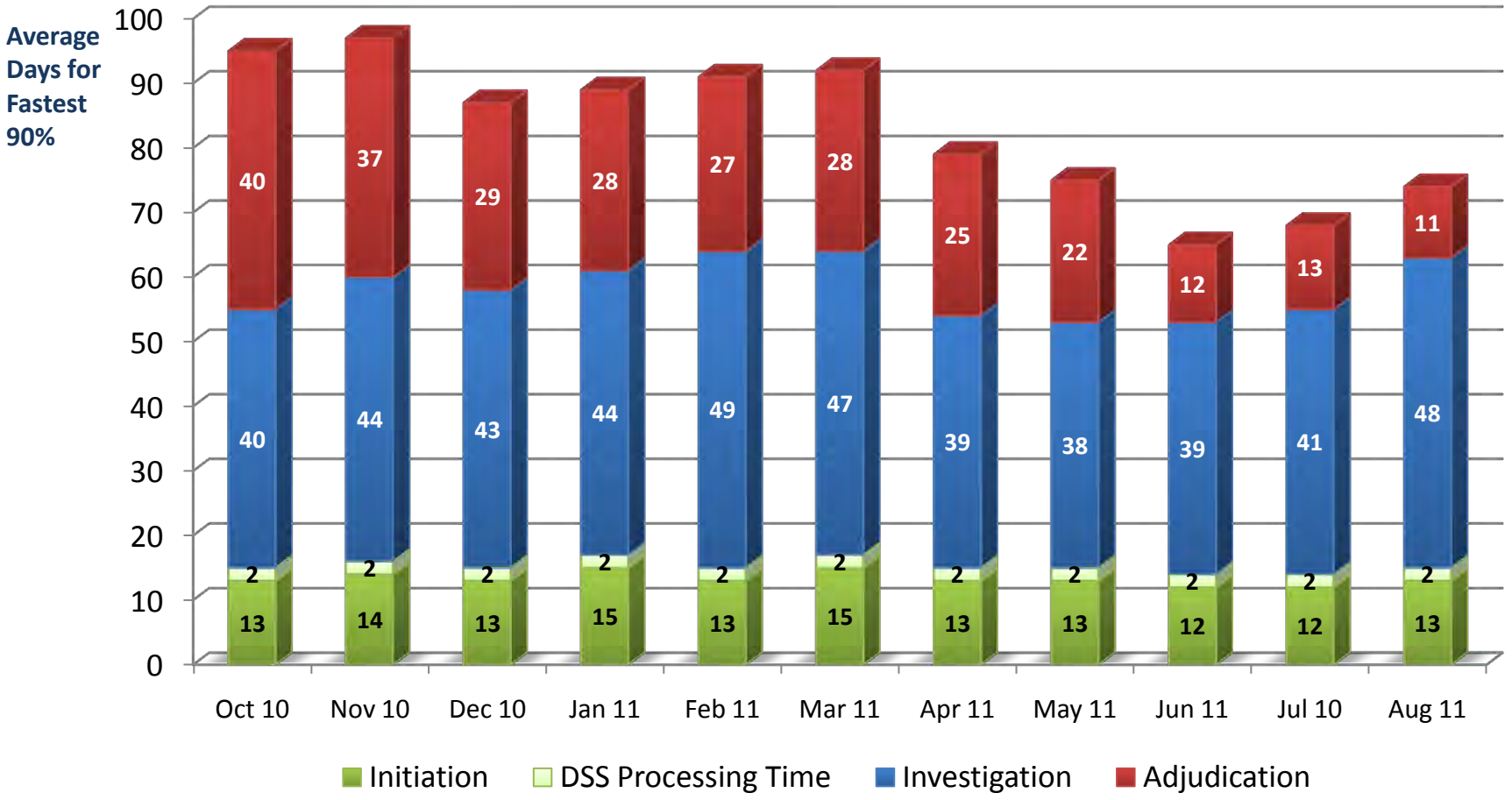
Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 4th Q FY10	25,446	5,247	20,199	4,051
Adjudication actions taken – 1st Q FY11	29,639	6,766	22,873	6,894
Adjudication actions taken – 2nd Q FY11	28,912	6,763	22,149	8,143
Adjudication actions taken – 3rd Q FY11	35,989	5,755	30,234	12,071

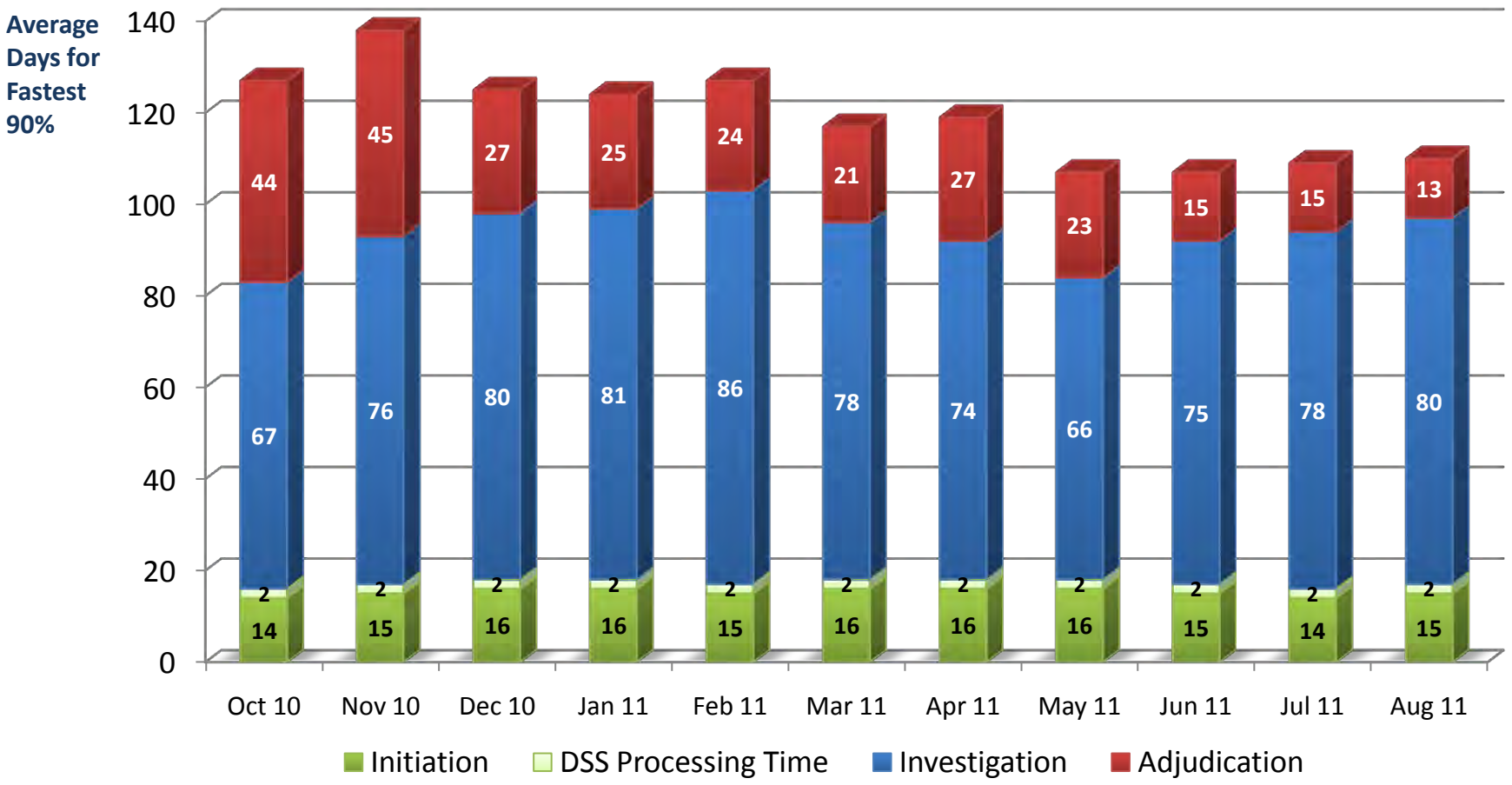
*The adjudication timelines include collateral adjudication by DISCO and SCI adjudication by other DoD adjudication facilities

Industry's Average Timeliness Trends for 90% Initial Top Secret and All Secret/Confidential Security Clearance Decisions



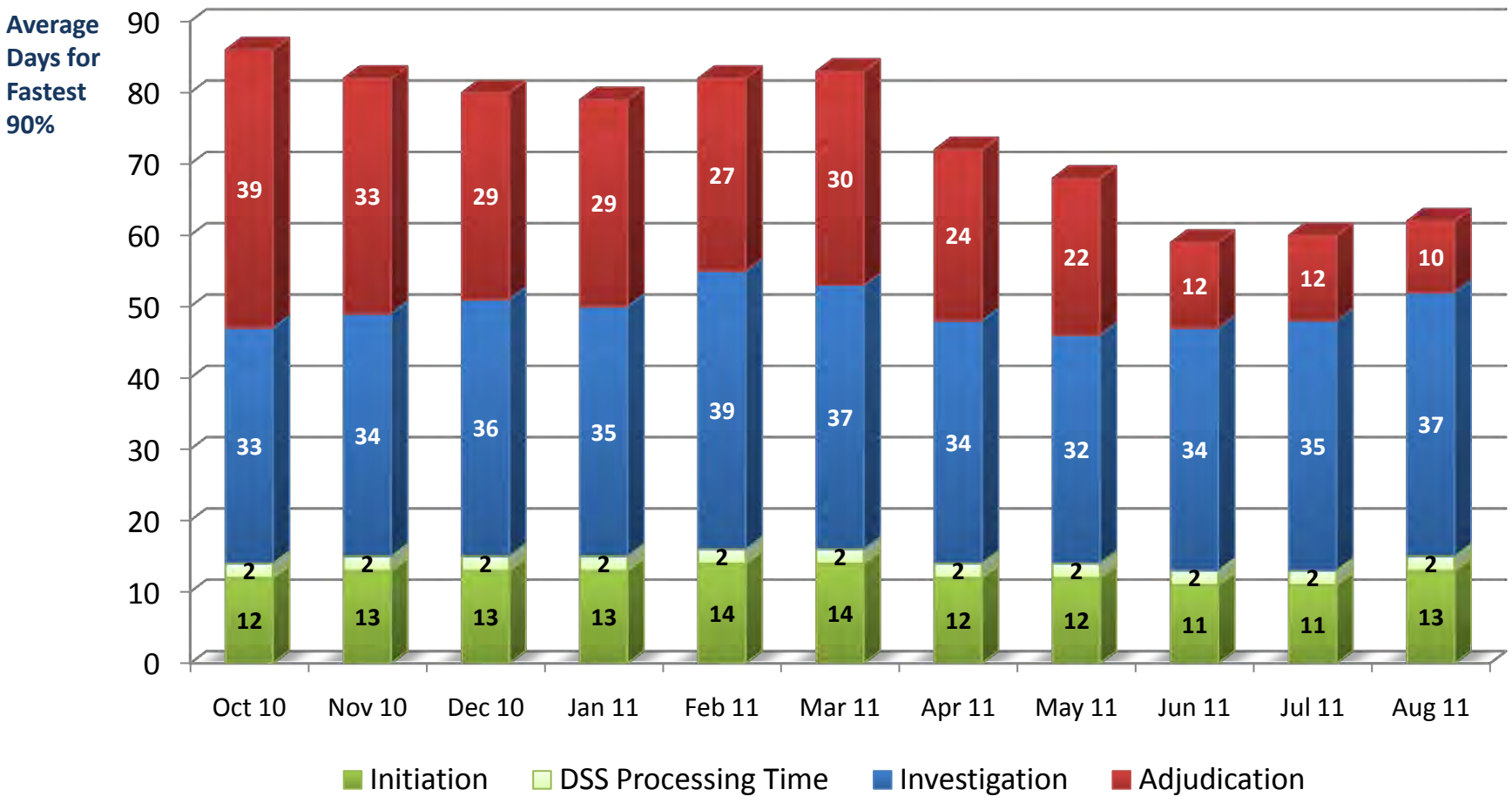
	Oct 10	Nov 10	Dec 10	Jan 11	Feb 11	Mar 11	Apr 11	May 11	Jun 11	Jul 11	Aug 11
100% of Reported Adjudications	9,994	9,729	9,662	9,087	8,100	11,678	11,737	11,907	12,358	8,917	8,952
Average Days for fastest 90%	95 days	97 days	87 days	89 days	91 days	92 days	79 days	75 days	65 days	68 days	74 days

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



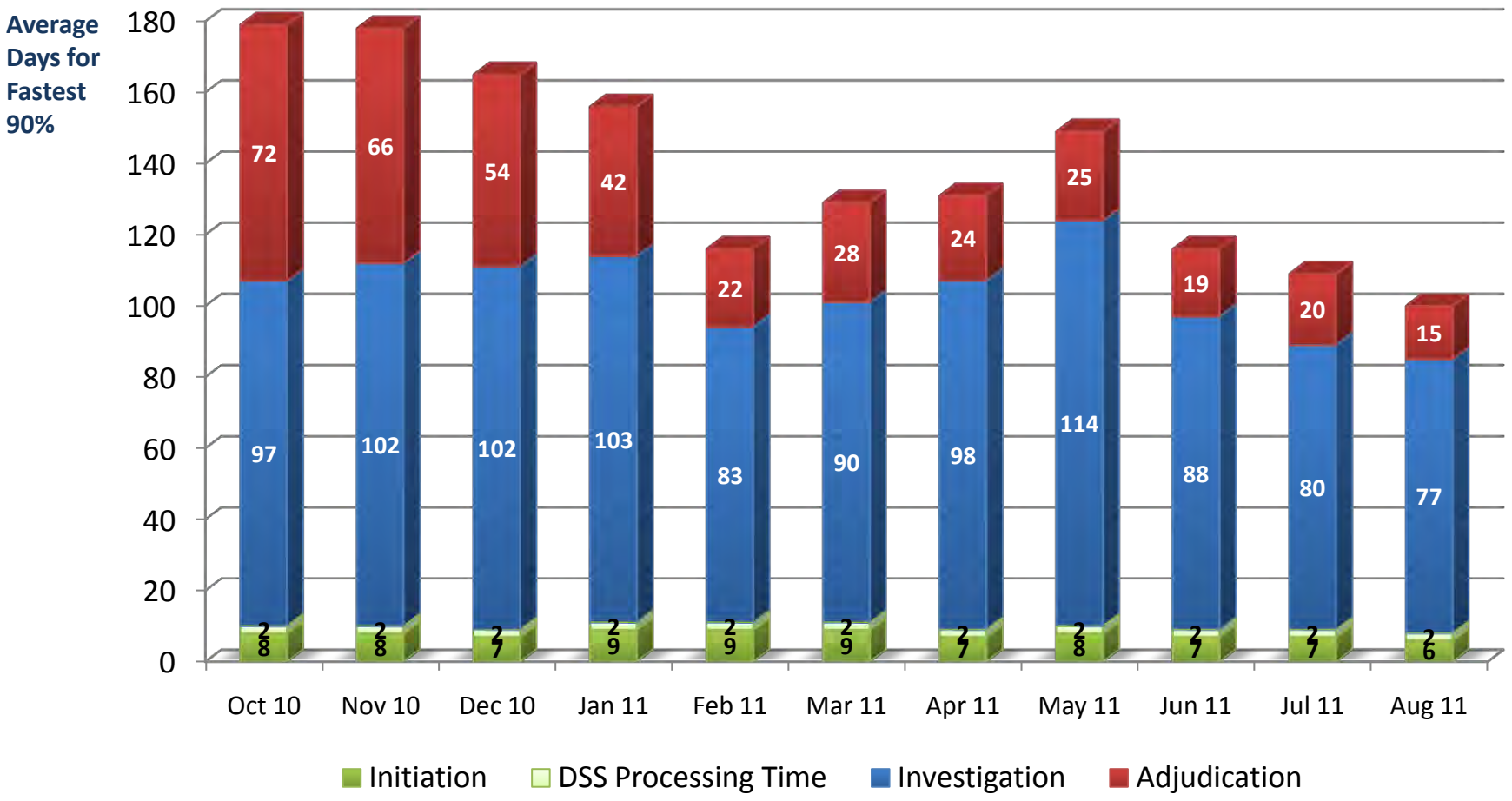
	Oct 10	Nov 10	Dec 10	Jan 11	Feb 11	Mar 11	Apr 11	May 11	Jun 11	Jul 11	Aug 11
100% of Reported Adjudications	2,282	2,669	1,781	2,035	1,776	2,943	1,714	2,301	1,743	1,511	2,166
Average Days for fastest 90%	127 days	138 days	125 days	124 days	127 days	117 days	119 days	107 days	107 days	109 days	110 days

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



	Oct 10	Nov 10	Dec 10	Jan 11	Feb 11	Mar 11	Apr 11	May 11	Jun 11	Jul 11	Aug 11
100% of Reported Adjudications	7,712	7,060	7,881	7,052	6,324	8,735	10,023	9,606	10,615	7,406	6,786
Average Days for fastest 90%	86 days	82 days	80 days	79 days	82 days	83 days	72 days	68 days	59 days	60 days	62 days

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



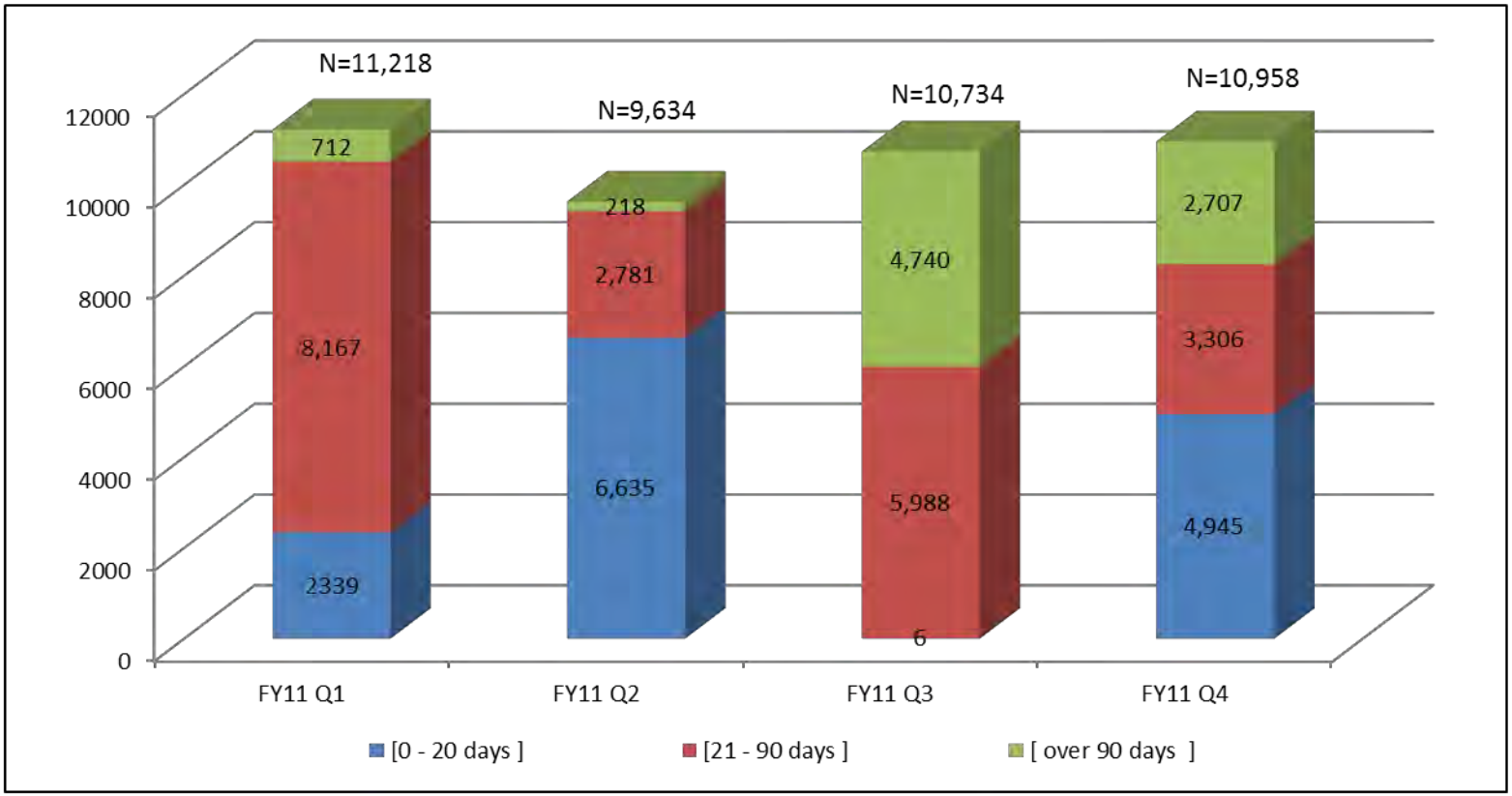
	Oct 10	Nov 10	Dec 10	Jan 11	Feb 11	Mar 11	Apr 11	May 11	Jun 11	Jul 11	Aug 11
Reported Adjudications	2,197	2,008	2,522	2,869	3,133	1,902	3,362	3,097	5,585	1,841	3,051
Average Days for fastest 90%	179 days	178 days	165 days	156 days	116 days	129 days	131 days	149 days	116 days	109 days	100 days

Attachment #3- DISCO PCL Presentation

Defense Industrial Security Clearance Office

FY11 Initial Pending Adjudications

SSBI / NACLC

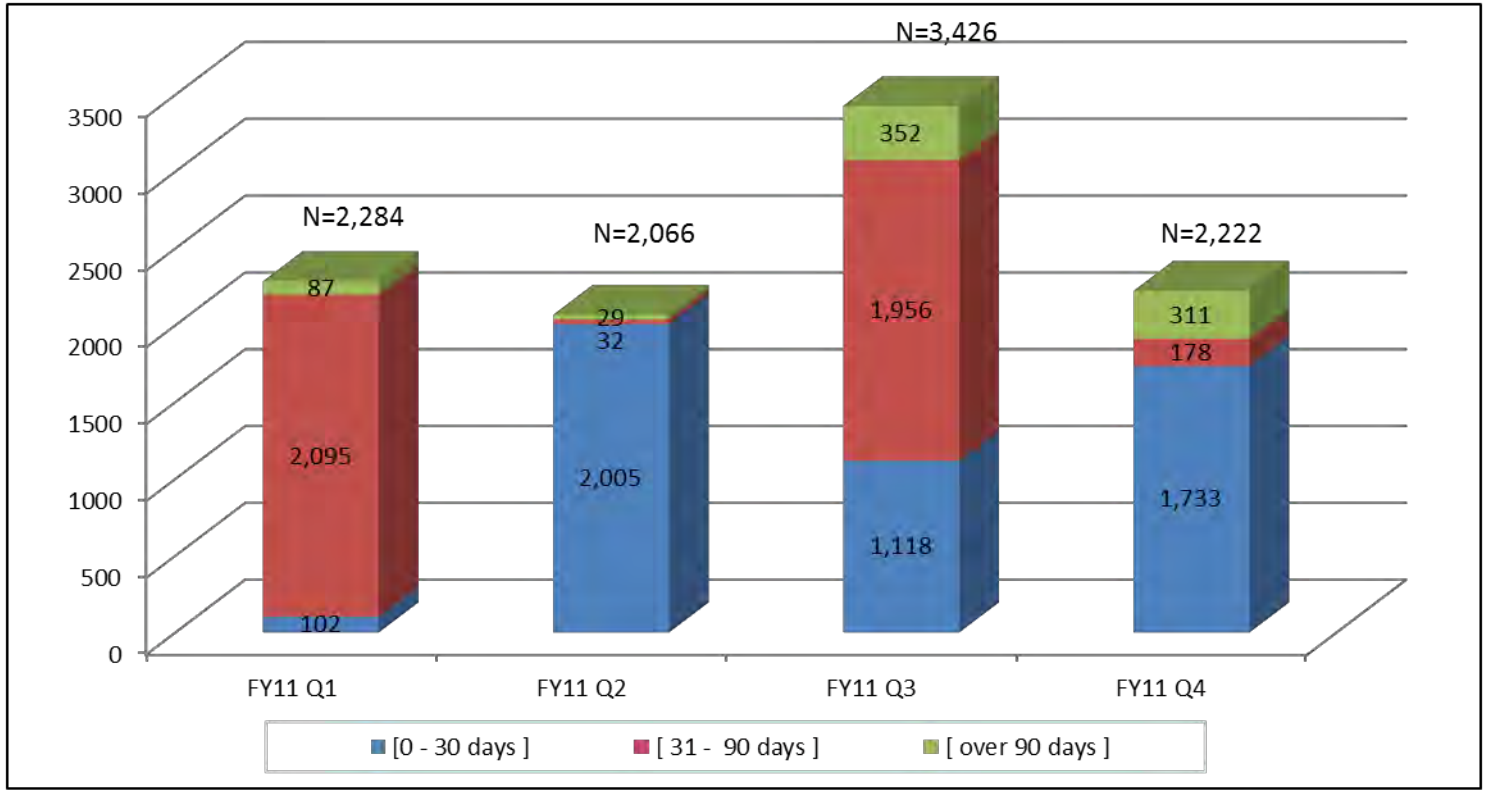


Case Type	Day Category	FY11 Q1	FY11 Q2	FY11 Q3	FY11 Q4
Initial (SSBI and NACLC)	[0 - 20 days]	2,339	6,635	6	4,945
	[21 - 90 days]	8,167	2,781	5,988	3,306
	[over 90 days]	712	218	4,740	2,707
Initial Total		**11,218**	**9,634**	**10,734**	**10,958**

Defense Industrial Security Clearance Office

FY11 Renewal Pending Adjudications

SBPR / PPR

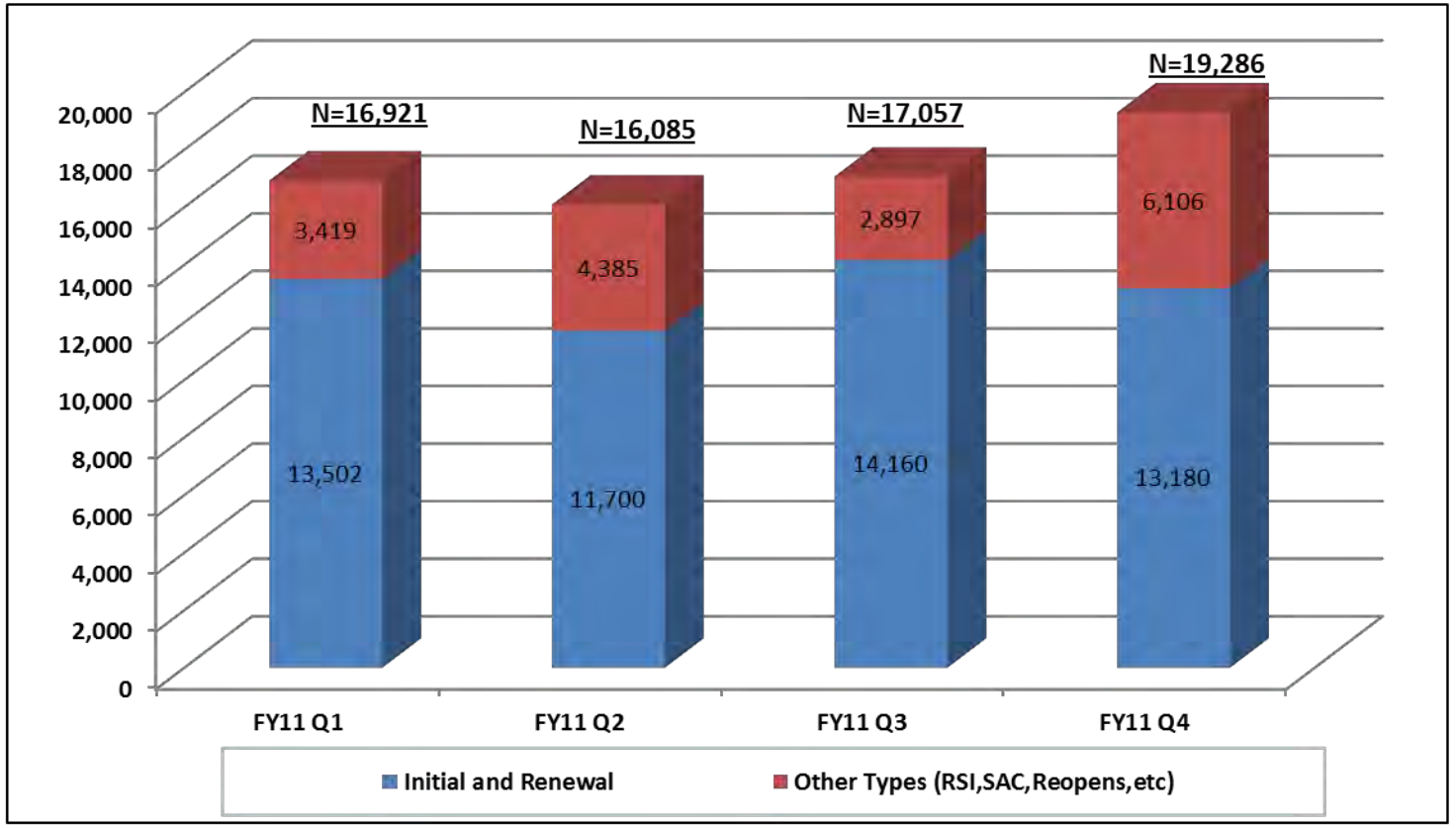


Case Type	Day Category	FY11 Q1	FY11 Q2	FY11 Q3	FY11 Q4
Renewal (SBPR and PPR)	[0 - 30 days]	102	2,005	1,118	1,733
	[31 - 90 days]	2,095	32	1,956	178
	[over 90 days]	87	29	352	311
Renewal Total		**2,284**	**2,066**	**3,426**	**2,222**

Defense Industrial Security Clearance Office

FY11 Overall Pending Adjudications

SSBI / NACLC / TSPR / Other (Suspended Cases)



Case Type	FY11 Q1	FY11 Q2	FY11 Q3	FY11 Q4
Initial and Renewal	13,502	11,700	14,160	13,180
Other (RSI, SAC, Reopens, etc)	3,419	4,385	2,897	6,106
Total	**16,921**	**16,085**	**17,057**	**19,286**

FY11 Industry Cases Pending at OPM

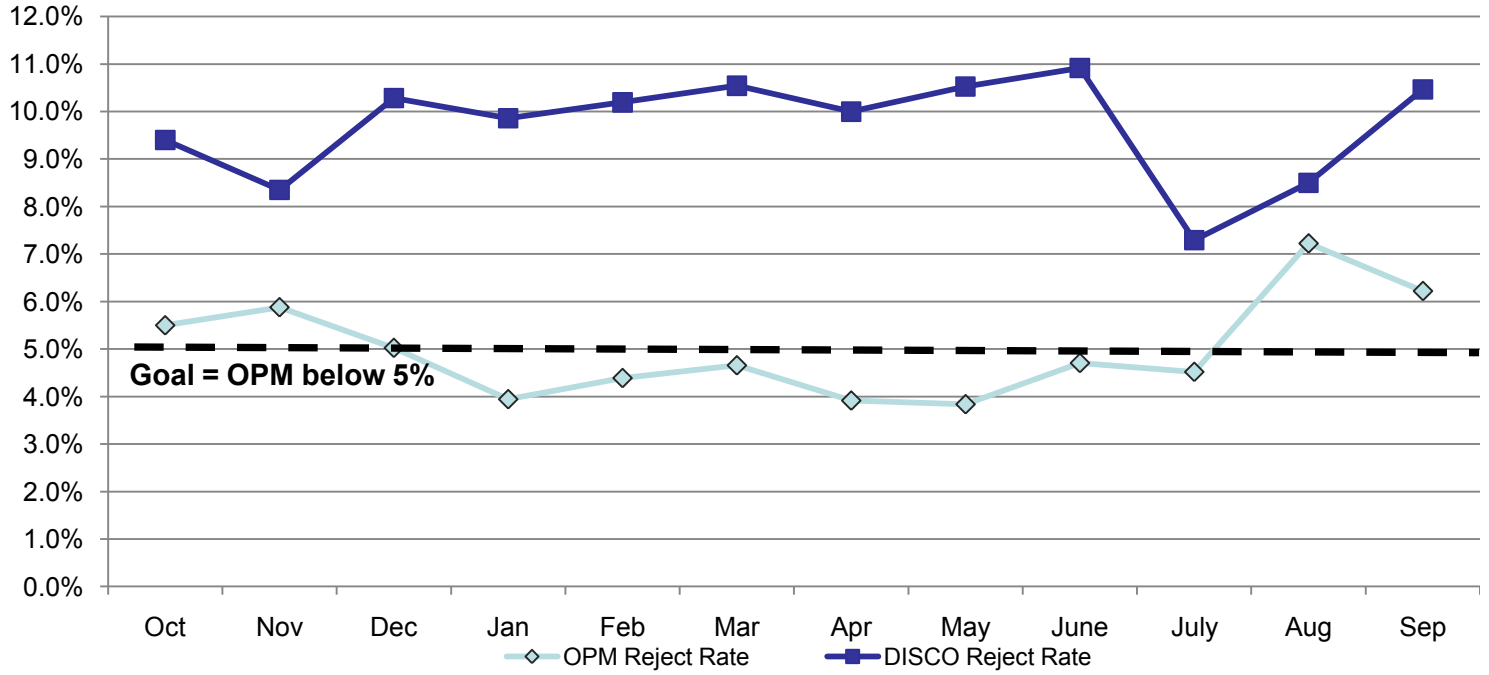
Case Type	FY09				FY10				FY11				FY11 Delta Q1 vs Q4
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
NACLC	13,209	13,982	13,900	12,307	11,730	11,685	13,016	13,556	13,118	13,243	13,861	12,929	-1%
SSBI	6,626	6,687	6,944	6,561	6,782	7,012	6,561	6,178	6,308	5,578	6,274	5,821	-8%
SSBI-PR	3,772	4,160	4,692	3,703	4,096	4,521	4,859	5,115	5,436	7,521	4,662	4,349	-20%
Phased PR	5,430	2,771	2,476	2,640	3,158	3,629	3,665	4,248	4,781	5,148	4,097	5,768	21%
Total Pending	29,037	27,600	28,012	25,211	25,766	26,847	28,101	29,097	29,643	31,490	28,894	28,867	-3%

NACLC, SSBI, TSPR inventory combined decreased 3% over FY11.

Source: OPM Customer Support Group

FY11 DISCO and OPM Reject Rates

Initial and Periodic Reinvestigation Clearance Requests



- DISCO Received 205,768 investigation requests
  - Rejects – DISCO rejected 18,770 (9.7% on average) investigation requests for FSO re-submittal

- OPM Received 187,069 investigation requests
  - Rejects – OPM rejected 9,590 (5.0% on average) investigation requests to DISCO (then FSO) for re-submittal
  - Non-receipt of fingerprint cards within 30 days accounts for an estimated 70% of rejections by OPM.

Note: Case rejection and re-submission times is not reflected in timeliness
- When a case is re-submitted, the timeline restarts for the PSI/PCL process
- Source: JPAS / OPM / DISCO Monthly Reports

FY11 DISCO Case Rejections by Facility Category

Month	FACILITY CATEGORY						
	A	AA	B	C	D	E	OTHERS
Oct	0.3%	0.1%	0.3%	0.5%	2.0%	3.5%	0.0%
Nov	0.3%	0.1%	0.3%	0.6%	2.0%	3.3%	0.0%
Dec	0.4%	0.1%	0.3%	0.7%	2.2%	3.7%	0.1%
Jan	0.4%	0.1%	0.4%	0.7%	2.7%	4.2%	0.1%
Feb	0.4%	0.1%	0.4%	0.7%	2.7%	4.8%	0.1%
Mar	0.4%	0.1%	0.4%	0.7%	3.5%	5.6%	0.1%
Apr	0.3%	0.1%	0.3%	0.7%	2.4%	4.6%	0.1%
May	0.3%	0.0%	0.4%	0.8%	2.6%	4.4%	0.1%
June	0.3%	0.0%	0.4%	0.8%	3.1%	4.9%	0.1%
July	0.3%	0.0%	0.3%	0.6%	2.0%	3.3%	0.0%
August	0.3%	0.0%	0.3%	0.6%	2.3%	4.1%	0.1%
September	0.3%	0.0%	0.4%	0.8%	3.1%	4.5%	0.2%
Grand Total	4.0%	0.9%	4.2%	8.3%	**30.5%**	**50.9%**	1.2%

100%

DISCO Case Rejections

- **81.4% of cases rejected by DISCO originate from smaller Category D and E facilities**

Source: e-Qip

FY11 Reasons for Case Rejection by DISCO

#	REASON	% Rejected	% Accounted
1	Missing employment information for the submitting agency	**26%**	26%
2	Missing complete and accurate information concerning listed debts or bankruptcy	**26%**	51%
3	Request ID Number does not match e-QIP and Certification and/or Release(s)	**9%**	60%
4	Missing legal exemption for not registering with the Selective Service	**7%**	68%
5	Non-receipt of Certification or Release Forms	**6%**	74%
6	Missing information on relative born abroad	**5%**	79%
7	Missing social security number of spouse	**4%**	83%
8	Missing social security number for adult co-habitant	**4%**	87%
9	Missing information for former spouse	**2%**	89%
10	Missing references, character, residential, employment or educational	**2%**	**91%**
11	Missing documentation of U.S. Citizen born abroad	2%	93%
12	Missing information pertaining to arrest	1%	94%
13	Missing passport information with recent foreign travel	1%	96%
14	Current residence and employment are not within commuting distance	1%	96%
15	Missing complete and accurate information concerning listed drug use	1%	97%
16	Missing complete and accurate information concerning listed foreign passport	1%	98%
17	Illegible or missing information on release forms	1%	98%
18	Missing 7 years consecutive employment history (10 years for SSBI)	1%	99%
19	Missing 7 years consecutive residence history (10 years for SSBI)	0%	99%
20	Missing complete and accurate information concerning listed foreign travel	0%	100%
21	Missing complete and accurate information concerning listed foreign financial interests	0%	100%
22	Discrepant place of birth.	0%	100%
		100%	

- 50% are attributable to missing current employment activity and financial information
- Top 10 reasons account for 91% of DISCO's case rejections

FY11 Reasons for Case Rejection by OPM

REASON	% Rejected
Missing fingerprint cards	**70%**
Certification/Release	21%
Place of Birth	6%
Miscellaneous Reasons	2%

- **The majority of OPM case rejections are due to missing fingerprint cards.**

Attachment #4- Phased PR Presentation

Phased Periodic Reinvestigation

NISPPAC

16 November 2011

PHASED PR WORKING GROUP

- Current policy permits use of the Phased Periodic Reinvestigation (PPR) for Top Secret/SCI investigations in the absence of security issues

- Investigative Service Providers (ISP) do not have a common understanding of when a PPR must convert to a full SSBI-PR

- The Security and Suitability Executive Agents established an inter-agency working group to re-evaluate and recommend “triggers” for PPR conversions

PHASED PR WORKING GROUP (continued)

- Developed “triggers” in accordance with the proposed Federal Investigative Standards “flagging” criteria (EFI) and the new SF-86
- Security Executive Agent intends to issue government-wide policy
- Issuance of policy targeted for February 2012
- Policy will be used by all ISP’s pending the implementation of the revised Federal Investigative Standards

Questions?

CONTACTS

Security Executive Agent Inquiries:
SecEA@dni.gov

Office of Personnel Management
Federal Investigative Services P.O. Box 618
1137 Branchton Road
Boyers, PA 16018-0618
(724)794-5612
www.opm.gov/investigate

Attachment # 5- Executive Order 13587 Presentation

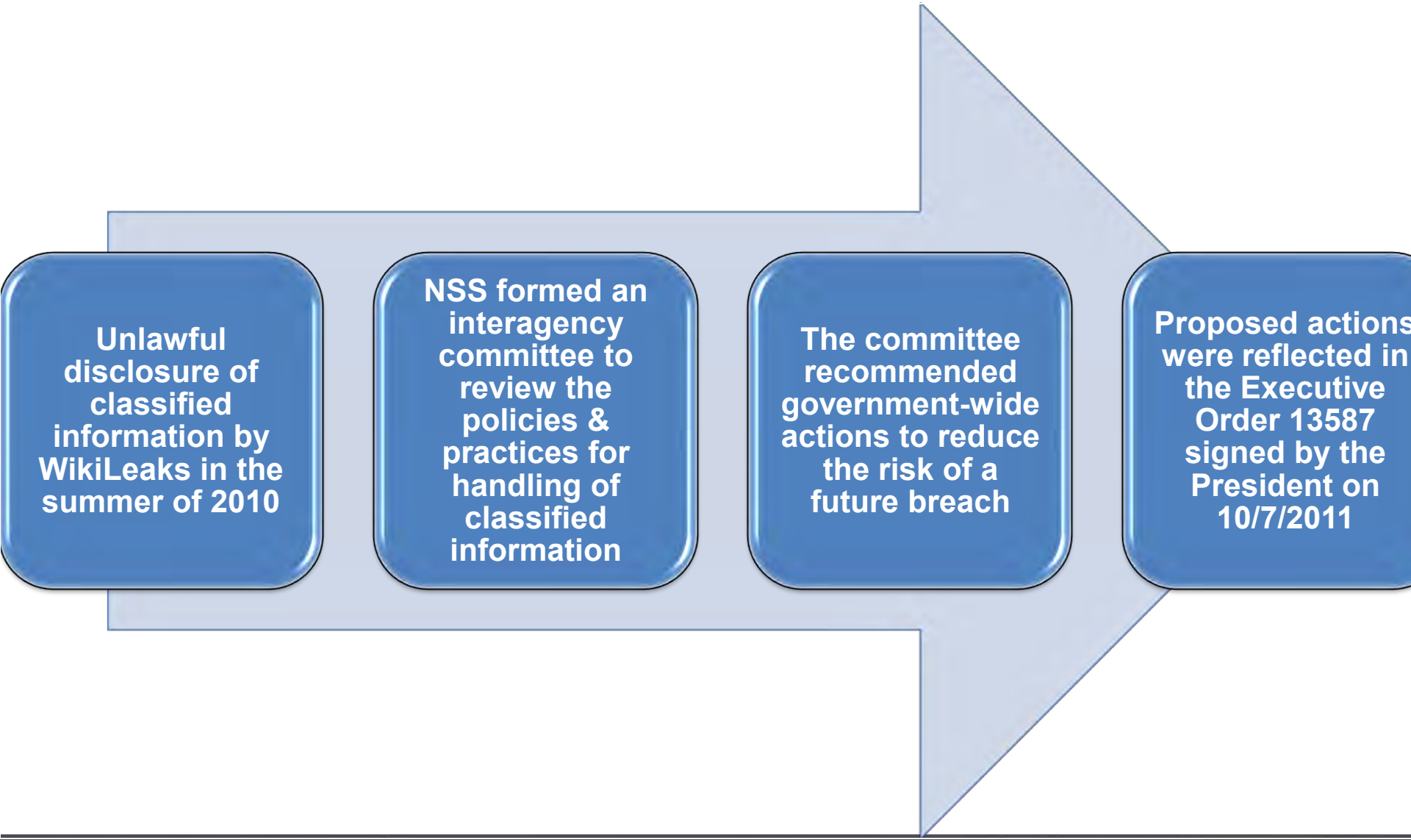
Structural Reforms to Improve Classified Information Sharing & Safeguarding

October 2011

prepared by

Classified Information Sharing and Safeguarding Office

Background


Unlawful disclosure of classified information by WikiLeaks in the summer of 2010
NSS formed an interagency committee to review the policies & practices for handling of classified information
The committee recommended government-wide actions to reduce the risk of a future breach
Proposed actions were reflected in the Executive Order 13587 signed by the President on 10/7/2011

Guiding Principles for Proposed Reforms

- Reinforce the importance of responsible information sharing – preserve all of the significant and important progress made in interagency information sharing since 9/11
- Ensure that policies, processes, technical security solutions, oversight, and organizational cultures match information sharing & safeguarding requirements
- Emphasize *consistent* guidance and implementation across the entire Federal government
- Recognize the importance of shared risk and shared responsibility
- Continue to respect the privacy, civil rights, and civil liberties of the American people

Governance Structure Established by EO

- A ***Senior Information Sharing and Safeguarding Steering Committee*** will have overall responsibility for fully coordinating interagency efforts and ensuring that Departments and Agencies are held accountable for implementation of information sharing and safeguarding policy and standards.

- A **Classified Information Sharing and Safeguarding Office** within Program Manager, Information Sharing Environment, will provide sustained, full-time focus on sharing and safeguarding of classified national security information. Will consult partners to ensure the consistency of policies and standards

- Senior representatives of the Department of Defense and the National Security Agency will jointly act as the **Executive Agent for Safeguarding Classified Information on Computer Networks** to develop technical safeguarding policies and standards and conduct assessments of compliance.

- An **Insider Threat Task Force** will develop a government-wide program for insider threat detection and prevention to improve protection and reduce potential vulnerabilities of classified information from exploitation, compromise or other unauthorized disclosure.

Responsibilities of Departments & Agencies

Agencies bear the primary responsibility for sharing and safeguarding classified information

- Designate a Senior Official
- Implement an Insider Threat Program
- Report to the Steering Committee
- Perform Self-Assessments of Compliance

Areas of Focus & Ongoing Improvement

- Enhancing control of removable media
- Identity Management; including reducing user anonymity and increasing user attribution
- Building a more robust insider threat program
- Enhancing access controls
- Improving enterprise audit capabilities

Questions?

Appendix A: References

- National Security Staff (**NSS**). Part of the Executive Office of the President (EOP). http://www.whitehouse.gov/administration/eop
- Office of the Director of National Intelligence (**DNI** or ODNI). Contains information about the organization, including the Intelligence Community Information Sharing Executive, and Intelligence Community policies (http://www.dni.gov/electronic_reading_room.htm). http://www.dni.gov/
- Information Security Oversight Office (**ISOO**), an office within the National Archives and Records Administration (NARA); responsible to the President for policy and oversight of the Government-wide security classification system and the National Industrial Security Program. www.archives.gov/isoo/index.html
- Program Manager - Information Sharing Environment (**PM-ISE**). Established by the Intelligence Reform and Terrorism Prevention Act (IRTPA). www.ise.gov
- Committee on National Security Systems (**CNSS**) website. The Assistant Secretary of Defense and Information Integration/DoD Chief Information Officer is the Chair of the CNSS http://www.cnss.gov/
- The Office of the National Counterintelligence Executive (**NCIX**) merged with the DNI's Special Security Center (SSC) and the Center for Security Evaluation (CSE) in 2010. Link to National Counterintelligence Strategy, Insider Threat Detection and Prevention Guide, and related tips. http://www.ncix.gov/

Attachment # 6- Combined Industry Presentation

NATIONAL INDUSTRIAL SECURITY PROGRAM

POLICY ADVISORY COMMITTEE

(NISPPAC)

INDUSTRY PRESENTATION

NOVEMBER 16, 2011

Outline

- Current Membership
  - NISPPAC
  - Industry MOU's
- Charter
- Working Groups
- Areas of Interest

National Industrial Security Program Policy Advisory Committee Industry Members

Members	Company	Term Expires
Scott Conway	Northrop Grumman	2012
Marshall Sanders	Cloud Security Associates	2012
Frederick Riccardi	ManTech	2013
Shawn Daley	MIT Lincoln Laboratory	2013
Rosalind Baybutt	Pamir Consulting LLC	2014
Mike Witt	Ball Aerospace	2014
Rick Graham	Huntington Ingalls Industries	2015
Steve Kipp	L3 Communications	2015

Industry MOU Members

AIA	Vince Jarvie
ASIS	Marshall Sanders
CSSWG	Randy Foster
ISWG	Mitch Lawrence
NCMS	Tony Ingenito
NDIA	Jim Hallo
Tech America	Kirk Poulsen

National Industrial Security Program Policy Advisory Committee

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

National Industrial Security Program Policy Advisory Committee Working Groups

- Personnel Security Clearance Processing
  - PKI Enabling JPAS
  - Clearance Reform
- Automated Information System Certification and Accreditation
  - Industrial Security Field Operations Manual Revision
  - End-to-End processing time metrics
- NISPOM Review
- DoD SAP Manual Review
- Industry request ISOO Sponsor a new Special Program Working Group which will take on opportunities specific to that community

Industry Areas of Interest

- Information Sharing – Threat
- Clearance Reform - Status
- Industrial Security Policy Modernization
  - National Industrial Security Program Operations Manual revision and update
  - Department of Defense Special Access Program Manual development
  - Industrial Security Regulation, Volume II update
  - CUI Reform
  - E.O. Safeguarding the U.S. Government's Classified Information & Networks

Industry Areas of Interest

- IT Security Strategy
  - Implementation – DFAR Case 2011-D039
- Repercussions from Wiki-Leaks: New Executive Order
  - Insider Threat Programs
  - Increased focus on counterintelligence
- CEO Certifications of the Company's Security Program
- Data Spills
  - Costs & Impact
  - Damage to National Security

Thank You