Minutes of the June 6, 2016 Meeting of the National Industrial Security Program Policy Advisory Committee (NISPPAC)

The NISPPAC held its 54th meeting on Monday, June 6, 2016, at the Gaylord Opryland Hotel, Nashville, Tennessee, in conjunction with the Annual Seminar of NCMS. Greg Pannoni, Associate Director, Information Security Oversight Office (ISOO), served as Chair. The minutes of this meeting were certified on September 6, 2016.

I. Welcome, Introductions, and Administrative Matters

The Chair began the meeting by acknowledging NCMS, its President, Mr. Dennis Arriaga, and its members for hosting the NISPPAC during their annual seminar.

The Chair provided an oversight of the NISPPAC, its history and purpose.

The NISP was established by Executive Order, which also established the National Industrial Security Program Policy Advisory Committee. Its purpose is to bring together the two primary partners in this program, government and industry, to work together, bring up issues that may be in dispute, make recommendations to improve the program, and serve as the official forum for communication between the government and industry. The NISPPAC has working groups whose efforts may make its way up to the committee for discussion, to advocate for or recommend a change to policy. There are two standing work groups: personnel security and certification and accreditation for information systems. A new insider threat working group was recently established. Ad hoc working groups are established as needed to address short-term matters.

Membership is comprised of 16 government representatives from agencies most affected by the NISP, and eight industry members that rotate. Industry members have four-year terms, with two coming off and two new coming on.

The Chair recognized two industry members, Tony Ingenito and J.C. Dodson, whose service is ending with this meeting. The Chair thanked them for their valuable contributions to the committee.

The Chair explained that the NISPPAC that is subject to the provisions of the Federal Advisory Committee Act (FACA).The minutes are published on the ISOO and on FACA websites. NISPPAC meetings are open to the public.

The Chair acknowledged Kathy Branch as the designated federal official for the meeting. FACA requires that the NISPPAC have a designated federal official attend all meetings.

Finally, the Chair gave an overview of the agenda (see Attachment 1) and introduced the members. (See Attachment 2 for a list of attendees.)

II. Old Business

The Chair advised members that minutes of the April 2016 meeting had been sent out for review and comment and reminded them that they had two weeks to respond to ISOO with any proposed changes.

III. New Business

(A) Proposed Change to NISPPAC Bylaws

The Chair advised that the NISPPAC has had one of the industry members serving as the spokesperson on behalf of all of the industry members for a number of years; however, the position has never been formalized in the bylaws. Mr. Ingenito is the current industry member serving as spokesperson. Industry has proposed formalizing the position in the bylaws. The chair presented proposed language to be included in the NISPPAC bylaws. (See Attachment 3.)

The Chair advised the members that the proposed language will be sent out by email subsequent to this meeting for their review and comment. Any change to the bylaws must be agreed to by two-thirds of the government members and two-thirds of the industry members. The individual filling the position of industry spokesperson should be in a position to respond relatively quickly to issues that come up from the NISPPAC and be available to attend meetings.

(B) Performance Accountability Council

The Chair introduced Teresa Nankivell, Director of the Performance Accountability Council (PAC) Program Management Office (PMO).

Ms. Nankivell provided information on the history of the personnel security reform, PAC strategic intent, and continuous performance improvement in the personnel security investigative process.

The PAC is responsible to the President for driving implementation of the reform effort, ensuring accountability by agencies, ensuring the Security and Suitability Executive Agents align their respective processes, and sustaining reform momentum. The Office of Management and Budget (OMB) is the PAC lead. The Office of the Director of National Intelligence (ODNI) is the Security Executive Agent. The Office of Personnel Management (OPM) is the Suitability Executive Agent. Those agencies, along with DoD, Treasury, Justice, FBI, and DHS make up the PAC PMO members. Thirteen agencies comprise the PAC membership. DoD is a major stakeholder because they represent 80% of the government's clearance holders.

The Chair pointed out that ISOO is a PAC member to serve as the voice for industry through the NISPPAC industry members.

Ms. Nankivell addressed the PAC strategic intent. There are three goals:

1. Instill a sense of shared responsibility and enable the Federal workforce to improve early detection of potential areas of concern.
2. Strengthen capabilities to assess the trustworthiness of the Federal workforce and manage risk.
3. Optimize government-wide capabilities to streamline service, promote reciprocity, and deliver quality and efficacy.

The PMO is working on developing performance metrics to ensure continuous improvement. Numbers and timeliness are critical measures, but future metrics will also focus on quality and effectiveness. Once desired metrics are identified, the PAC will develop a metrics implementation plan. The intent of continuous performance improvement is to improve the quality of decisions to ensure a trusted workforce.

Tony Ingenito, industry member, asked about the timeline for the next step. Ms. Nankivell responded that the PAC anticipates having the metrics reporting portfolio done sometime this summer, but that identifying what metrics to capture and coordinating is a slow process.

Greg Pannoni, ISOO, asked what linkage there is between the work that is being looked at and researched and the ability to pay for the best way forward. He mentioned that all have limited budgets. Ms. Nankivell responded that reform has emphasized automation to the greatest extent possible and practical. The research projects look at ways to further automate. E-adjudication is an example of trying to eliminate the manual components of the process as much as possible. Continuous evaluation is another example. Even further, there is the idea of continuous vetting for the entire trusted federal workforce; i.e., a continuous process to re-look at decisions already made. Those are some examples of possible cost savings.

(C) Security Executive Agent – Policy Update

The Chair introduced Gary Novotny from the National Counterintelligence and Security Council, Office of the Director of National Intelligence, to give a policy update on behalf of the Security Executive Agent on continuous evaluations (CE) and recent policy on the use of social media in background investigations. See the Security Executive Agency Policy Update slides at Attachment 4.

Mr. Novotny described CE as the process to review an individual's background between the original initial background investigation and in between the periodic reinvestigations. It is applied for those individuals who have been determined eligible for access to classified information or those individuals in those sensitive positions. It includes automated record checks of commercial databases, U.S. government databases, or other information lawfully available to security officials. It applies the business rules from the 2012 Federal Investigative Standards and allows for notification to personnel security officials of adjudicatively relevant information on a more frequent basis. A CE working group has been meeting for the last few years to identify the appropriate checks. The Federal Investigative Standards, which were signed by both the director of OPM and the DNI in December 2012, state that CE is required for individuals cleared at the tier five level, which is scheduled to be implemented in September 2016 for 5% of tier five individuals. Recent omnibus legislation addressed application to the tier three population; i.e., cleared at the secret level.

The ODNI is working on both policy and technical capability. Policy will address the standards and requirements. Technical capability is being addressed right now on TS/SCI classified networks. Those agencies that don't have access to TS/SCI networks will receive a flag that there is an issue. The technical capability will be able to process the entire tier three and tier five eligible populations.

Mr. Novotny addressed the CE program milestones which anticipate that each executive branch agency will have enrolled at least 5% of its tier 5 population in the CE process by September 30, 2017. ODNI also has an oversight role to review agency compliance.

Greg Pannoni, ISOO, asked when CE will be expanded to all the tier 5 TS/SCI individuals, and not just the projected 5% by 2017. Mr. Novotny did not have the answer as to any plan to expand and have that percentage go up every year; however, there will not be a plan that involves redoing the same 5% over and over again. He advised that full operating capability for CE is 5% of the tier five population and that it will be up to the agencies to identify those individuals.

Michelle Sutphin, industry member asked how CE ties into the Enhanced Personnel Security Program which requires two records checks within a five-year period for the tier three population. Mr. Novotny responded that the ODNI is still trying to determine if CE and the technical capability that ODNI is creating will fulfill that requirement.

Mr. Novotny addressed the policy to allow the collection, use, and retention of publicly available social media information in background investigations and adjudications. The DNI recently issued Security Executive Agent Directive Five to address the use of social media. It applies only to publicly available social media information on the individual that is undergoing a background investigation. Investigators and adjudicators cannot require individuals to provide a password, to login into any kind of private account, or take any action that would disclose non-publicly available social media information. This is just one piece of the background investigation that still needs to be corroborated under the whole person concept just like any other kind of investigative lead.

Dennis Keith, industry member, asked if any explanatory guidance was going to be offered with regard to what constitutes "publicly available". Mr. Novotny advised that definitions are in the Security Executive Agent Directive, some of which came from the office of the chief information officer.

Steve Kipp, industry attendee, asked if there is any type of vetting process to ensure that the social media information is reliable. Mr. Novotny responded that both the Federal Investigative Standards and the adjudicative guidelines require corroboration of information.

IV. Reports and Updates

(A) National Background Investigations Bureau (NBIB) Transition Team

The Chair introduced Christy Wilder, Deputy Team Lead for the National Background Investigations Bureau (NBIB) Transition Team to give an update on the progress the NBIB. Ms. Wilder announced that she will be hosting two breakout sessions during the seminar where she will be providing more information for anyone who is interested in attending.

She provided some background on the NBIB, which came about as a result of recommendations from the 90-day review after the OPM data breach. The NBIB transition team was stood up in March of this year. It is an interagency team, with representatives from Veterans Affairs, ODNI, Justice, Alcohol, Tobacco, and Firearms, OPM, and OMB, to name a few, with more team members coming on board.

The NBIB has five main work streams:

1. Change management, with responsibility for a communication plan.
2. Business process, analysis, and reengineering.
3. Resource management, to develop metrics.
4. Information technology and cyber security to work with DoD to build the new system.
5. Mission management and support, responsible for the establishing the organization to ensure greater emphasis on national security.

The transition team is doing much work to maintain the current legacy system for investigations while waiting for the new system to be built.

NBIB will formally stand up on October 1, 2016. Just like the transition team, the NBIB will comprised of representatives from many different agencies, with a focus on national security.

(B) Industry Update

The Chair advised the attendees that the industry members of the NISPPAC represent all of industry. The eight industry members are listed on the ISOO website with contact information so that anyone in industry can reach out to them as necessary for issues to be addressed through the NISPPAC process. The Chair introduced Tony Ingenito to provide the industry update.

Mr. Ingenito began by thanking the NISPPAC for the opportunity to serve as an industry member for four years. The industry members will begin the nomination process to replace both him and J.C. Dodson, effective the next meeting in November. See NISPPAC Industry slides at attachment 5.

Mr. Ingenito reported on a recent issue concerning a Department of Commerce survey in conjunction with DSS that was being sent out to all cleared contractors under DoD cognizance. The 30-page survey asked for much information that went very deep into company business and raised many concerns across industry. The NISPPAC industry members notified ISOO, who scheduled an impromptu meeting with DSS and Department of Commerce that gave the

NISPPAC industry members an opportunity to share their concerns. The result of the meeting was considered to be positive, providing industry with a better understanding of the intent of the survey. As a next step, DSS will develop a communication plan for the survey.

One of the roles of the NISPPAC industry members is to stay on top of issues that impact industry. Mr. Ingenito addressed issues in the area of personnel security as one of those issues. Funding for credit monitoring as a result of the OPM data breach has impacted available funding for background investigations, and DSS has suspended processing periodic reinvestigations until FY 2017. This causes some agencies to consider that investigations of industry personnel are out of date, impacting such things as ability to access a particular program or get onto a particular base. The new investigative standards for tier three and tier five put additional stress on the already burdened personnel security system. The NISPPAC personnel security working group is looking for consistent implementation by the government regarding the age of investigations when it comes to providing access.

Mr. Ingenito advised that industry was pleased with the recently released Change 2 of the NISPOM, and the associated standup of the NISPPAC Insider Threat Working Group. The working group provides an opportunity for industry and the cognizant security agencies to address any inconsistencies that may arise from implementation of insider threat provisions for industry across agencies.

Industry is participating in a complete rewrite of the NISPOM through the NISPPAC NISPOM Working Group. Michelle Sutphin is the lead for industry on the rewrite effort, with outreach to approximately 75 industry representatives for feedback on proposed changes. This process ensures input from all sizes and types of companies.

Mr. Ingenito advised that all of the DoD Special Access Program (SAP) manuals have been issued, and that the Joint Air Force, Army, and Navy guidance has been rescinded. This will result in more consistent application of SAP policies across industry.

Industry members are tracking policy integration issues across the agencies by means of a policy tracking spreadsheet, and monitoring the impact of the policies on industry.

Mr. Ingenito advised that the personnel security working group is moving from a focus on statistics in order to address other issues that are impacting the personnel security clearance process and creating backlogs. Industry is interested in monitoring the standup of the NBIB.

The certification and accreditation working group is addressing the implementation of the risk management framework (RMF) process for information system authorization. Mr. Ingenito advised that Steve Kipp stays involved with the group, along with other NISPPAC industry members and other industry representatives. The working group is reviewing the revised DSS process manual for authorization and approval of industry systems to process classified information. He expressed concern on behalf of industry regarding DSS' plan to implement the RMF process in six months, based on the anticipated learning curve involved for both government and industry personnel. DSS initial rollout of RMF implementation will be for standalone systems that represent approximately 80% of the systems that are authorized to process classified information in industry.

Industry is interested in the implementation of the NISP Contract Classification System (NCCS) by DSS. Industry has been involved in identifying requirements and beta testing, and now looking forward to the roll-out.

Industry is also interested in the development and implementation of the National Industrial Security System (NISS) by DSS, and were pleased to be part of the requirements identification phase.

Finally, Mr. Ingenito addressed industry involvement in the development of the Joint Verification System (JVS). Quinton Wilkes, NISPPAC member, actively represents industry. Industry is concerned about system roll-out without a training plan in place to ensure data reliability for the long-term.

(C) Implementing Directive Update

The Chair introduced Kathy Branch to give an update on the revision of the NISP Implementing Directive, which is the NISP policy guidance for the federal agencies.

Ms. Branch provided some background on the NISP Executive Order which directs ISOO to issue implementing directives for the agencies under the NISP. The current directive was last updated in 2010 to add the NID process to the national policy. Since then a number of new policies have come out that impact the NISP. Executive Order (EO), "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information", required establishment of insider threat programs, with requirements for both industry and NISP agencies. Another EO, "Promoting Private Sector Cybersecurity Information Sharing", amended the NISP executive order to make DHS a cognizant security agency (CSA). ISOO had never updated the directive to incorporate the establishment of the ODNI from the "Intelligence Reform and Terrorist Prevention Act". ODNI became the CSA to replace CIA. In addition, DoD started the NISPOM rewrite process, which pointed out many gaps in the policy for the CSAs and other government agencies that release classified information to industry. ISOO is addressing all of this in the revision.

The draft revision is in the process of informal coordination with all of those government agencies that either are a CSA or that release classified information to industry. ISOO will have comments back at the end of June. The draft will likely be formally coordinated through the interagency as well as a 30-day public review process through the OMB federal register process. ISOO is committed to publishing the revised directive during this current administration.

(D) Controlled Unclassified Information (CUI) Update

The Chair introduced Mark Riddle, from the ISOO CUI staff, to provide an update on the progress of the CUI program. Under the National Archives and Records Administration

(NARA), ISOO serves as the Executive Agent for the CUI program. The Chair advised that there are an estimated 300,000 contractors that have access to CUI.

Mr. Riddle announced that he will be hosting two breakout sessions on CUI during the seminar where he will be providing more information for anyone who is interested in attending.

CUI is unclassified information for which a law, regulation, or government-wide policy establishes protection requirements. Mr. Riddle addressed the timeframe for the CUI program. ISOO is waiting for OMB to provide the date for publication of the 32 CFR 2002, CUI. Once published, agencies have 60 days to implement. Expectations for the first couple of years of the programs include agencies marking documents with appropriate CUI markings and contracts modified to reference the CUI standards. Agencies will be developing and implementing their own internal agency policies.

Mr. Riddle provided his email address: mark.riddle@nara.gov, for any questions after the meeting.

(E) Department of Energy (DOE) Update
The Chair introduced Carl Piechowski to provide a CSA update from DOE.

Mr. Piechowski first addressed DOE personal security processing timelines. DOE normally meets its 20-day mandate for adjudication process. However, the time has been increasing at two of the eight DOE adjudication centers. This should be a temporary issue as old cases are being worked through, which tends to skew the numbers. DOE should be back to a steady state by the end of the summer.

Mr. Piechowski addressed the impact of OPM's backlog of investigations on DOE. DOE is granting more interim security clearances.

He addressed the NBIB, noting that DOE is pleased with the progress of the organization, and expressed encouragement to OPM from DOE.

Finally, Mr. Piechowski reported that DOE has been working with DoD and NRC to develop agreements on how the agencies are going to work together when two or more of them have an interest in the same contractor. The agreements address security cognizance and consistency in implementing NISP policy. Among the issues being addressed are security cognizance, use of contractors, processes, and conflicting requirements.

(F) Department of Defense (DoD) Update

The Chair introduced Greg Torres to provide the NISP Executive Agent update on behalf of DoD.

Mr. Torres began by noting the high level of cooperation between government and industry.

Mr. Torres addressed the issue of reciprocity that had been raised during the industry update, and the problems associated with overdue periodic reinvestigations (PRs). He advised that this is inconsistent interpretation of policy across the agencies. He encouraged industry to notify either his office or DSS when they encounter access problems because of overdue PRs. It is only by having specific information that DoD can make any change. Anecdotal information is not helpful or sufficient for any action to make change happen.

Mr. Torres addressed the issue of training for JVS that had been raised in the industry update. He advised that his office is responsible for ensuring that training is created, but acknowledged that the development team is working on a condensed time schedule.

Mr. Torres discussed clearance delays, noting that a small group comprised of DoD, the DoD CAF, DSS, OPM, and others have been meeting to address the impact to DoD and make recommendations. This group developed several recommendations that is pushing to ODNI for consideration. Mr. Torres acknowledged the precariousness of the situation; i.e, this can'tbe business as usual.

Mr. Torres mentioned the Industrial Security Letter issued to clarify the insider threat provisions in the recently issued change #2 to the NISPOM. He thanked Valerie Heil and Priscilla Matos of his staff for their efforts in getting the NISPOM change published.

Mr. Torres shared that Carrie Wibben, now the Director of Counterintelligence and Security in the Office of the Under Secretary of Defense for Intelligence, has a vision for better integrating counterintelligence and security. He acknowledged the work that DSS is doing to move toward a more risk-based approach, which ties into that vision.

Lastly, Mr. Torres addressed the NBIB, noting the positive changes coming to the investigative process, and the opportunity that will result from OPM and DoD working together to build the new IT system. The NBIB's the business process reengineering process includes many stakeholders from across the government. They will take the best of what they have and improve it, with the opportunity to build what isn't there today. It will take time to do all this, but DoD will be an excellent partner with OPM to develop the system.

(G) Defense Security Service (DSS) Update

The Chair introduced Dan Payne, Director of DSS. Mr. Payne began by addressing the issue of DSS delays in processing reinvestigations and submitting them to OPM. He advised that this is a temporary situation, expected to be resolved by mid-September. He recognizes that delays in the reinvestigations causes additional risk as individuals continue to have access to classified information.

Mr. Payne addressed the new insider threat provisions in change 2 of the NISPOM. DSS will be providing sessions on insider threat during the seminar. Insider threat training is required for personnel who access classified information in accordance with change 2 of the NISPOM. DSS Center for the Development of Security Excellence (CDSE) offers the training. Since the beginning of this fiscal year, more than 5,000 industry personnel have completed the course.

Industry personnel assigned duties related to insider threat program management also have minimum training requirements, also available CDSE. Nearly 500 industry personnel have completed this training in the first six months of 2016.

Mr. Payne noted that this training is more important than ever before because of the threats we face from foreign intelligence services. In response to the threat, DSS is moving to a risk-based analysis and mitigation approach to oversight rather than strict compliance, based on intelligence coming from the intelligence community relative to what is being targeted. DSS wants to work with industry to identify what needs to be protected and establish focused security programs. The goal is to add more analytical rigor, and to secure what needs to be secured, and secure it in way that actually provides protection.

(H) NISP Contract Classification System (NCCS)

The Chair introduced Ms. Lisa Gearhart, DSS program manager and functional lead for the NCCS. Ms. Gearhart provided some background on NCCS development. The system is intended to automate the current manual process for contract security classification specifications (DD Form 254), provide a central repository for information, and disseminate and maintain the information. It is a single, web-based system that eliminates the paper and manual process and defines rule-based workflow. DSS partnered with DoD's Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD(AT&L)) to build NCCS within their existing wide area workflow system. DSS met with both industry and government stakeholders to define the requirements and the capabilities for the system.

DSS has established an NCCS governance board to identify future requirements. It held its kick-off meeting in May. DSS is also working with OUSD(AT&L) to develop a FAR clause to mandate use of NCCS. DSS would also like to be able to link NCCS to other NISP-related systems in the future.

Implementation of NCCS is being phased. Initially, it will begin with three or four agencies and industry partners. DSS plans to add two or three additional agencies and industry partners every two months. The system should reach full operating capability in December of this year with the release of version 5.91, which will allow both primes and subcontractors to view their DD Forms 254 in the system, providing transparency into the supply chain. DSS will continue to enhance NCCS and add the requirements identified by the governance board.

Ms. Gearhart will be conducting sessions through the week of the NCMS annual seminar for those who are interested in more information.

V. Working Groups

(A) Insider Threat Working Group Report

The Chair provided the report for the recently established NISPPAC Insider Threat Working Group. ISOO hosted the initial meeting. The working group will continue as long as the

NISPPAC members decide it is useful. Insider threat is a new program for industry, so implementation will present challenges. One size does not fit all for the different types of companies and circumstances. The government has to be flexible; programs need to be scalable. The goal is to prevent the insider from doing harm.

(B) Personnel Security Clearance Working Group Report

OPM:

The Chair introduced Lisa Loss to provide the timeliness performance metrics for submissions, investigations, and adjudications of DoD industry cases. (See attachment 6.) Ms. Loss reported that investigations are taking longer right now: over 200 days for top secret investigations, over 100 days for secret investigations, and those numbers are continuing to grow for FY16. With additional resources and targeted measures applied to the backlog, the numbers will begin to come down, but it will be a few more quarters until there is a noticeable difference.

Ms. Loss explained some of the factors contributing to the backlog, which began in August, 2014, when OPM issued a stop work order to their prime contractor. OPM then made the decision not to renew the terms of that contract, and had to distribute investigative capacity to their two other contractors. In addition, for the first six months of this year, there has been a heavier than expected workload. OPM is doing all that it can to maximize efficiency to address the resulting backlog. OPM is continuing to backfill vacancies as they occur, with a plan to hire 400 additional federal investigators by the end of FY16. However, new hires require training and the impact of the learning curve before they can make an impact on reducing the backlog. OPM contractors are also committed to increasing production. OPM is re-competing both field work and support contracts. OPM has a number of efficiency initiatives underway, such as working with the central adjudicative facilities to implement streamlined report writing.

To accommodate granting interim clearances, OPM is tracking the timeliness of national agency checks and working with the interagency to resolve time lags. FBI name checks are one of those experiencing lengthy timeframes. OPM and FBI are working together, and FBI is hiring additional people to solve the problem.

ODNI

The Chair re-introduced Mr. Gary Novotony from ODNI to provide the intelligence community industry performance metrics. (See attachment 7.) Mr. Novotny reported an increase in timelines for initial SECRET and TOP SECRET, and for periodic reinvestigations. ODNI is trying to determine if the sharp increase in the time for the SECRET cases is the impact of implementation of Tier 3 or the impact of legacy cases on the system.

Mr. Novotony addressed industry concerns about reciprocity because of periodic reinvestigations more than five years old. DNI Clapper issued Intelligence Community

Directive (ICD) 704 that addresses reciprocity of TS/SCI clearances more than five years old and due for a periodic investigation. The ICD advises users in the intelligence community that if the previous investigation is over five years, and between five and seven years, an agency may grant access if they conduct a review and initiate the periodic reinvestigation. For previous investigations between seven and nine years old, reciprocity is on a case-by-case basis. Director Clapper extended the guidance in ICD 704 to collateral clearances by executive correspondence in October 2013. However, the DNI's guidance is marked FOUO, so it cannot be publicly posted or disseminated. ODNI is working to make the DNI's guidance on reciprocity of collateral clearances publicly available.

DoD CAF

The Chair introduced Mr. Ned Fish to provide the update for the DoD CAF. (See attachment 8.) Mr. Fish reminded attendees that about three years ago the DoD CAF had a backlog of about 14,000 cases. The CAF has now completed 91% of these cases though the efforts of the Defense Office of Hearings and Appeals (DOHA) and its director, Mr. Russell Hunter. There are currently approximately 3,000 industry cases in some stage of due process, but with about 1,300 counted as backlog.

Mr. Fish addressed some of the items that will impact the DoD CAF operations in the near future:

> The Clearance Adjudication Tracking System (CATS), the single joint system for adjudications to replace JAMS and JPAS will be deployed soon by the Defense Manpower Data Center (DMDC). There is some slippage in the deployment date. The single portal for security managers and facility security officers (FSOs) will likely be deployed in the early part of next year. Once deployed, personnel will have to be taken off production for training.
>
> The DoD CAF is working closely with the OUSD(I) and the ODNI on the continuous evaluation (CE) efforts. The reports from CI that are expected to increase the CAF workload require resources to be hired and trained.
>
> There will be benefit from the revised e-adjudication. It should be out soon for tier three investigations, with tier one and tier two e-adjudication capability to follow. However, it first has to be incorporated into version 4 of CATS.

Mr. Fish reminded attendees that when he first addressed NISPPAC three years ago, the backlog portion of the industry portfolio represented about 7-8% of the total. Now, that number stands at less than 1%. The CAF found that between 23 - 27% of the cases that were closing were the old backlog cases. Getting those cases out of the system makes a big improvement in meeting the timelines.

(C) Certification and Accreditation Working Group Report

The Chair introduced Ms. Tracy Brown, DSS, to present the Certification and Accreditation Working Group report. (See attachment 9.) The priority for the working group right now is the transition to the risk management framework (RMF) and the implementation of the new DSS authorization and assessment process manual. DSS is conducting a pilot with industry through June 30. One of the lessons learned so far from this pilot is the learning curve required to transition to the RMF process.

The working group is considering a name change to align more closely with current policy. The name change will be addressed at the next working group meeting.

Ms. Brown advised that she will be hosting two workshops during the coming week's seminar for anyone who is interested in learning more about RMF and DSS implementation.

VI. General Open Forum/Discussion

There was no further discussion and no additional questions.

VII. Closing Remarks and Adjournment

The Chair announced the next two NISPPAC meetings, to be held in the National Archives in Washington, DC, on November 10, 2016, and March 15, 2017.

The Chair adjourned the meeting.

List of Attachments

1. Agenda
2. NISPPAC Attendee List, June 6, 2016
3. Proposed Change to NISPPAC By-Laws
4. Security Executive Agent Policy Update
5. NISPPAC Industry Update
6. OPM Update
7. ODNI Update
8. DoD CAF Update
9. C&A Working Group Update

Attachment #1

National Industrial Security Program Policy Advisory Committee (NISPPAC) Meeting
Monday, June 6 – 2:00 p.m. – 4:30 p.m.
Gaylord Opryland Hotel, Delta Ballroom D, Nashville, TN

Agenda

I. **Welcome, Introductions, and Administrative Matters** **5 minutes**
Greg Pannoni, Associate Director, Information Security Oversight Office (ISOO)

II. **New Business**

- **Proposed Change to NISPPAC Bylaws** **5 minutes**
  Greg Pannoni, ISOO

- **Performance Accountability Council (PAC)** **35 minutes**
  - **PAC Strategic Intent**
  - **Continuous Performance Improvement**

  Teresa Nankivell, PAC Program Management Office

- **Security Executive Agent – Policy Update** **15 minutes**
  - **Continuous Evaluation**
  - **Social Media and Background Investigations**

  Gary Novotny, Office of the Director of National Intelligence
  National Counterintelligence and Security Center

III. **Reports and Updates:**

- **National Background Investigations Bureau (NBIB) Transition Team** **5 minutes**
  James Onusko, Team Lead
  Christy Wilder, Deputy Team Lead

- **Industry Presentation** **10 minutes**
  Tony Ingenito, Industry Spokesperson

- **NISP Implementing Directive Update** **5 minutes**
  Kathleen Branch, ISOO

- **Controlled Unclassified Information (CUI) Update** **10 minutes**
  Mark Riddle, ISOO

- **Department of Energy (DOE) Update** **5 minutes**
  Carl Piechowski, DOE Industrial Security Policy

- **Department of Defense (DoD) Update** **5 minutes**
  Ben Richardson, Office of the Undersecretary of Defense for Intelligence

- **Defense Security Service (DSS) Update** **5 minutes**
  Dan Payne, Director, DSS

- **NISP Contract Classification System (NCCS)** **10 minutes**
  Lisa Gearhart, Defense Security Service

IV. Working Groups:

- **Insider Threat Working Group Report** **5 minutes**
  Greg Pannoni, ISOO

- **Personnel Security Clearance Working Group Report** **10 minutes**
  Lisa Loss, OPM
  Gary Novotny, ODNI
  Ned Fish, DoD CAF

- **Certification & Accreditation Working Group Report** **5 minutes**
  Tracy Brown, DSS

V. General Open Forum/Discussion **10 minutes**

VI. Closing Remarks and Adjournment **5 minutes**

Attachment #2

NISPPAC MEETING ATTENDEES

The following individuals attended the June 6, 2016, NISPPAC meeting:

Greg Pannoni	Information Security Oversight Office	Acting Chair
Kathleen Branch	Information Security Oversight Office	Designated Federal Official
Teresa Nankivell	Performance Accountability Council	Observer/Presenter
Gary Novotny	Office of the Director of National Intelligence	Attendee/Presenter
Christy Wilder	Office of Personnel Management	Attendee/Presenter
Tony Ingenito	Industry	Member/Presenter
Mark Riddle	Information Security Oversight Office	Attendee/Presenter
Carl Piechowski	Department of Energy	Attendee/Presenter
Greg Torres	Department of Defense	Alternate/Presenter
Dan Payne	Defense Security Service	Attendee/Presenter
Lisa Gearhart	Defense Security Service	Attendee/Presenter
Lisa Loss	Office of Personnel Management	Observer/Presenter
Edward Fish	DoD Central Adjudication Facility	Attendee/Presenter
Tracy Brown	Defense Security Service	Attendee/Presenter
Justin Walsh	Department of Defense	Attendee
Chris Heilig	Nuclear Regulatory Commission	Attendee (by phone)
Amy Roundtree	Nuclear Regulatory Agency	Attendee
Scott Ackiss	Department of Homeland Security	Member (by phone)
Anthony Smith	Department of Homeland Security	Alternate (by phone)
Zudayaa-Taylor Dunn	NASA	Attendee (by phone)
Anna Harrison	Department of Justice	Member (by phone)
Mary (Beth) Podzemny	Central Intelligence Agency	Attendee
Anna Harrison	Department of Justice	Member (by phone)
Michael Hawk	Department of State	Attendee
David Lowy	Department of the Air Force	Member
Jeffrey Bearor	Department of the Navy	Member
Glenn Clay	Department of the Navy	Alternate (by phone)
Dennis Hanratty	National Security Agency	Member
Shirley Brown	National Security Agency	Attendee
Fred Gortler	Defense Security Service	Member
Keith Minard	Defense Security Service	Alternate
Michelle Sutphin	Industry	Member
Bill Davidson	Industry	Member
Quinton Wilkes	Industry	Member
Phil Robinson	Industry	Member
Dennis Keith	Industry	Member
Rick Lawhorn	MOU Representative	Attendee
Dennis Arriaga	MOU Representative	Attendee
Brian Mackey	MOU Representative	Attendee

Perry Russell-Hunter	Defense Office of Hearings and Appeals	Attendee
Jim Kren	Defense Security Service	Attendee
Gus Greene	Defense Security Service	Attendee
Kevin Jones	Defense Security Service	Attendee
Heather Sims	Defense Security Service	Attendee
Selena Hutchinson	Defense Security Service	Attendee
Heather Green	Defense Security Service	Attendee
Charles Tench	Defense Security Service	Attendee
Ryan Dennis	Defense Security Service	Attendee
Jeff Spinnanger	Defense Security Service	Attendee
Stephanie LaBeach	Defense Security Service	Attendee
Miladys Ortiz	Defense Security Service	Attendee
Denise Arel	Defense Security Service	Attendee
Betty Leach	Defense Security Service	Attendee
Charlena Edge	Defense Security Service	Attendee
Robert Tringali	Information Security Oversight Office	Attendee (by phone)
Joseph Taylor	Information Security Oversight Office	Attendee (by phone)
Dolly Hawk	Public	Attendee

Other Industry Attendees:

Lisa Benner
Jessica Blevins
Krista Chase
Jane Coble
Glynn Davis
Jane Dinkel
Mary Edington
Sheri Escobar
William Fallica
Liz Fant
Sheila Garland
DeAngelo Gatling
Suzanne Gregory
Debora Hansen
Kathryn Hare
Jim Harris
Kelly Higgin
Felicia Jefferson
Phil Jones
Trish Keller
Dan Kennard
Steve Kipp
Jen Kirby
Gary Klein

Nissa Kunkel
Mitch Lawrence
Wanda Lothrop
Edith Mate
Melanie Miller
Leandra Mosher
Leonard Moss
Amanda Moutogiannis
Ashley Moya
Larry Mustonen
Ron Newsom
Trevor Odell
Carla Peters-Carr
Rhonda Peyton
Tamara Polling
Dorothy Rader
Todd Rosenthal
John Staunton
Ana Thomas
Margaret Thomas
Katie Timmons
Jim Wenzel
Debbie Young

Attachment #3

NISPPAC Bylaws

Proposed change to the bylaws:

Industry Spokesperson

The NISPPAC Industry Spokesperson serves as the focal point representative to ISOO on behalf of the industrial base to coordinate collective points of view of the eight member NISPPAC Industry Representative body on national policy implications. The Industry Spokesperson is responsible for representing the NISPPAC Industry Representatives at each NISPPAC meeting, recommends to the NISPPAC Chair the addition or deletion of NISPPAC Working Groups, assignment of an industry lead to all NISPPAC Working Groups, and recommends industry subject matter expertise representation to all NISPPAC Working Groups.

The NISPPAC Industry Spokesperson is selected from within the eight NISPPAC Industry who currently serve on that body and nominated to ISOO for the NISPPAC Chairman's consideration and approval. The Spokesperson is expected to be flexible throughout the year for attendance to impromptu government meetings where industry representation is required. The Spokesperson is also expected to engage with various facets of industry to include those representing professional, trade, and other organizations whose membership is substantially comprised of business within the NISP.

Attachment #4

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

SECURITY EXECUTIVE AGENT POLICY UPDATE

LEADING INTELLIGENCE INTEGRATION

Gary Novotny
Chief, Security Oversight Branch
Special Security Directorate
National Counterintelligence and Security Center

June 6, 2016

What is Continuous Evaluation (CE)?

- A personnel security investigative process to review the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position.
  - Assists in on-going eligibility determinations throughout the period of eligibility.
  - Conducts automated records checks of commercial databases, US Government databases, and other information lawfully available to security officials.
  - Applies standardized business rules based on the 2012 Federal Investigative Standards (FIS).
  - Notifies personnel security officials of adjudicatively relevant information on a more frequent basis than current periodic reinvestigations.

CE Authorities

Executive Order 13467: CE is defined as "reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility."

Executive Order 12968 (as amended by EO 13467): States that any individual who has been determined to be eligible for or who currently has access to classified information shall be subject to continuous evaluation under standards (including, but not limited to, the frequency of such evaluation) as determined by the DNI.

Federal Investigative Standards (Signed by the DNI December 2012): Require that a continuous evaluation program be in place for all individuals cleared to Tier 5 (individuals eligible for access to TS or TS/SCI information, or eligible to hold a sensitive position). Tier 5 implementation is scheduled for September 2016.

Program Implementation Strategy

- Policy and Oversight:
  - Developing policy guidance to inform agencies of CE capability, standards, requirements.

- ODNI Technical Capability:
  - Developing a capability to conduct automated records checks and apply standardized business rules to identify security relevant information.
  - Using data sets to address seven categories/areas of concern based on the federal investigative standards.
  - Building core capability on JWICS (TS/SCI network), but components planned on all security fabrics.
  - Will have capability to process entire Tier 3 and Tier 5 eligible population.

CE Program Milestones

- FY 2015:
  - √ Develop and disseminate Executive Correspondence (EC) on the Implementation of CE - 30 June 2015.
- Summer 2016:
  - Issue an EC on departments and agencies determination of CE Options.
- 60 Days Post EC on CE Options:
  - Departments and agencies required to decide on CE option.
- 30 September 2016:
  - Departments and agencies can begin CE activities.
- 30 September 2017:
  - Each executive branch agency has enrolled at least five percent of its Tier 5 population in the CE process, in compliance with T5 FOC.

CE System (CES) Technical Milestones

- FY 2015:
  - √ Preliminary demonstration capability is available for the CES for automated records checks.
- June 2016:
  - √ Interim Approval To Test CES with live ODNI Data.
- 30 September 2016:
  - – Development is complete for initial capability of CES automated records checks from seven data sources.
- 31 March 2017:
  - – Authorization for CES to operate in production.
- 30 September 2017:
  - – Full compliance, with the CES in production, is reached.

Security Executive Agent Directive – 5 (SEAD 5)

- Collection, Use, and Retention of Publicly Available Social Media Information in Background Investigations and Adjudications.
  - Only publicly available social media information of the individual under investigation will be collected.
  - Absent a National Security concern, or criminal reporting requirements – information pertaining to US citizens other than the individual being investigated will not be pursued.
  - Investigators and adjudicators may not request individuals to:
    - Provide passwords;
    - Log into a private account; or
    - Take any action that would disclose non-publicly available social media information.

For questions, please contact:

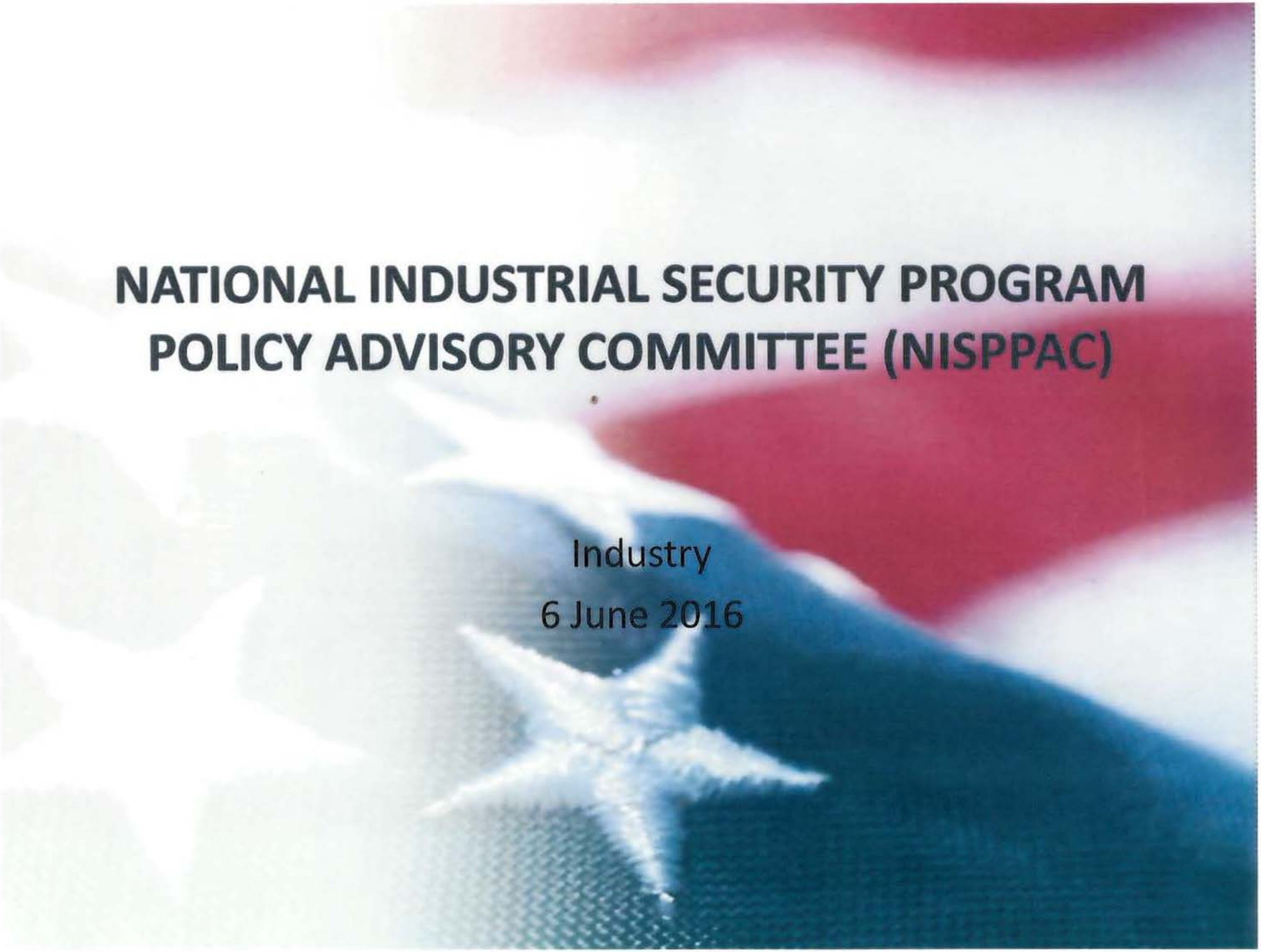
- Gary Novotny

  Chief, Security Oversight Branch
  NCSC/SSD/PSG
  Phone: 301-243-0474
  Email: Garymn@dni.gov

- General Inquiries

  Email: SecEA@dni.gov

Attachment #5



NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

Industry

6 June 2016

Outline

- Current NISPPAC/MOU Membership

- Policy Changes

- Working Groups

National Industrial Security Program

Policy Advisory Committee Industry Members

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

National Industrial Security Program

Industry MOU Members

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

New Business

Department of Commerce and DSS Survey

- Industry is concerned with the scope of this questionnaire and the lack of coordination/discussion to understand the impact it will have on our thinly stretched FSO's and support teams.
  - Industry is not staffed across multiple organizations to collect this data within the 10 hour estimate, nor do we believe that time expenditure is accurate.
  - Industry has already provided the requested data to the USG; via ISFD, ATOs, IATOs, Merger & Acquisition data (10K) and SF 328, Products and Services Category DUNS, Customer list – this is a resubmission of data from Security, Contracts, Finance, Legal, etc...
  - Significant OPSEC issues – internet accessible pdf and compiled data stored? This is a targeting list made simple for our adversaries.
  - This data is good the day it is provided – then it deteriorates the day after submittal
- ISOO, Commerce, DSS & Industry meeting to address concerns.
  - Historical perspective and authority provided on Survey development and dissemination approach.
  - Revised communication plan and approach for collection discusses (Multiple Facility organization).
  - OPSEC and protection levels discussed.
  - Next steps

OPM Data Breach

- IMPACT
  - Significant delays in BI process directly impacting contract performance (SCI/SAP efforts).
  - BI cost increase (40% since 2014).
  - Funding for credit monitoring impacting DSS BI funds causing additional growing backlog on the SF86 submittals. Plan to suspend the PR processing until FY2017.
- National Background Investigations Bureau (NBIB)
  - Federal Investigative Services (FIS) transition to NBIB.
    - What will be the transition plan?
    - Impact to the current lagging investigative process?
- Next Step
  - Planned hire of 400 Investigators in 2016. Slow pace of hiring and training not expected to have impact on growing backlog.
  - NISPPAC involvement to ensure consistent agency actions.
  - Interim policy guidance to address:
    - Interim Clearances and Out of Scope BIs.
    - Failure of PR initiation date in JPAS creating issues with some SAP and IC PSO's & SSO's
    - ODNI Memo to Components (similar to OUSD, Robert Andrews Memo 7/31/2006) indicating eligibilities do not expire. Link to the DSS website.

Security Policy Update

Executive Order #13587

EO # 13587

Structural Reforms to improve security of classified networks

7 OCT 2011

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

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

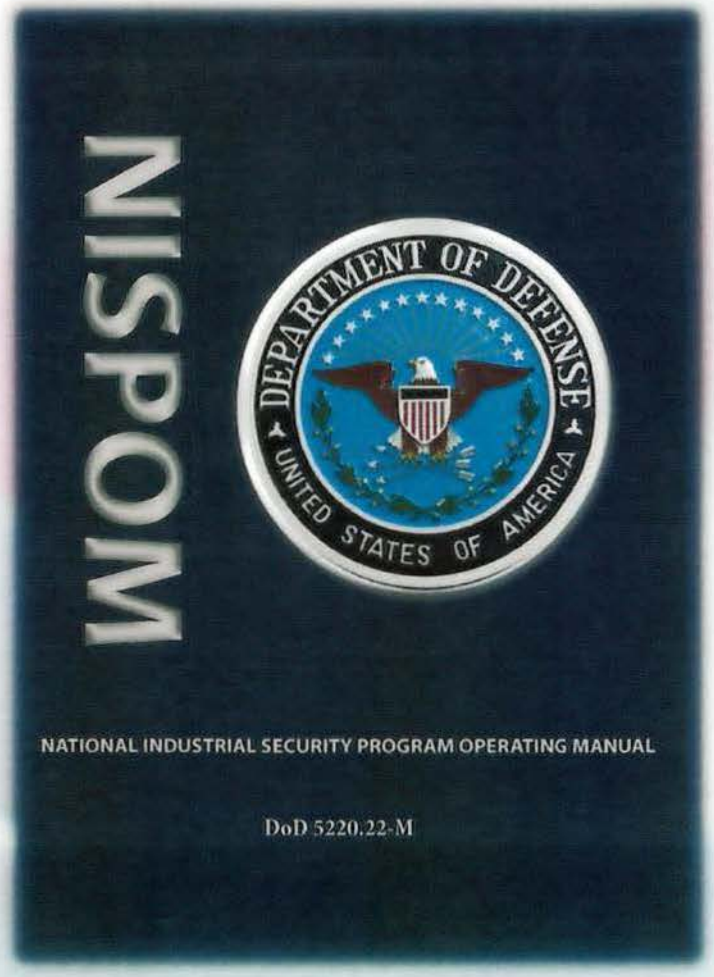
INSIDER THREAT

- Directing structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks
  - Integrating InfoSec, Personnel Security and System Security
- Need consistent requirement across all the User Agencies relating to implementation SOPs.
  - NISPPAC Insider Threat Working Group (ITWG) established.
- NISPOM Conforming Change # 2 has been released and published (May 2016).
  - Limited field level discussions thus far; need to flow down strategic implementation discussions (ITWG) to ensure common expectations.

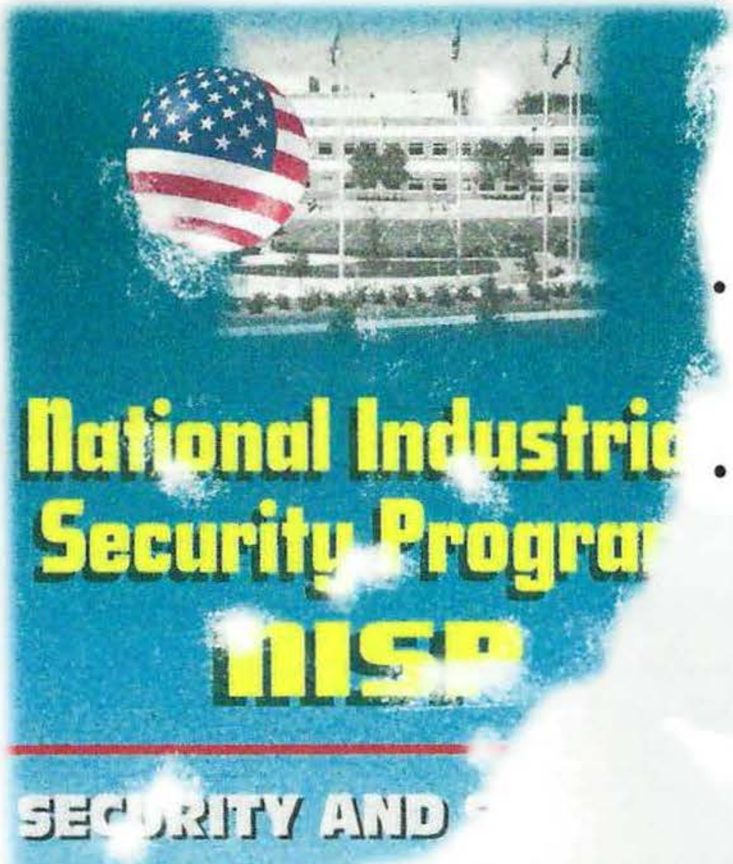
Security Policy Update

Industrial Security Policy Modernization

- National Industrial Security Program Operating Manual revision and update
  - NISPOM Re-Write WG : Gov/Industry team completed review of all buckets. Draft converted to new USG policy format. Next step for CSA's to review updated draft.
  - OUSDI, DSS & Industry collaborated on Insider Threat ISL (published 25 May).
- Department of Defense Special Access Program Manual development
  - Vol 1 (General procedures) Published
  - Vol 2 (Personnel Security) Published
  - Vol 3 (Physical Sec) Published
  - Vol 4 (Classified Info Marking) Published
  - Eliminates JFAN and NISPPOM SAP Supplement upon publication of all the above.
  - AF SAPCO officially rescinds JFAN's
- IMPACT
  - Industry working under a series of interim directions
  - Strong industry coordination for this interim direction is inconsistent
  - Delay of single, integrated policy is leading to differing interpretation of interim direction by user agencies



Policy Integration Issues



- National & world events have stimulated reactions for policy changes and enhanced directives to counter potential vulnerabilities
  - Key areas include Cyber Security, Insider Threat and PERSEC
- Process for directive/policy development and promulgation has become cumbersome and complicated. (Multiple years in most cases)
- Complications and delays have resulted in fractured lower level organization implementing a singular focused plan.
  - Inconsistency among guidance received. Driving increased cost for implementation. Not flowing changes thru contract channels.
  - Need to process tactically 1st before becoming procedural.

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

National Industrial Security Program

Policy Advisory Committee Working Groups

- Personnel Security
  - E-adjudication business rules being aligned with new Federal Investigative Standards. New FIS expected decrease in e-adjudication across the board.
  - DOHA SOR Process. Definitively ID true caseload and aging of those cases. Consider adding WHS representation since DOHA & CAF align under them.
  - Interim Clearance impacts due to FBI Name Check backlog (2 days to 6 wks)
  - Expecting backlog to continue growing based on OPM Breach, new FIS and DSS change to 90 day PR clearance initiation process and funding lag-time
- Automated Information System Certification and Accreditation
  - Working group focus is on incorporating the Risk Management Framework (RMF) into future process manual updates. Early collaboration on this initiative will be key to successful transition. Positive interactions in the multiple meetings.
  - Industry has identified 7 participants (large and small companies) to participate in DSS RMF beta test.
  - Reviewing new DSS Assessment & Authorization Manual (due 16 Jun).
  - Implementation period (6 months) for standalone systems may need to be expanded.

National Industrial Security Program

Policy Advisory Committee Working Groups (cont.)

- Ad-hoc
  - NISP Contractor Classification System (NCCS) – Automated DD254 system
    - What is plan for deployment and account administration?
    - Industry need to plan for training of security, contracts and PM's. Continues to slip.
  - Development of National Industrial Security System (NISS)
    - Participated on the system requirements phase and standing by for further development meetings.
  - Joint Verification System (JVS)
    - Continuing to work functionality issues.
    - Release slipping from Aug to Nov.
    - Looking for training plan for USG and industry. Indication that there will be no formal training for this system. Did not work with JPAS.

Attachment #6

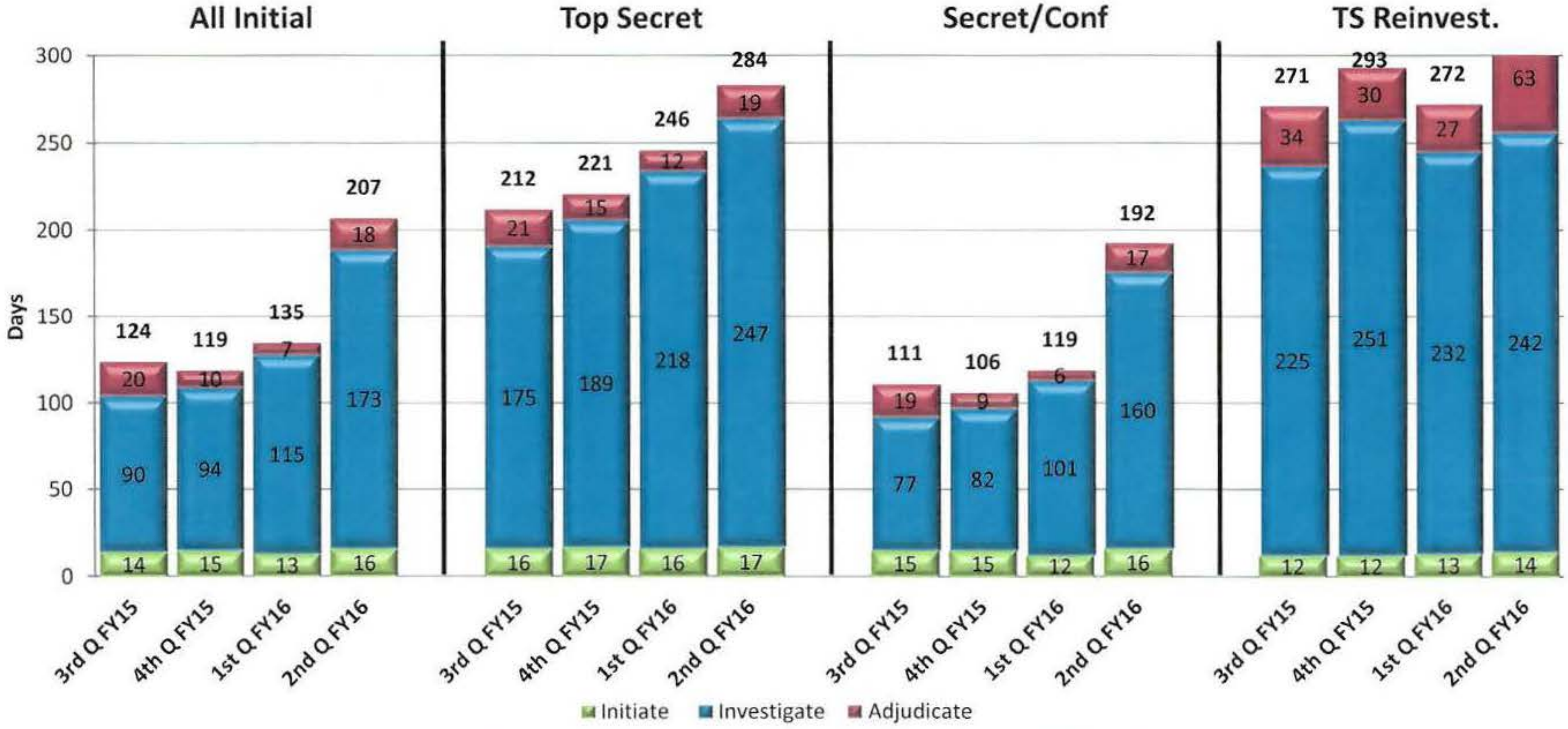
Timeliness Performance Metrics for Submission, Investigation & Adjudication Time

DoD-Industry

May 2016

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

Average Days of Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations
Adjudication actions taken – 3rd Q FY15	20,791	2,906	17,885	7,299
Adjudication actions taken – 4th Q FY15	21,047	2,597	18,450	7,357
Adjudication actions taken – 1st Q FY16	16,262	2,125	14,137	7,459
Adjudication actions taken – 2nd Q FY16	12,809	2,085	10,724	7,300

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

Attachment #7

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

INDUSTRY PERFORMANCE METRICS

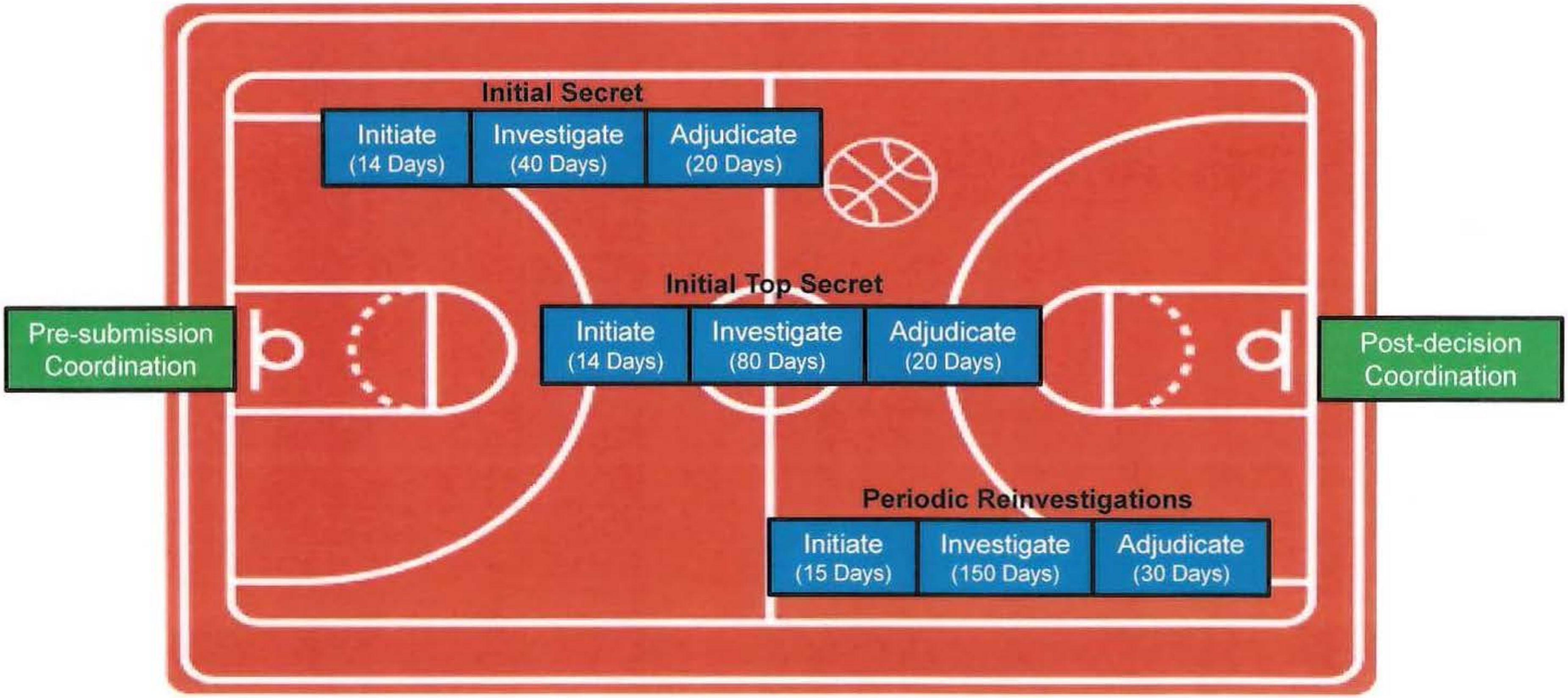
LEADING INTELLIGENCE INTEGRATION

Gary Novotny

Chief, Security Oversight Branch
Special Security Directorate
National Counterintelligence and Security Center

June 6, 2016

Performance Accountability Council (PAC) Security Clearance Methodology



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

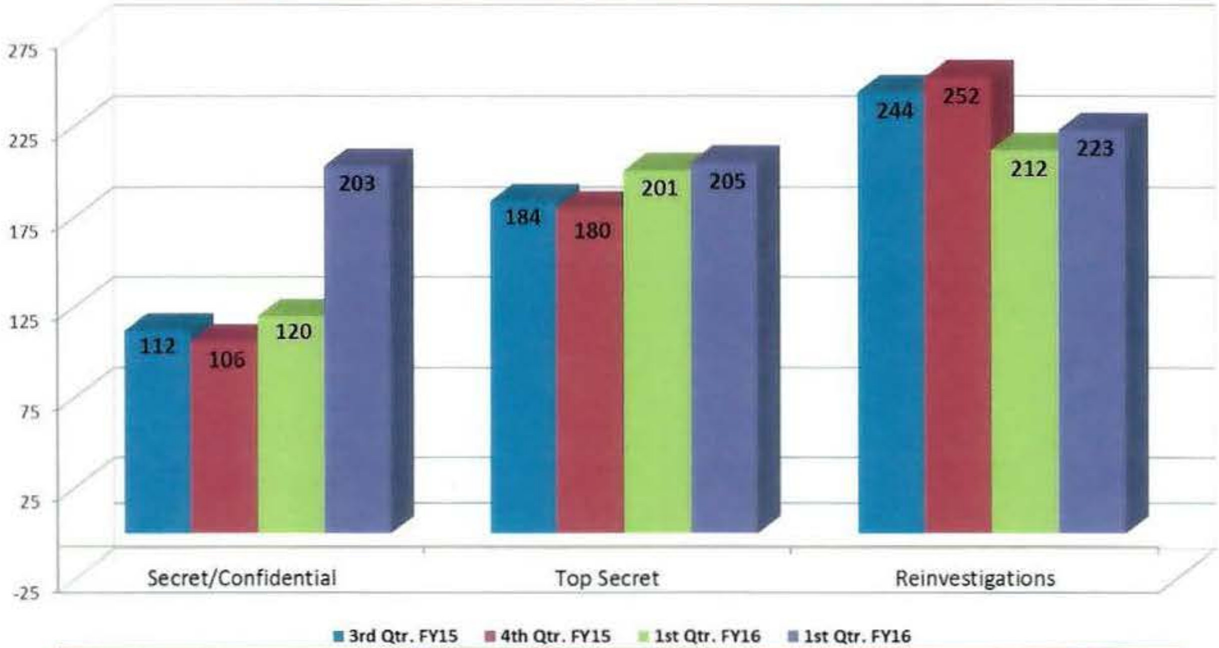
Initiate (15 Days) | Investigate (150 Days) | Adjudicate (30 Days)

Post-decision Coordination

Timeliness Performance Metrics for IC and DSS Industry

Industry Personnel Submission, Investigation and Adjudication* Time

Average Days of Fastest 90% of Reported Clearance Decisions Made

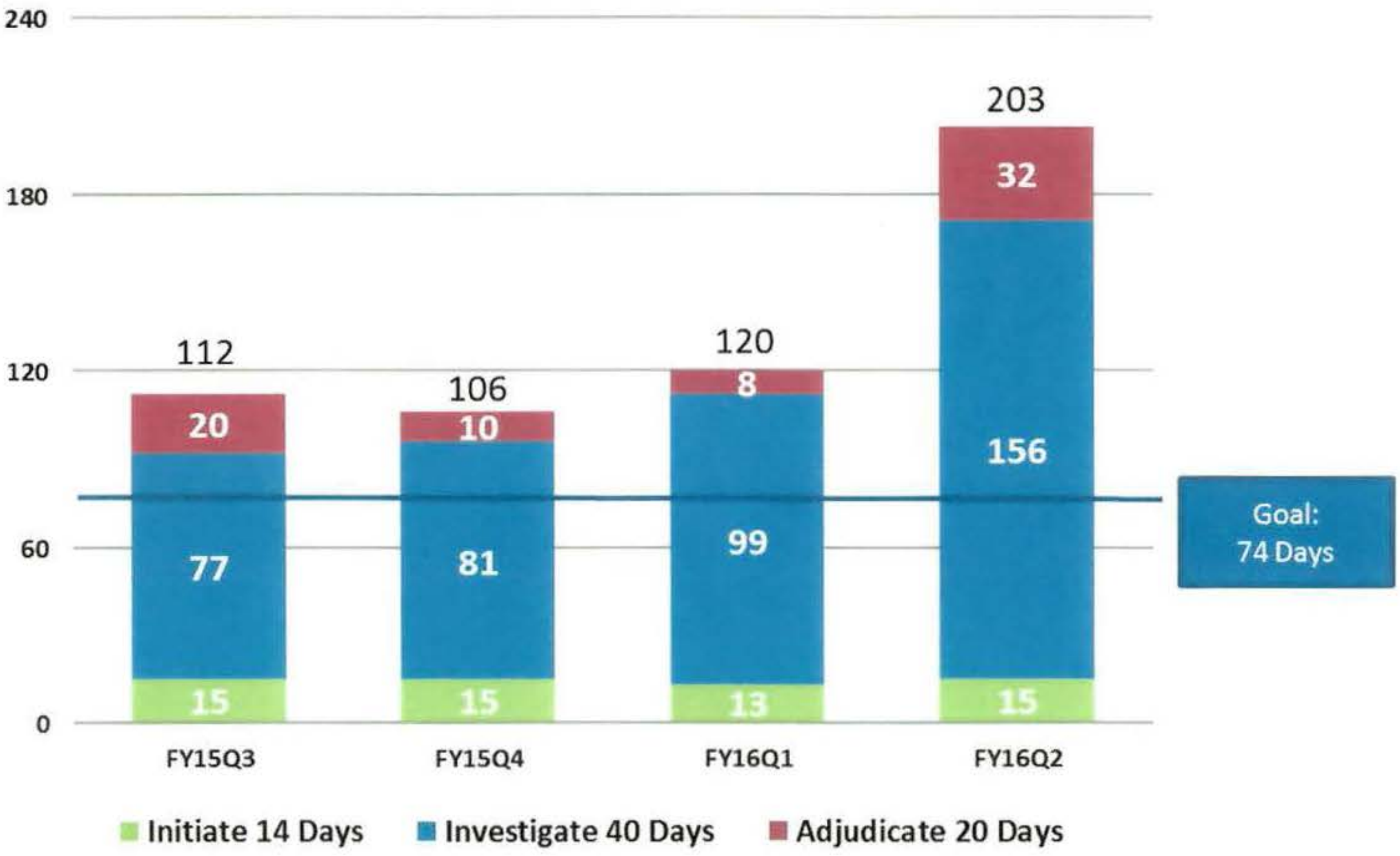


	Secret/ Confidential	Top Secret	Periodic Reinvestigations
Adjudication actions taken – 3rd Qtr. FY15	20,165	4,473	8,827
Adjudication actions taken – 4th Qtr. FY15	19,007	4,436	10,519
Adjudication actions taken – 1st Qtr. FY15	14,776	3,624	12,315
Adjudication actions taken – 2nd Qtr. FY16	11,340	4,176	14,110

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

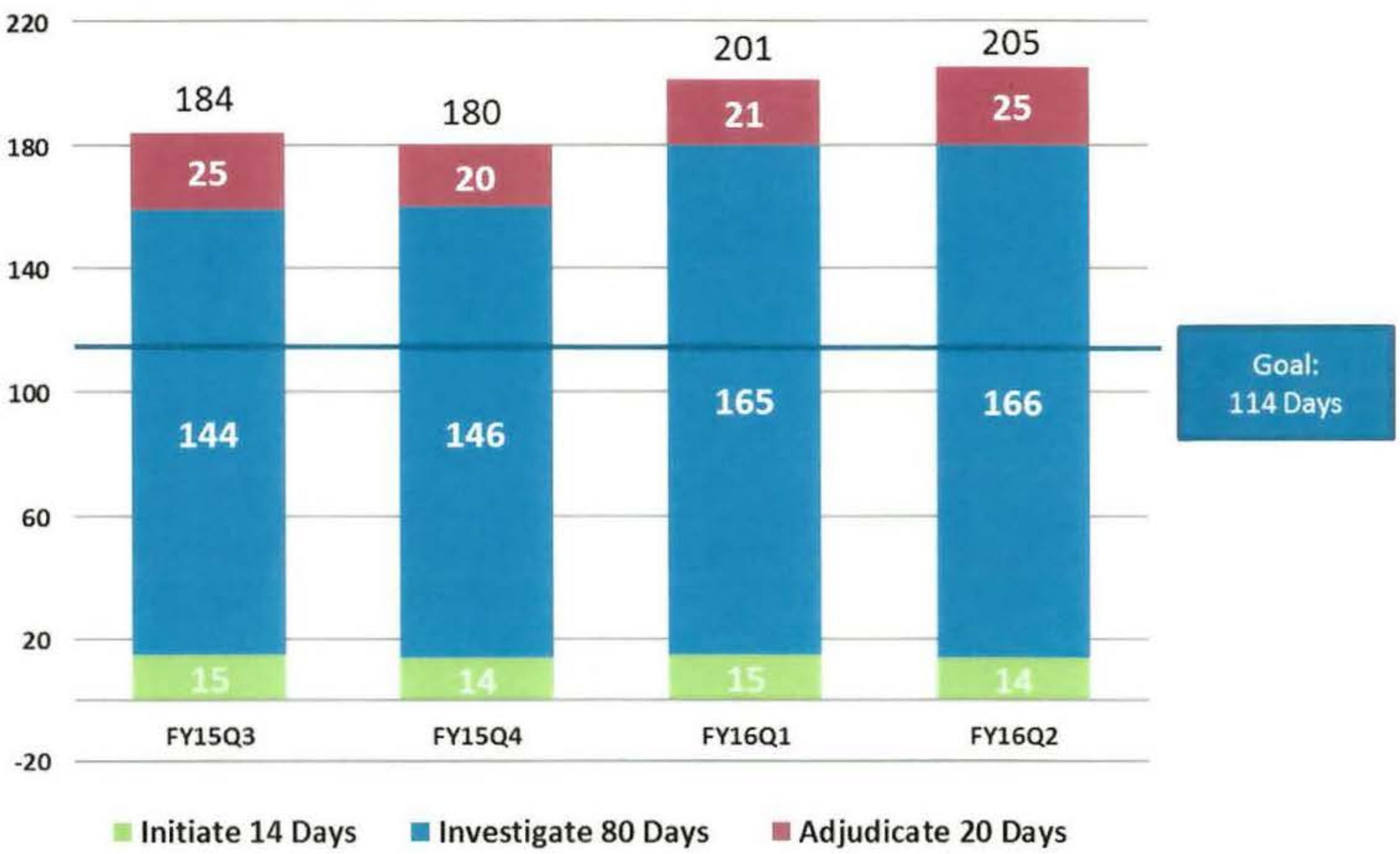
IC and DoD Industry – Secret Clearances

Average Days of Fastest 90% of Reported Clearance Decisions Made



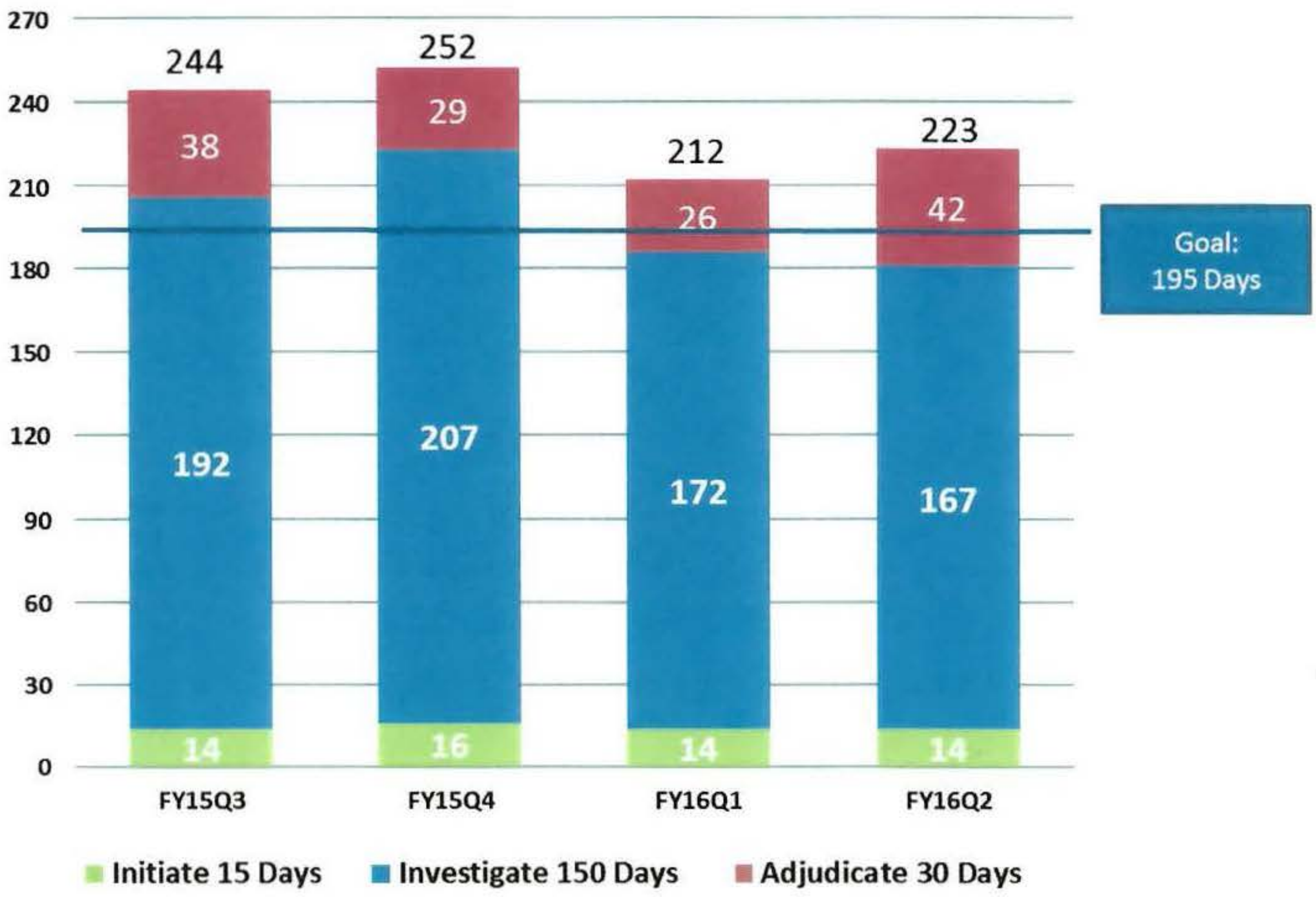
IC and DoD Industry - Top Secret Clearances

Average Days of Fastest 90% of Reported Clearance Decisions Made



IC and DoD Industry - Periodic Reinvestigations

Average Days of Fastest 90% of Reported Clearance Decisions Made



Questions?

Gary Novotny
NCSC/SSD/PSG
Chief, Security Oversight Branch
Phone: 301-243-0474
Email: GARYMN@dni.gov

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

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

Attachment #8

Department of Defense Consolidated Adjudications Facility

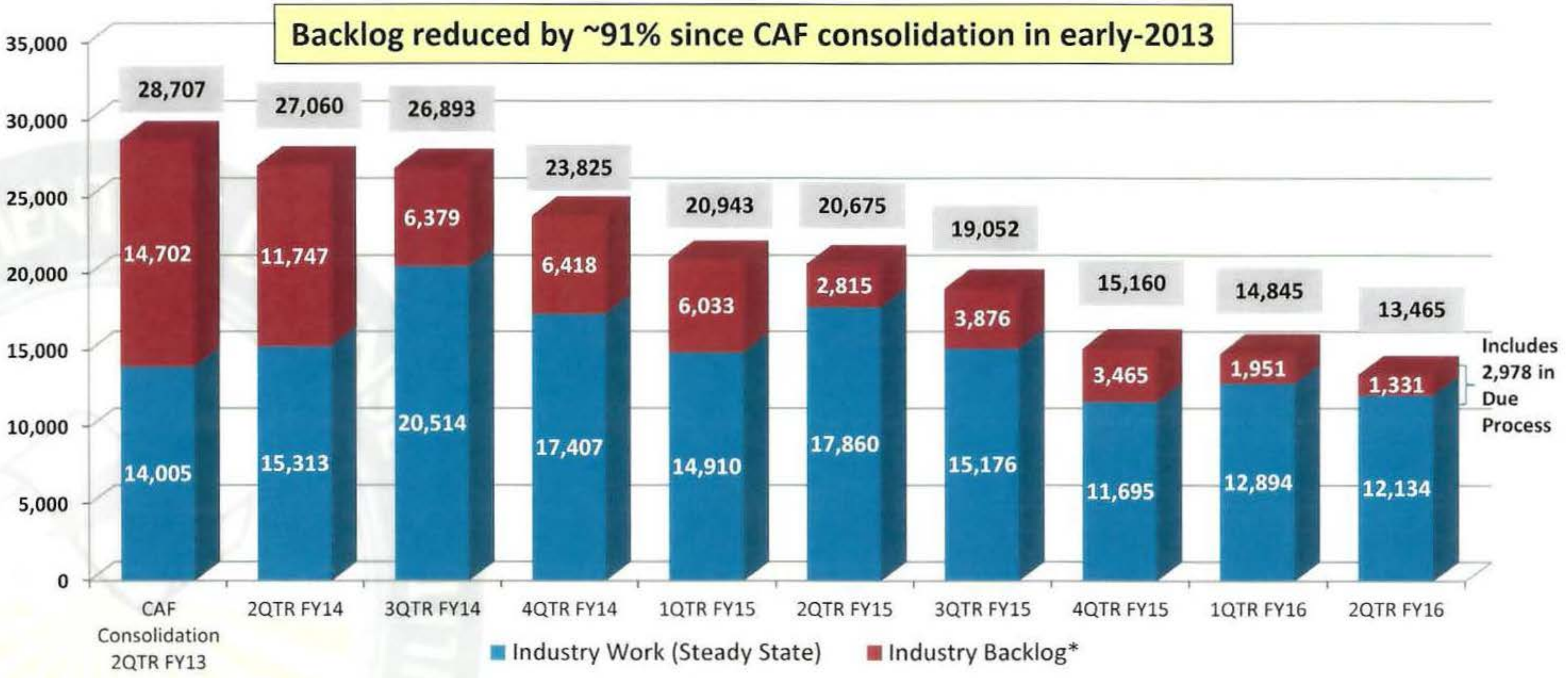
JUNE 2016

NISPPAC WORKING GROUP

Industrial Cases Pending Adjudication

Includes cases Undergoing Legal Sufficiency Review (LSR) at DOHA

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



•Backlog to be eliminated not earlier than late-FY16
•Potential Complications Remain:

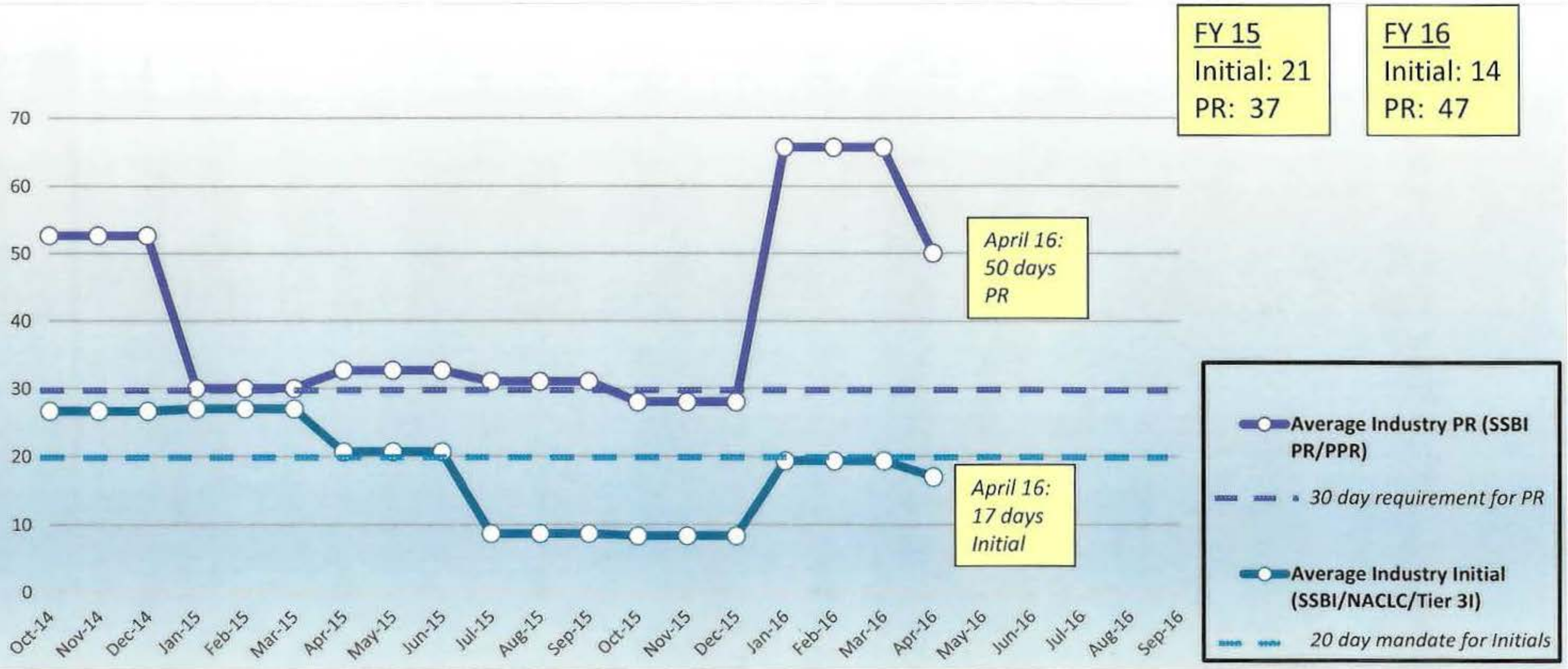
+ CATs v4 Deployment to reduce production by ~20% (Jun 16 – Jan 17)
+ Full impact of CE implementation not yet realized
+ FY16-18 – New FIS increase of workload and reduction of e-Adjudication
+ Loss of e-Adj. in FY16 resulted in an increase of ~3,100 (+3%) for Industry

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

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

As of: 05/31/2016

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



FY 15
Initial: 21
PR: 37

FY 16
Initial: 14
PR: 47

April 16: 50 days PR

April 16: 17 days Initial

- **FY 15 - Both NISP and non-NISP timeliness metrics fluctuated as backlogs were addressed**
- **FY 16 - Timelines to remain more stable, and within IRTPA mandates, as last vestiges of "old"(backlog) cases are closed**
- **Increase in Initial and PR timeliness in 2nd and 3rd Qtrs (FY 16) due to an emphasis on closing backlogged & suspense cases (e.g. 23%-27% of the PRs and initials closed since February 2016 are "old"/backlog cases)**

DoD CAF
Bldg. 600, 10th Street, FGGM

QUESTIONS???

Attachment #9

Defense Security Service

C&A Working Group Update

June 2016

Working Group Initiatives

- Risk Management Framework Pilot

- Assessment and Authorization Process Manual Review

- Supporting Documentation
  - Template and Job Aids Review
  - RMF Transition Guidance