11/10/2009

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

SUMMARY MINUTES OF THE MEETING

The NISPPAC held its 33rd meeting on Wednesday, July 22, 2009, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, N.W., Washington, D.C. William J. Bosanko, Director, Information Security Oversight Office (ISOO) chaired the meeting. The meeting was open to the public. The following minutes were finalized and certified on 19 October 2009.

The following members/observers were present:

- William J. Bosanko (Chair)
- Daniel McGarvey (Department of the Air Force)
- Lisa Gearhart (Department of the Army)
- George Ladner (Central Intelligence Agency)
- Stephen Lewis (Department of Defense)
- Gina Otto (Office of the Director of National Intelligence)
- Richard Donovan (Department of Energy)
- Anna Harrison (Department of Justice)
- Jeffery Moon (National Security Agency)
- Sean Carney (Department of the Navy)
- Kimberly Baugher (Department of State)
- Richard Lee Engel (Industry)
- Sheri Escobar (Industry)
- Douglas Hudson (Industry)
- Vincent Jarvie (Industry)
- Scott Conway (Industry)
- Marshall Sanders (Industry)
- Chris Beals (Industry)
- Darlene Fenton (Nuclear Regulatory Commission)
- Richard Lawhorn (Defense Security Service)
- Steven Peyton (National Aeronautics & Space Administration)
- Deborah Smith (Office of Personnel Management) – Observer

I. Welcome, Introductions, and Administrative Matters

William J. Bosanko, Director, ISOO and NISPPAC Chair, greeted the membership and called the meeting to order at 10:00 a.m. The Chair informed the members that the minutes from the April 7, 2009, meeting had been finalized and certified on July 16, 2009 and are posted at http://www.archives.gov/isoo/oversight-groups/nisppac/committee.html on the ISOO website.

The Chair announced that the President released a memo in May, regarding the review of Controlled Unclassified Information (CUI) policy and procedures and Executive Order 12958, as amended, "Classified National Security Information," (the Order). Both efforts have a 90-day suspense. The CUI effort is led by the Department of Homeland Security and the Department of Justice. The respective task force leads have been meeting for about six weeks with stakeholders and Industry and are now at the point of preparing their final reports. The Chair stated that ISOO and the National Security Council (NSC) had been holding interagency meetings regarding the review of the Order. The Chair informed the membership that at the next meeting of the NISPPAC in October he would invite Bill Leary from the NSC to provide a more detailed overview of the changes.

II. Old Business

The Chair requested that Greg Pannoni, ISOO, review the action items from the last meeting. Mr. Pannoni stated that updates from the three NISPPAC working groups—Personnel Security Clearances (PCL), Foreign Ownership, Control or Influence (FOCI), and Certification and Accreditation of Information Systems (C&A)—would be provided during the presentations.

ACTION: The Chair requested that the PCL Working Group address, at the next working group meeting, Industry's current capabilities, as well as any other options available that would help address the issue of supporting small industrial facilities with the introduction of the new SWFT technology.

Mr. Pannoni stated that the PCL update would include a status report on the Secure Web Fingerprint Transmission (SWFT) program.

ACTION: Members of the NISPPAC are to provide formal responses with regard to the proposed changes to the Directive within 30 days.

Industry will provide a draft definition of "organization" within 30 days.

Per the Chair, following the next meeting of the FOCI Working Group, the issues involving FOCI will be reevaluated at a later date.

Mr. Pannoni stated that the FOCI working group update would include a briefing on the draft policy language for National Interest Determinations (NID) and the material-change matrix. Industry also submitted a draft definition of "organization" that is under coordination.

ACTION: The ODAA will provide a metrics update at the next meeting of the NISPPAC.

Mr. Pannoni stated that this action item would be provided as a part of the C&A Working Group Report.

ACTION: The NISPPAC members are to review the proposed amendments to the bylaws and provide formal comments within 30 days. Following Article 9 of the bylaws, a vote to approve the proposed bylaws will occur at the next meeting of the NISPPAC.

Mr. Pannoni stated that the NISPPAC Bylaws were reviewed and updated and are now compliant with the Federal Advisory Committee Act (FACA) requirements. The Chair thanked Mr. Pannoni for his update. The Chair moved discussion to the NISPPAC Bylaws.

The Chair stated that the revisions to the bylaws were required to update standard operating procedures and to address FACA requirements. The Chair stated that the bylaws were disseminated to the membership and comments had been accepted to correct two grammatical errors. The Chair stated that there were no substantive changes to the bylaws and motioned for a vote. A vote was taken, and with no opposition, the NISPPAC Bylaws were amended. The revised bylaws will be posted to the ISOO website.

ACTION: The Chair stated that there were no substantive changes to the bylaws and motioned for a vote. A vote was taken and with no opposition, the NISPPAC Bylaws were amended. The revised bylaws will be posted to the ISOO website.

The Chair moved discussion to updates on the NISPPAC Working Groups. The Chair stated that the FOCI Working Group would suspend operations as its main initiative has been completed and is in final coordination. The PCL and the C&A Working Groups would continue to meet based on significant activity within the Executive branch, particularly to bring classified national security systems under a unified set of standards. This will be a major topic at the October meeting.

ACTION: The Chair stated that the FOCI Working Group would suspend operations as its main initiative has been completed and is in final coordination. The PCL and the C&A Working Groups would continue to meet based on significant activity within the Executive branch, particularly to bring classified national security systems under a unified set of standards.

III. Working Group Updates

A) PCL Working Group Report

The PCL Working Group provided updates regarding investigation metrics, the Case Adjudication Track System (CATS), and SWFT. These updates were provided by Deborah Smith, Office of Personnel Management (OPM), Vera Denison, Defense Security Service (DSS), Janice Condo, Department of Defense (DoD), and Richard Mansfield, DSS, respectively.[1]

Ms. Smith and Ms. Denison provided the PCL metrics update. Ms. Smith reported that the metrics in her presentation represented the adjudicative decisions as reported by DSS to OPM for the third quarter of fiscal year (FY) 2009. Ms. Smith stated that investigations for initial Top Secret and all Secret and Confidential clearances totaled 30,260 and averaged 106 days. Ms. Smith also stated that the end-to-end completion time for the fastest 90 percent of these investigations was 77 days, down from last quarter’s 93 days and the first quarter’s 97 days. Ms. Smith stated the fastest 90 percent of investigations for initial Top Secret were completed in 107 days and for initial and reinvestigations for Secret and Confidential, clearances were 69 days, down from 84 days last quarter. Ms. Smith stated that the 5,965 Top Secret periodic reinvestigations averaged 163 days, and the fastest 90 percent were 121 days, down from 125 days from the last quarter.

Ms. Smith also stated that DoD, through the DSS Defense Industrial Security Clearance Office (DISCO), makes all the adjudicative decisions for Industry investigations at the collateral level. Sensitive Compartmented Information (SCI) adjudications are made by

[1] See appendix 1 for Ms. Smith’s presentation. See appendix 2 for Ms. Denison’s presentation. See appendix 3 for Mr. Mansfield’s presentation.

other DoD entities. Ms. Smith provided the month-to-month, end-to-end timeliness for the fastest 90 percent of initial investigations for Top Secret, and the initial and reinvestigations for Secret and Confidential clearances. The data for the last three months were 80 days for April, 73 days for May, and 78 days for June. Ms. Smith provided investigation-only time for the same cases; these were 45 days for April, 41 days for May, and 43 days for June. Ms. Smith also stated that OPM's calculations show an additional 10 days for mailing time of the investigations to DISCO. Ms. Smith stated that this additional time was due to having to mail hard-copy investigation packets as opposed to submitting them electronically.

Ms. Smith provided end-to-end timeliness data for the fastest 90 percent of initial Top Secret investigations; these were 111 days for April, 103 days for May, and 106 days for June. Ms. Smith provided this data for Secret and Confidential initial and reinvestigations; these were 71 days for April, 66 days for May, and 70 days for June. Finally, for Top Secret periodic reinvestigations, the end-to-end timeline for the fastest 90 percent were 116 days for April, 122 days for May, and 127 days for June.

Vincent Jarvie, Industry, asked if OPM saw a reduction in clearance actions because of a real or perceived downturn in the Aerospace and Defense Industry. Ms. Smith responded that there was actually a 10 percent increase in the number of investigations. Mr. Jarvie requested a metric for investigation initiations from Industry to provide an accurate measurement of the improvement of the PCL process. Ms. Smith agreed to build a specific trend line covering request for clearance receipts from Industry and provide the data at the next NISPPAC meeting. The Chair then introduced Ms. Denison for her metrics update.

Ms. Denison presented an update on the adjudication inventory of DISCO that showed an overall reduction rate of 55 percent between the 1st quarter of FY 09 and May 09. Ms. Denison stated that DISCO's inventory has been reduced by nine percent since April. Ms. Denison stated that the inventory of cases at OPM had also seen a one percent reduction for Industry cases. Ms. Denison stated that the adjudicative timeliness would be further reduced once completed OPM investigations were received electronically. Ms. Denison stated that DISCO's adjudication timeliness for Top Secret periodic reinvestigations for the last three months were 11 days for April, 13 days for May, and 15 days for June.

Ms. Denison provided the third quarter rejection rates for initial and periodic reinvestigation requests, which was 13 percent, with DISCO's rejections at 7.6 percent and OPM's at 5.4 percent. Ms. Denison stated that the majority of rejections at OPM are due to fingerprints either not being received or not being paired with the Electronic Questionnaires for Investigation Processing (e-QIP) within a 30-day timeframe. Ms. Denison discussed tips for investigation submissions to make the process more efficient and stated that the tips are posted on the OPM e-QIP website. Ms. Denison noted that a disproportionate number of rejections were from smaller facilities.

Ms. Denison concluded her presentation by summarizing actual FY 09 industry clearance submissions versus projections. Ms. Denison noted that at the end of May 2009, Industry clearance submissions were two percent below overall DSS and Industry projections. The Chair thanked both Ms. Smith and Ms. Denison and moved discussion to Ms. Condo for her CATS presentation.

Ms. Condo stated that CATS, which was developed by DoD, allows for electronic case receipt from OPM and an electronic adjudication and screening function. Ms. Condo stated that CATS would initially be piloted by DISCO by the end of July 2009. Ms. Condo also stated it is projected that CATS will reduce case receipt time to about one day.

Mr. Jarvie raised two questions: first, how would Industry receive notification of denial, revocation or granting of a clearance, and second, will CATS have the capacity to determine if any other investigations are open and submitted through CATS, as is currently available in the Joint Personnel Adjudication System (JPAS). Ms. Condo and Ms. Denison responded to the first question, indicating that the notification would be entered into JPAS and CATS. Addressing the second question, they stated that CATS only handles adjudications and would not change anything available in JPAS. The Chair thanked Ms. Condo and moved discussion to Mr. Mansfield's presentation.

Mr. Mansfield presented on the status SWFT, an electronic system to assist fingerprint processing for investigations submitted through DSS and sent to OPM for processing by the Federal Bureau of Investigation (FBI). Mr. Mansfield stated that SWFT was transitioning pilot participants into the production system with the goal of bringing in new Industry partners by August 3, 2009. Mr. Mansfield stated that his office forwarded a SWFT survey to Industry to gauge interest in SWFT implementation. Mr. Mansfield stated that 777 surveys were sent to the 401 companies that submitted 75 percent of the Personnel Security Investigation's in FY 08. Company responses were as follows: 140 responded that they wanted to participate in SWFT; 121 had not decided whether to participate; 42 did not want to participate; and 98 did not respond.

Sheri Escobar, Industry, asked if there were data on the number of small businesses responding that they would not implement SWFT. Mr. Mansfield stated that this information was not captured in the survey. Douglas Hudson, Industry, asked whether government sponsors where requiring additional standards for fingerprint technology systems. Mr. Mansfield responded that authorized systems were on the FBI approved list for vendor solutions. Mr. Mansfield also stated that it was Industry's responsibility for procuring and implementing their systems. While DSS will provide configuration guidance, it will be the company's responsibility to provide technical support.

Mr. Mansfield also explained how DSS is planning to streamline the registration process. The DSS call center will create account managers for the SWFT system, and the DSS system access form has been updated to reflect SWFT. Mr. Mansfield explained that there is a test print cycle of transferring fingerprints to OPM before going "live" in the SWFT system. Mr. Mansfield stated that other helpdesk resources and a mailbox were created by DSS to assist in the SWFT process and that the management of SWFT would eventually transfer from DSS to the Defense Manpower Data Center. Mr. Mansfield concluded his presentation by providing resource information to begin using the SWFT system. The Chair, thanked Mr. Mansfield and yielded time for questions.

Ms. Escobar asked about the SWIFT phase-in process. Mr. Mansfield stated that if a business is ready to implement, DSS and SWFT is ready to support it. Richard Lee Engel, Industry, asked where the approved list for systems was located. Mr. Mansfield stated it was on the FBI website for approved vendor solutions. Mr. Jarvie stated that the usage of SWFT would increase later in the next FY rather than in October because of fiscal budgeting concerns. Mr. Jarvie also raised concerns over the cost/benefit outcome of implementing the SWFT system. Mr. Mansfield stated that DSS has received positive feedback from pilot participants. Mr. Pannoni stated that 80 percent of case rejections from OPM were a result of fingerprint cards not corresponding to e-QIP investigation submissions. Marshall Sanders, Industry, asked if other Industry members could solicit information on the cost and benefit of SWFT implementation.

B) Foreign Ownership, Control, or Influence (FOCI) Working Group Report
Mr. Pannoni provided a report on the Working Group's progress.[2] He stated that the FOCI Working Group met once since the previous NISPPAC meeting. Mr. Pannoni provided a slide that outlines the changes to the NISP Implementing Directive that pertain to National Interest Determinations (NIDs). He stated that changes included language to ensure that NIDs were consistent with national security interests and to clarify NID requirements for pre-contract activity, new contracts, and existing contracts. Mr. Pannoni also stated that the NID language provided a timeline for decisions and follow-up. Mr. Pannoni yielded to questions.

Mr. Engel commented that he foresees significant improvements once the new NID language and updates are approved. Mr. Pannoni expressed that this was the impetus for establishing the FOCI Working Group in order to monitor and track the process of FOCI adjudications and provide direction for processing NIDs. Mr. Pannoni then yielded to Stephen Lewis, DoD, for an update on the material-change matrix.

Mr. Lewis provided an update to the material-change matrix, advising that it had been coordinated within the FOCI Working Group for comment on what needed to be included into an Industrial Security Letter (ISL). Mr. Lewis stated that he had received feedback and approval and was in the process of incorporating the information into the ISL. The Chair thanked Mr. Lewis and moved discussion to the C&A Working Group Report.

C) Certification and Accreditation Working Group Report
Mike Farley, DSS, provided a report on the Working Group's progress.[3] Mr. Farley reported that DSS is averaging 40 days to issue an Authority to Operate/Interim Authority to Operate an information system to process classified information. Mr. Farley stated it is currently taking DSS an average of 16 days to review system security plans (SSPs). Scott Conway, Industry, asked why the metrics reflected an upward timeline trend. Mr. Farley responded that the trend was a result of different DSS regions and areas taking different times.
Mr. Conway asked if the rejections of SSPs were included in the metrics. Mr. Farley stated that rejected system plans were not included and the metrics were based upon accepted SSPs.

Mr. Jarvie asked where significant discrepancies were occurring and whether they were at small or large businesses. Mr. Farley responded that significant discrepancies are being found at both small and large businesses. Mr. Jarvie stated that Industry should be contacted when a significant discrepancy occurs so that DSS does not have time taken away from accrediting other systems. Mr. Farley discussed examples of the most common discrepancies

[2] See appendix 4 for Mr. Pannoni's presentation.
[3] See appendix 5 for Mr. Farley's presentation.

submitted in the packages and stated that the SSPs needed to be completed accurately to avoid discrepancies.

IV. New Business

A) Security Operations Curriculum Development

Teresa Shoup-Stirlen and Jay Chambers, Office of the Director of National Intelligence, Special Security Center (SSC) and Mitch Lawrence, Industrial Security Working Group (ISWG) provided a presentation on this topic.[4] Ms. Shoup-Stirlen provided a detailed overview of the curriculum and collaboration program to attract and retain the best people in the intelligence community. A DNI security education council was created to develop concepts and requirements for Government and Industry. Ms. Shoup-Stirlen also highlighted cooperative efforts among the SSC, DoD, and other Federal agencies to bring investigators, adjudicators, and program security specialists into both the formal program and its certification program.

Mr. Chambers expressed that the combined vision of the SSC and the ISWG was the creation of a dedicated baccalaureate degree program. Mr. Chambers stated that there was no in-residence course for security management in academia that handled security the way the government does. Mr. Chambers stated that the curriculum was not training but education on principles and application. Mr. Chambers presented specific curriculum requirements.

Mr. Lawrence indicated that industry would support the security professional curriculum program. Mr. Lawrence stated that the program would give credibility to the security profession in Government and Industry, provide a “supply chain” of educated professionals, and ensure the continuity of the security profession. Mr. Lawrence also provided an overview of the ISWG and stated that although it is oriented toward the SCI community the impact and benefits to others associated with the NISPPAC were vast. Mr. Lawrence stated that a college curriculum would allow someone to choose Information Security as a career path.

B) Combined Industry Presentation

Mr. Jarvie provided the Industry combined presentation.[5] Mr. Jarvie presented the upcoming NISPPAC Industry membership expirations. He provided Industry comments on each NISPPAC Working Group Report and asked Mr. Lewis for clarification on ISL 2009-02, regarding pre-employment and FOCI mitigation. Mr. Lewis stated that for pre-employment security clearance eligibilities there is acceptable flexibility with regard to the needs of an interim clearance and a final determination. With regard to FOCI mitigation, Mr. Lewis stated that the company needs to have in place a suitable plan and agreement regarding what the company would do if it were acquired by or came under the control of a foreign interest. Mr. Lewis stated that a FOCI mitigation agreement had to be in place before the close of the transaction.

Next, Mr. Jarvie commented on the National Industrial Security Program Operating Manual (NISPOM) and asked Mr. Lewis when the proposed changes to the NISPOM would be made

[4] See appendix 6 for Ms. Shoup-Stirlen’s, Mr. Chamber’s, and Mr. Lawerence’s presentation.

[5] See appendix 7 for Mr. Jarvie’s presentation.

available for Industry to provide feedback and comments. Mr. Lewis stated that Government members were working on a draft of proposed changes. Once the Government entities consolidate their views, Industry would be given 60 days to provide comment. Mr. Jarvie outlined the top four Industry concerns: sharing of threat information, CUI, FOCI, and PCL processing. Mr. Jarvie spoke about strides being made addressing the four Industry concerns, and stressed the importance of providing threat information to Industry through the information-sharing environment. The Chair thanked Mr. Jarvie for his update.

C) NISP Signatories Update

No updates were reported.

V. Open Forum

Ms. Escobar raised a concern about the role of small business entities and expressed that there is a need for additional focus on small companies, suggesting that through education and training small companies could be more informed of program requirements.

Mr. Lawrence brought up the issue of Industry involvement with the NISPOM revision and concern that Industry was being added on at the end of the revision process.

ACTION: ISOO will host a meeting with Industry to provide the opportunity for Industry to make recommendations for changes to the NISPOM.

Kimberly Baugher, Department of State, suggested that larger companies should get involved in assisting smaller companies. The Chair responded that he would work on a small business solution.

ACTION: Kimberly Baugher, Department of State mentioned that larger companies should get involved in assisting smaller companies. The Chair responded that he would work on a small business solution.

VI. Closing Remarks and Adjournment

The Chair reminded the NISPPAC that the next full meeting would be October 8, 2009. The Chair adjourned the meeting at 11:57 p.m.

<u>Summary of Action Items:</u>

A) **The Chair stated that there were no substantive changes to the bylaws and motioned for a vote. A vote was taken, and with no opposition, the NISPPAC bylaws were amended. The revised bylaws will be posted to the ISOO website.**

B) **The Chair stated that the FOCI Working Group would suspend operations as its main initiative has been completed and is in final coordination. The PCL and the C&A Working Groups would continue to meet based on significant activity within**

the Executive branch, particularly to bring classified national security systems under a unified set of standards.

C) ISOO will host a meeting with Industry to provide the opportunity for Industry to make recommendations for changes to the NISPOM.

D) Kimberly Baugher, Department of State suggested that larger companies should get involved in assisting smaller companies. The Chair responded that he would work on a small business solution.

List of Appendices

Appendix 1 – Ms. Smith’s PCL Working Group Presentation
Appendix 2 – Ms. Denison’s PCL Working Group Presentation
Appendix 3 – Mr. Mansfield’s PCL Working Group Presentation
Appendix 4 - Mr. Pannoni’s FOCI Working Group Presentation
Appendix 5 - Mr. Farley’s Certification and Accreditation Working Group Presentation
Appendix 6 - Ms. Shoup-Stirlen, Mr. Chambers, and Mr. Lawrence’s Security Operations Curriculum Development Presentation
Appendix 7 - Mr. Jarvie’s Combined Industry Presentation

Appendix 1
Ms. Smith’s PCL Working Group Presentation

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

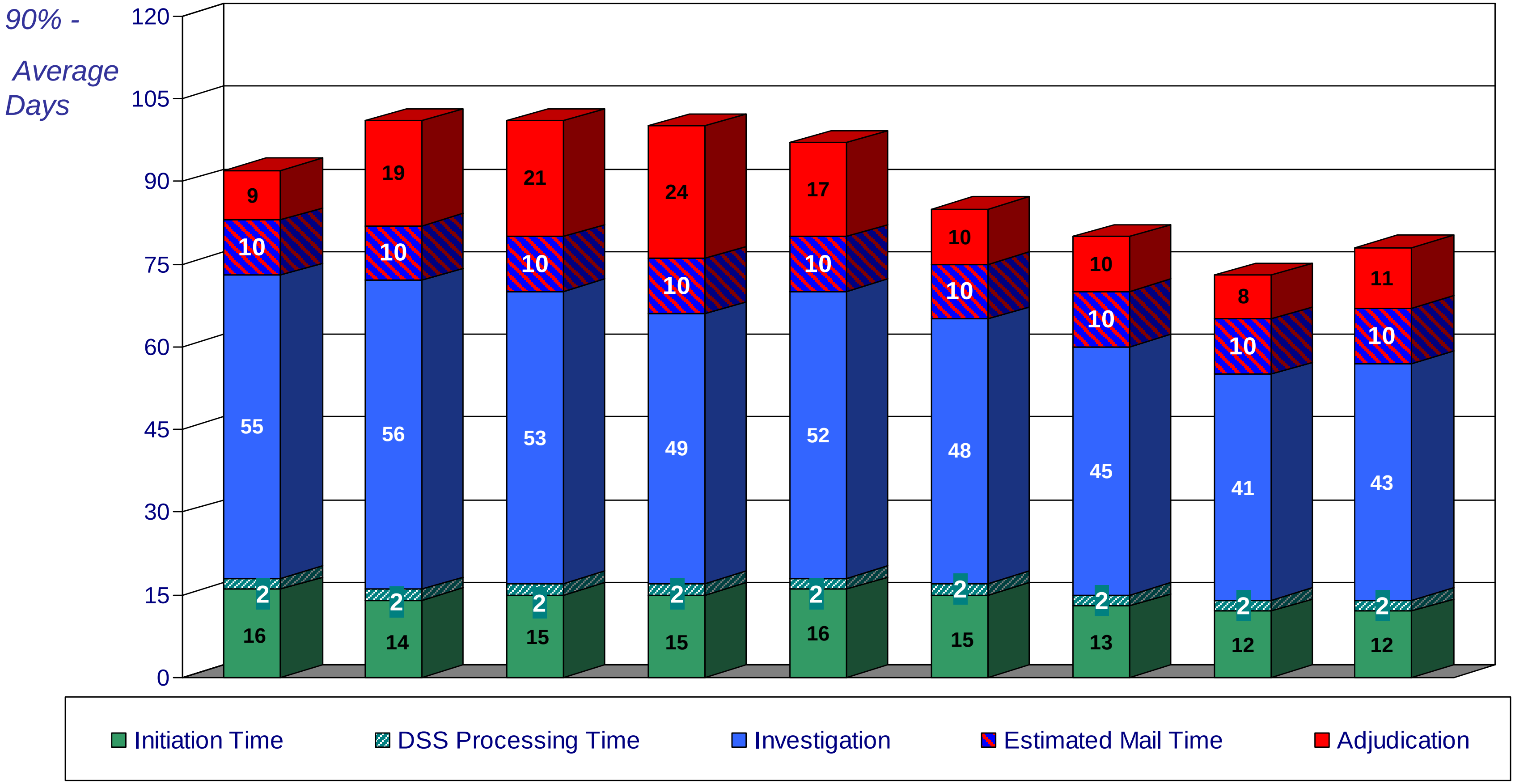
Reported Clearance Decisions Made During the 3rd Qtr FY 09

- Top Secret Initials & All Secret/Conf – All 30,260 cases: 106 day average cycle time
    - Fastest 80% cases: 70 day average
    - Fastest 90% cases: 77 days
        - TS Initial – All 6,564 cases: 134 day average cycle time
            - Fastest 80% cases: 100 day average
            - Fastest 90% cases: 107 days
        - All Secret/Conf – All 23,696 cases: 98 day average cycle time
            - Fastest 80% cases: 62 day average
            - Fastest 90% cases: 69 days
- TS PR – All 5,965 cases: 163 day average cycle time
    - Fastest 80% cases: 111 day average
    - Fastest 90% cases: 121 days

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

Data reflective of reported adjudicative decisions as of July 9, 2009

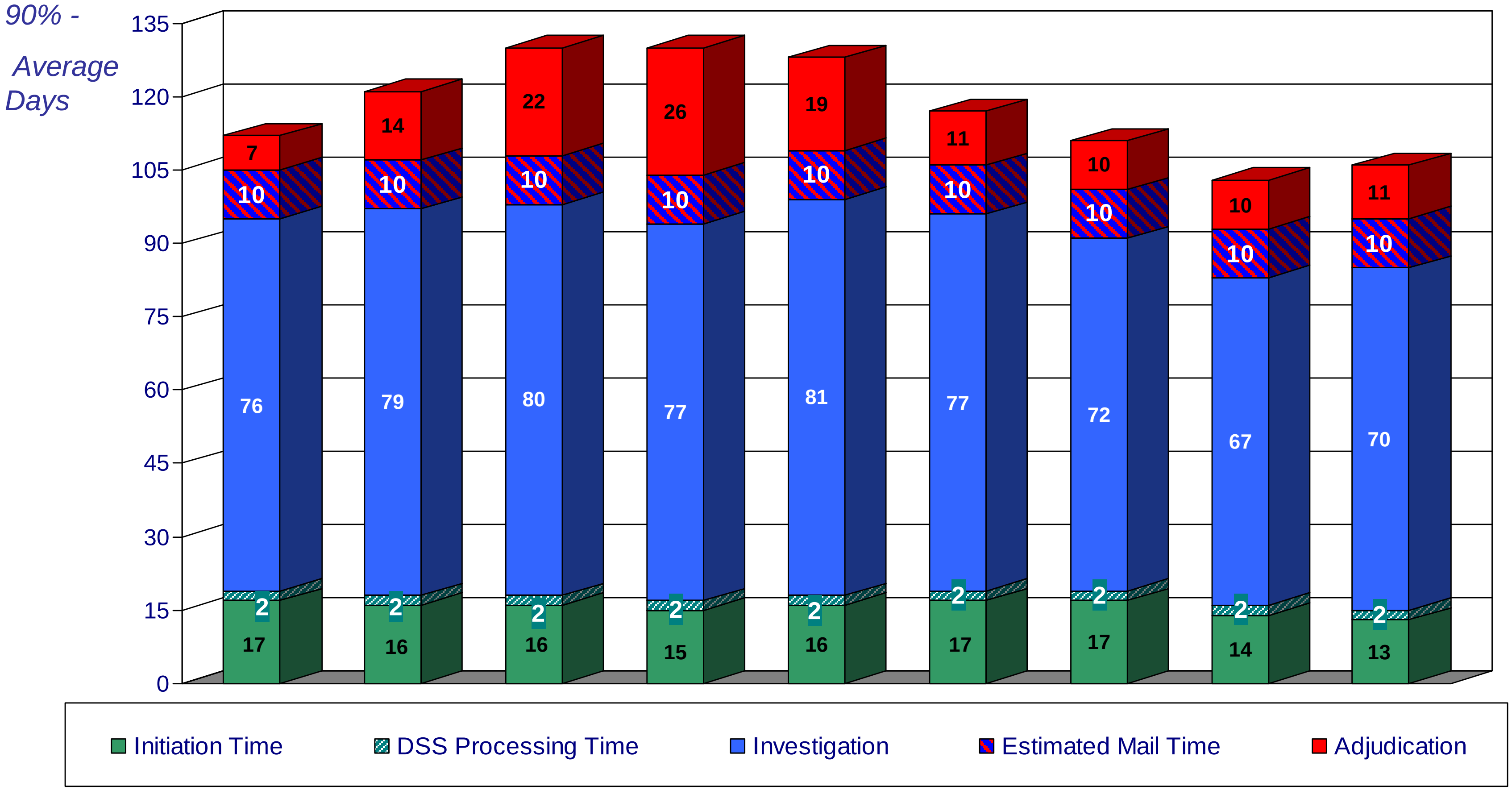
Industry's Average Timeliness Trends for 90%
Initial Top Secret and All Secret/Confidential Security Clearance Decisions



Adjudications actions taken:	Oct 08	Nov 08	Dec 08	Jan 09	Feb 09	Mar 09	Apr 09	May 09	Jun 09
100% of Reported Adjudications:	11,868	6,741	9,208	10,318	9,875	12,957	10,577	10,059	9,470
Average Days for the first 90%	92 days	101 days	101 days	100 days	97 days	85 days	80 days	73 days	78 days

Slide has been updated with reported adjudicative decisions made during March 09 through June 09. Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested. The time span for the rejections is not included in the above metrics.

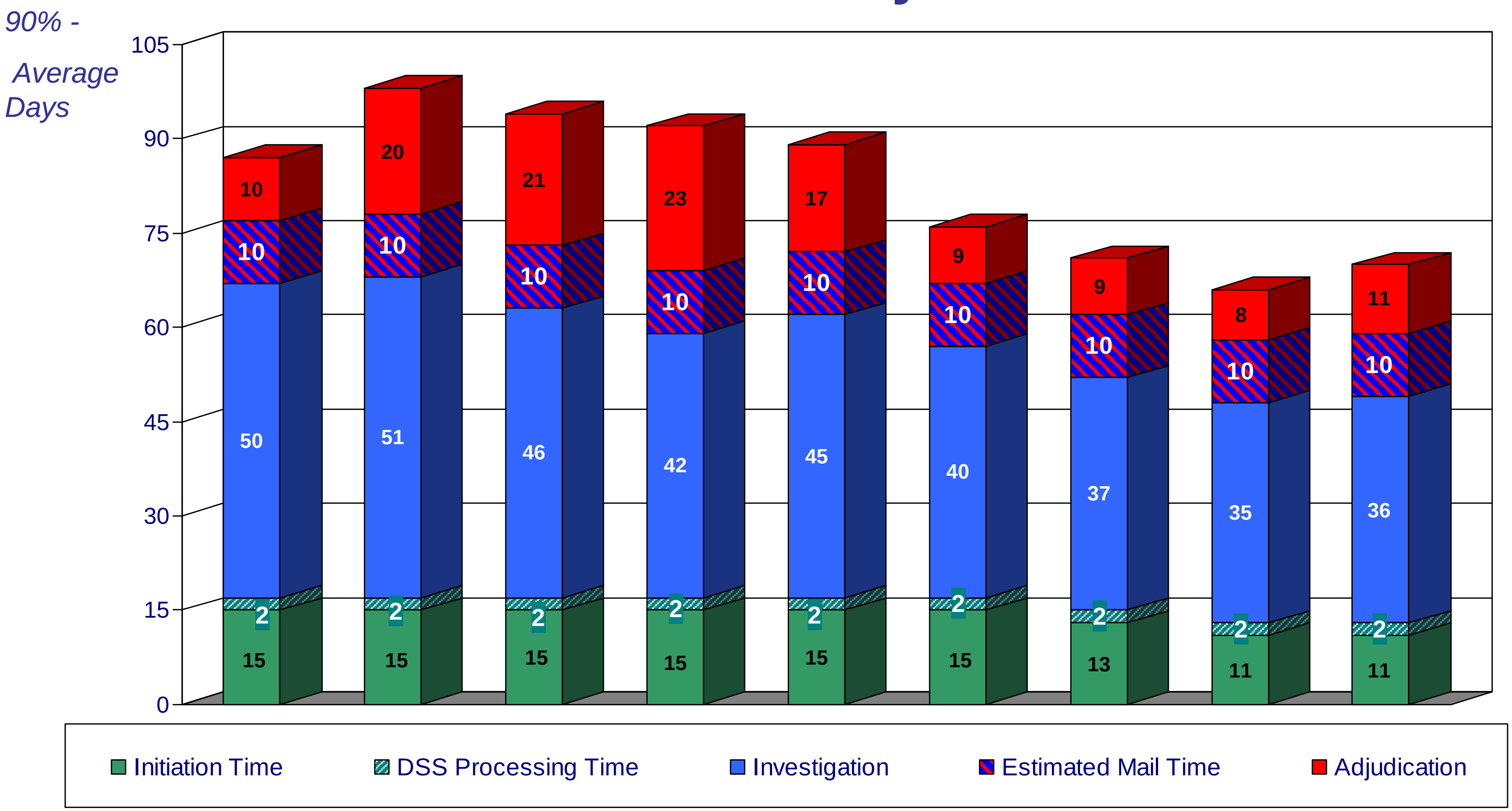
Industry's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions



Adjudications actions taken:	Oct 08	Nov 08	Dec 08	Jan 09	Feb 09	Mar 09	Apr 09	May 09	Jun 09
100% of Reported Adjudications:	2,450	1,086	1,778	2,231	2,134	3,092	2,409	2,136	1,998
Average Days for the first 90%	112 days	121 days	130 days	130 days	128 days	117 days	111 days	103 days	106 days

Slide has been updated with reported adjudicative decisions made during March 09 through June 09. Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested. The time span for the rejections is not included in the above metrics.

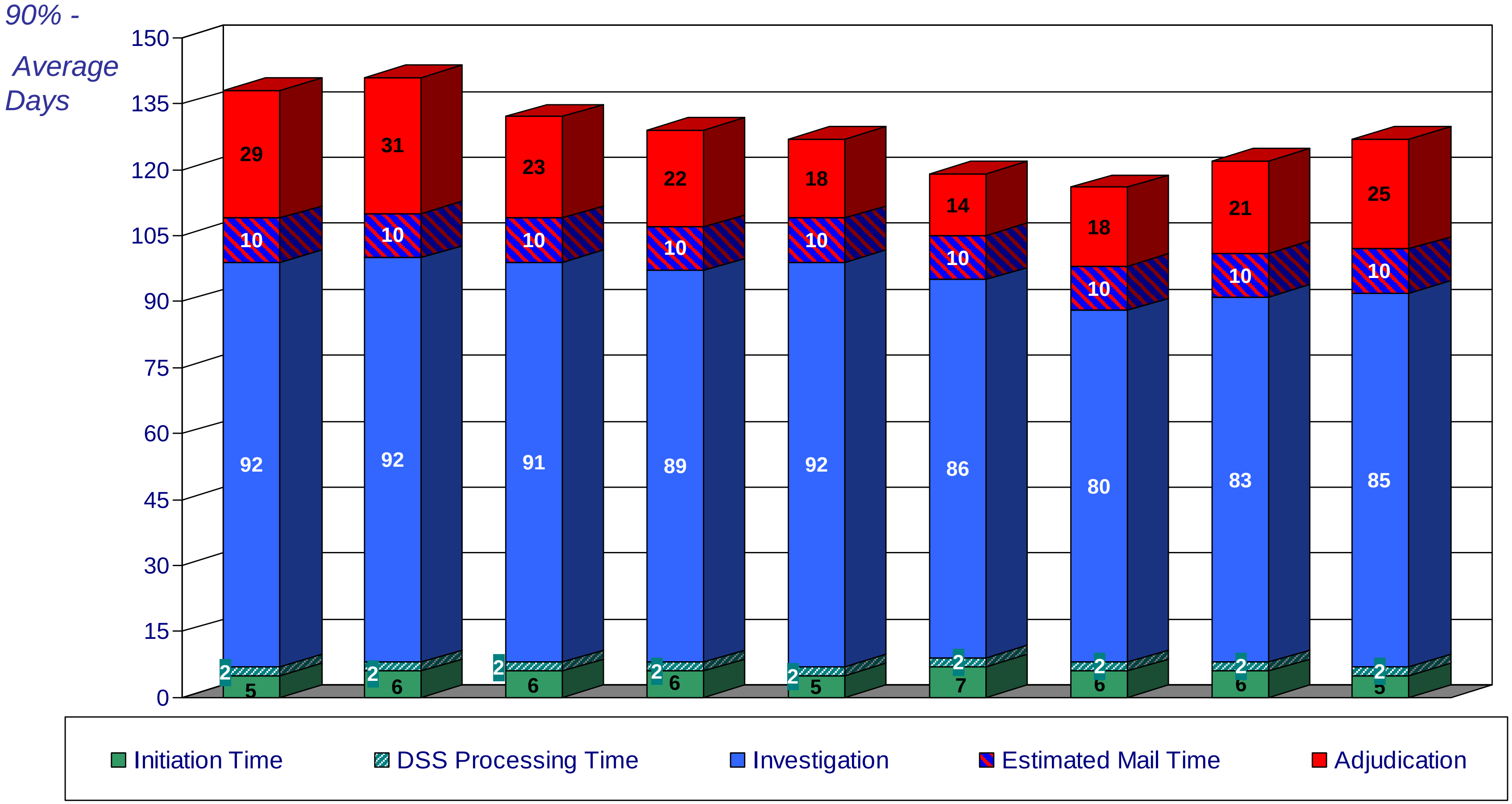
Industry’s Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions



Adjudications actions taken:	Oct 08	Nov 08	Dec 08	Jan 09	Feb 09	Mar 09	Apr 09	May 09	Jun 09
100% of Reported Adjudications as of July 9,’2009:	9,418	5,655	7,430	8,087	7,741	9,865	8,168	7,923	7,472
Average Days for the first 90%	87 days	98 days	94 days	92 days	89 days	76 days	71 days	66 days	70 days

Slide has been updated with reported adjudicative decisions made during March 09 through June 09. Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested. The time span for the rejections is not included in the above metrics.

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



Adjudications actions taken:	Oct 08	Nov 08	Dec 08	Jan 09	Feb 09	Mar 09	Apr 09	May 09	Jun 09
100% of Reported Adjudications as of July 9,2009:	4,471	2,252	3,116	3,408	3,070	3,729	2,210	1,891	1,812
Average Days for the first 90%	138 days	141 days	132 days	129 days	127 days	119 days	116 days	122 days	127 days

Slide has been updated with reported adjudicative decisions made during March 09 through June 09. Adjudication time includes any additional investigation required for adjudication that exceeds the scope of the original investigation requested. The time span for the rejections is not included in the above metrics.

Appendix 2
Ms. Denison’s PCL Working Group Presentation

DISCO

FY09 ADJUDICATION INVENTORY

CASE TYPE	FY 08				FY 09			FY09 Delta Q1FY09 vs May 09
	Q1	Q2	Q3	Q4	Q1	Q2	May	
NACLC	11,449	488	240	1,953	4,721	1,815	2,711	-43%
SSBI	9,337	5,625	30	354	1,448	634	826	-43%
SBPR	4,899	3,752	5,973	757	974	340	269	-72%
Phased PR	8,945	4,923	4,210	330	1,690	495	178	-89%
TOTAL PENDING	**34,630**	**14,788**	**10,453**	**3,394**	**8,833**	**3,284**	**3,984**	**-55%**

Overall reduction of 55% for NACLC, SSBI, SBPR and Phased PR case types from 1Q FY09 to May 09.

Source: DISCO Manual Counts

INDUSTRY CASES AT OPM

FY09 INVESTIGATION INVENTORY

CASE TYPE	FY 08				FY 09			FY09 Delta Q1FY09 vs May 09
	Q1	Q2	Q3	Q4	Q1	Q2	May	
NACLC	29,575	25,085	22,077	15,561	13,209	13,982	13,708	4%
SSBI	14,110	8,796	7,404	6,720	6,626	6,687	6,894	4%
SSBI-PR	11,761	9,943	5,639	4,167	3,772	4,160	5,127	36%
Phased PR	7,711	7,749	6,734	6,408	5,430	2,771	2,216	-59%
TOTAL PENDING	**63,157**	**51,573**	**41,854**	**32,856**	**29,037**	**27,600**	**27,945**	-4%

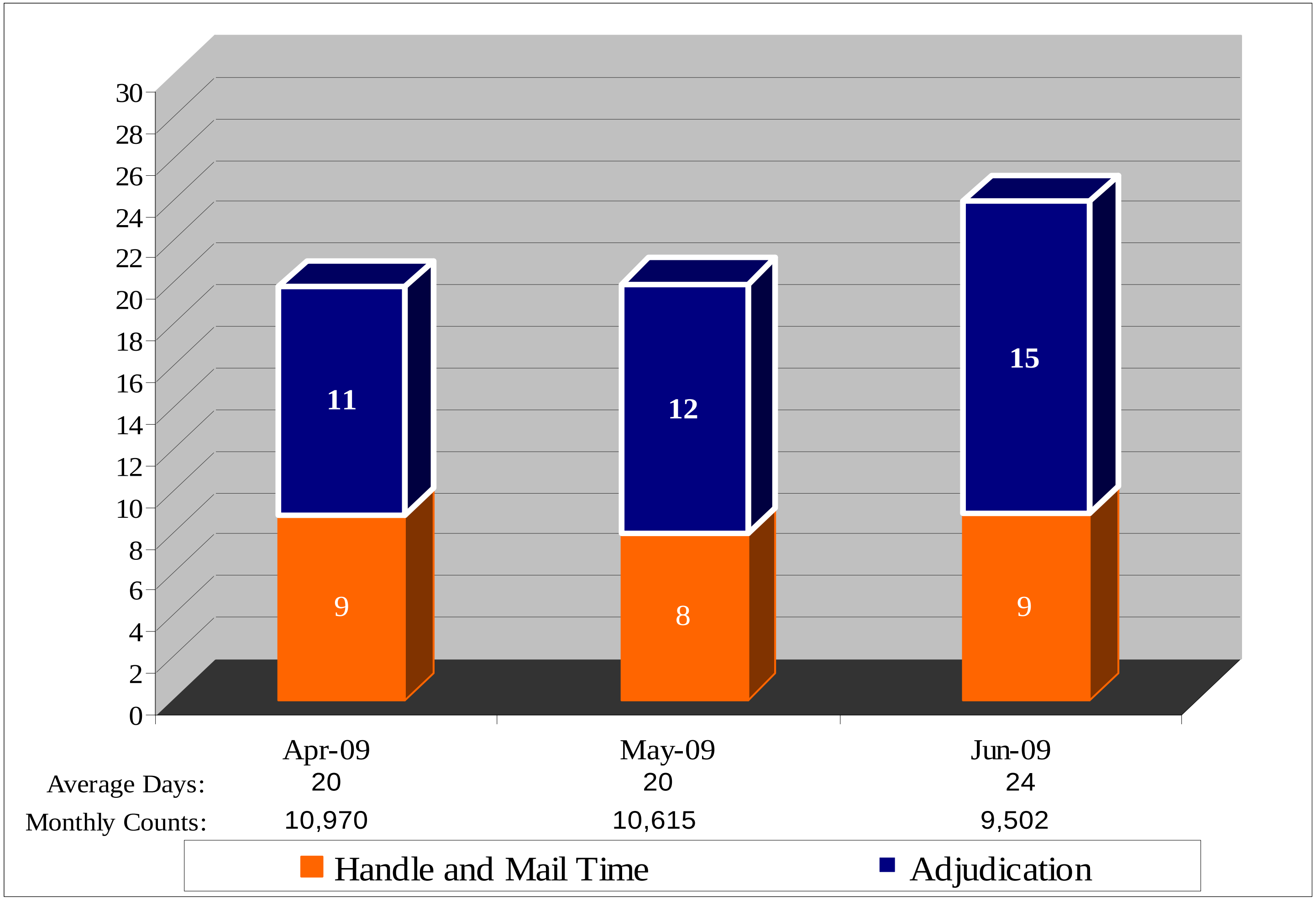
Overall reduction of 4% for NACLC, SSBI, SBPR and Phased PR case types from Q1 FY09 to May 09.

Source: OPM Customer Support Group

DISCO

Collateral* Adjudication Timeliness (90%)

All Initial Clearances (SSBI / NACLC / ANACI)



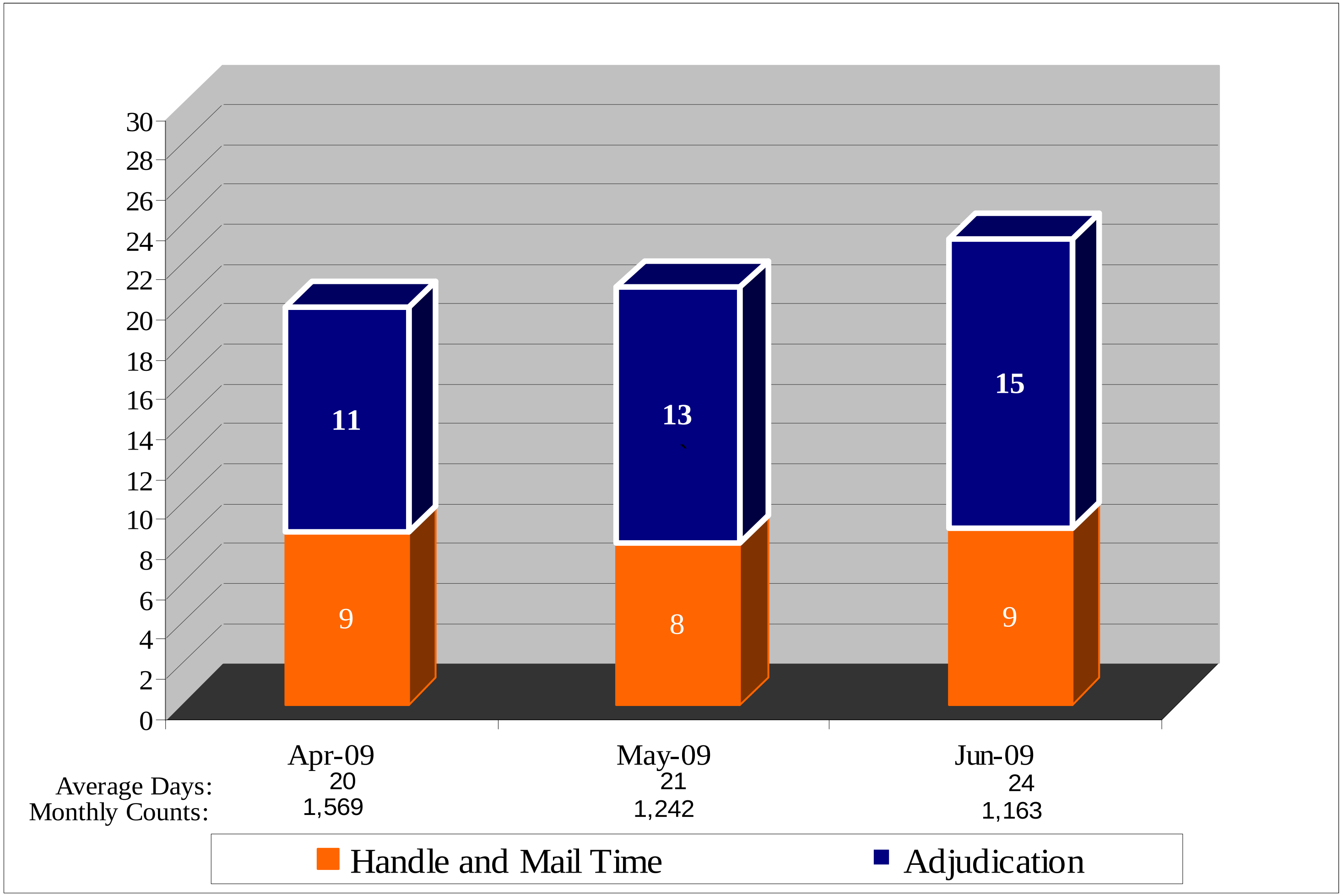
	Apr-09	May-09	Jun-09
Average Days:	20	20	24
Monthly Counts:	10,970	10,615	9,502

*Excludes SCI Adjudications

DISCO

Collateral* Adjudication Timeliness (90%)

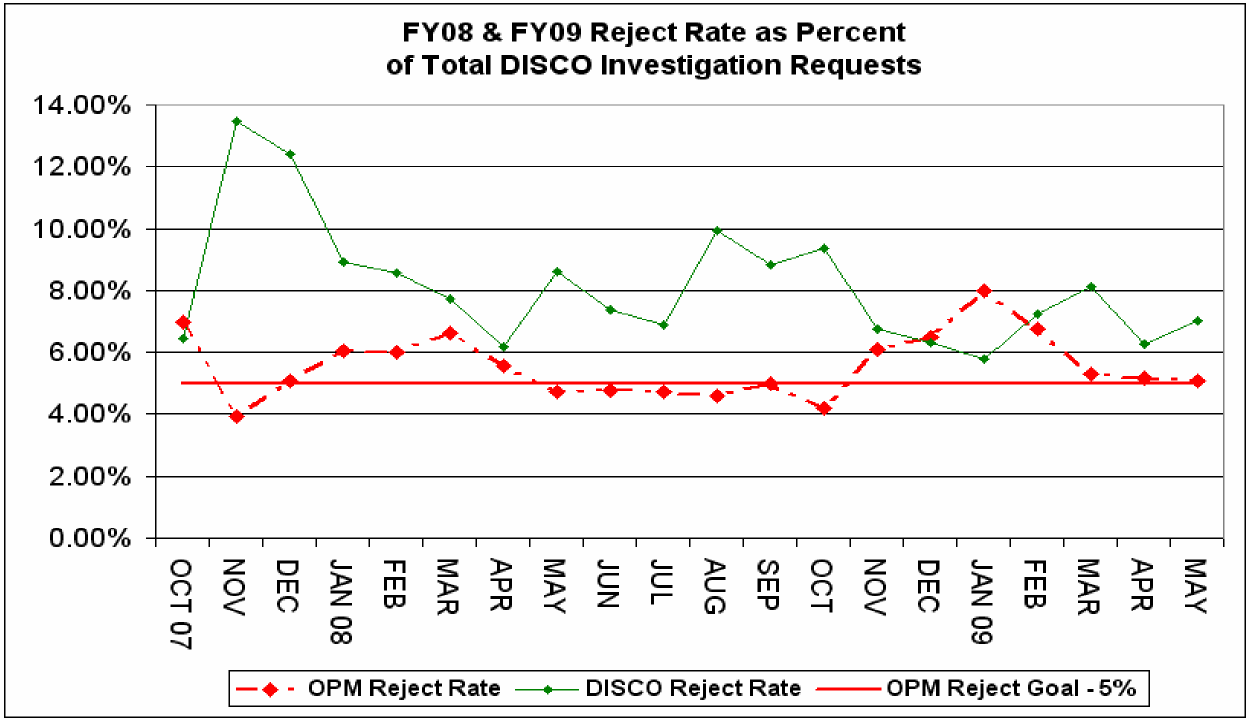
Top Secret Periodic Reinvestigations (PPR / SSBI-PR)



*Excludes SCI Adjudications

QUARTERLY REJECT RATES

(Initial & Periodic Reinvestigation Requests)



- **FY09 (As of May 31): DISCO received 120,921 investigation requests**
  - **Rejects -** Total of **15,727 (13.0%)** of incoming investigation requests rejected back to FSOs
    - DISCO rejected **9,230 (7.6%)** investigation requests to FSOs for re-submittal
    - OPM rejected **6,497 (5.4%)** investigation requests to DISCO (then to FSOs) for re-submittal
- **Note – Case rejection and re-submittal time is not reflected in timeliness.**
    - When a case is re-submitted, the timeline restarts for the PSI/PCL process.
- **For additional guidance please review *"Applicant Tips for Successful e-QIP Submission“* located on the DSS.mil JPAS site.**

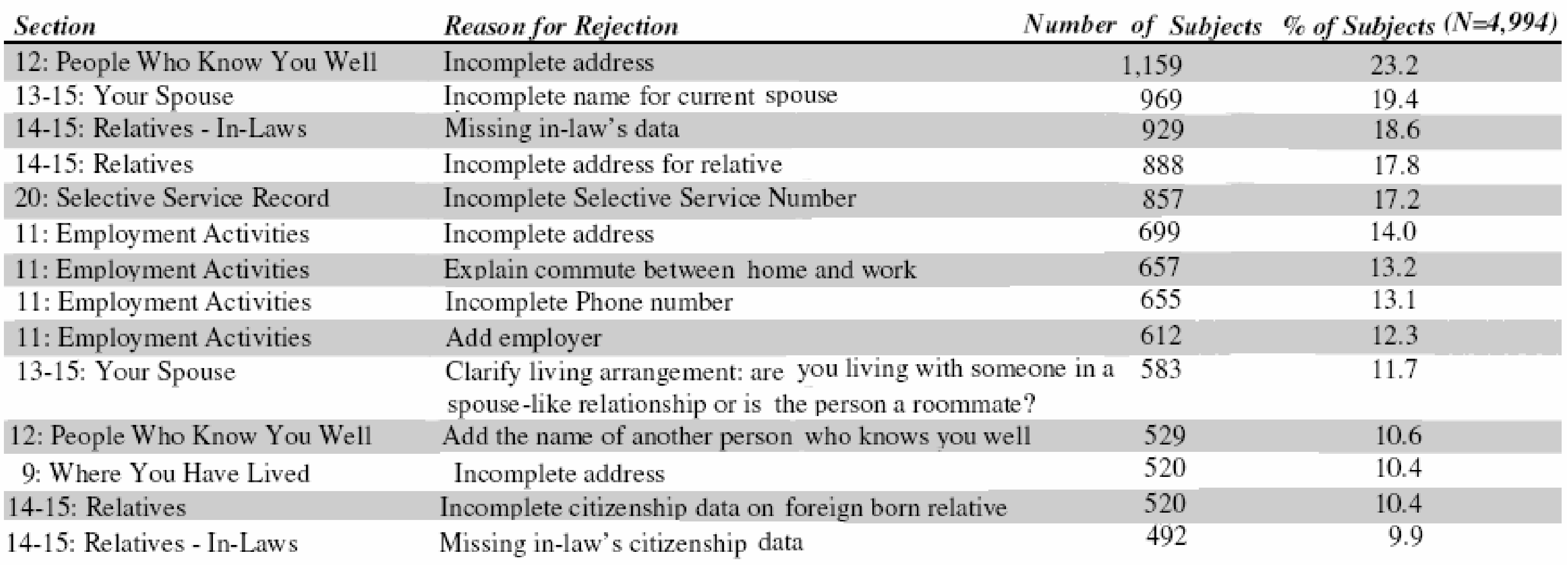
Source: JPAS / OPM IRTPA Monthly Reports

REJECTS

Reasons and Category

TOP REASONS FOR REJECTION

Source – "Analysis of Defective SF86 Submissions" PERSEREC Working Paper 09-03



Section	*Reason for Rejection*	*Number of Subjects*	*% of Subjects (N=4,994)*
12: People Who Know You Well	Incomplete address	1,159	23.2
13-15: Your Spouse	Incomplete name for current spouse	969	19.4
14-15: Relatives - In-Laws	Missing in-law's data	929	18.6
14-15: Relatives	Incomplete address for relative	888	17.8
20: Selective Service Record	Incomplete Selective Service Number	857	17.2
11: Employment Activities	Incomplete address	699	14.0
11: Employment Activities	Explain commute between home and work	657	13.2
11: Employment Activities	Incomplete Phone number	655	13.1
11: Employment Activities	Add employer	612	12.3
13-15: Your Spouse	Clarify living arrangement: are you living with someone in a spouse-like relationship or is the person a roommate?	583	11.7
12: People Who Know You Well	Add the name of another person who knows you well	529	10.6
9: Where You Have Lived	Incomplete address	520	10.4
14-15: Relatives	Incomplete citizenship data on foreign born relative	520	10.4
14-15: Relatives - In-Laws	Missing in-law's citizenship data	492	9.9

FACILITIES WHERE REJECTS MOST OFTEN OCCUR – FY09

- Smaller Category D / Non-possessing Category E
  - *These facilities proportionally have a higher amount of rejects than the amount of requests they have approved*

	% of Requests	**% of Rejects**
A / AA	22.30%	8.80%
B	6.90%	5.90%
C	8.50%	8.40%
D	27.20%	27.70%
E	35.10%	49.20%

FY09 INDUSTRY CLEARANCE SUBMISSIONS VS PROJECTIONS

- OMB performance goal is +/- 5%

  - ➢ 30 May '09 Status: At the close of May, Industry clearance submissions were 2% below overall Industry/DSS projections.

  - ➢ Historically, case submissions trend downward during winter months and peak during spring and summer months.

FY09 Projection	Weekly Projected	Year to Date	% of Projection
182,315	3,506	3,435	98%

Appendix 3
Mr. Mansfield’s PCL Working Group Presentation

Defense Security Service

Secure Web Fingerprint Transmission System (SWFT)

Office of the Chief Information Officer

July 22, 2009

New SWFT System Implementation

- **SWFT permits electronic delivery of fingerprints to OPM for contractors under the NISP**
- **SWFT 2.0 is scheduled for deployment late July 2009**
  - **SWFT Pilot participants are transitioning to the new system prior to phasing in additional users**
  - **Additional companies will be phased in starting August 2009**
- **DSS targeted equipment survey conducted in June 2009.**
  - **401 companies surveyed, representing 75% of FY08 Industry personnel security investigation (PSI) requests**
  - **DSS will use survey results to identify next companies to phase in.**

SWFT Survey Results

- Equipment survey responses indicate:
  - 140 companies forecast future participation (representing 29% of FY08 PSI requests)
  - 121 companies are unsure (representing 11% of the FY08 PSI requests)
  - 42 companies do not plan to participate (representing 3% of the FY08 PSI requests)
  - Remaining companies did not respond to the survey (representing 21% of the FY08 PSI requests)

- Equipment cost and uncertainty about equipment requirements/procurement were the main concerns.

Way Ahead

- Procurement of image machines/card scanners
  - Industry responsible for procurement and management
  - Length of procurement process has been reported to be 3 months (this timeline is company dependent)
  - Technical support is required to configure properly
- Configuration of fingerprint image capture machines and card scanners will be required
  - A basic configuration guide will be provided
  - DSS will not provide technical assistance with configuration

Way Ahead (Cont.)

- DSS Call Center will create two accounts for each FSO
  - FSO will create additional corporate accounts
  - DSS SAR was updated to include SWFT access

- Fingerprint machine registration and test
  - OPM requires each machine to be tested (x2) and provides authorization to submit via the production system
  - DSS & OPM are implementing a bulk registration process
  - DSS is dedicating a full time resource to support registrations
  - Estimated capacity in excess of 100 new machines per week

Way Ahead (Cont.)

- Explore a future SWFT enhancement
  - Validate data elements prior to submission to OPM
  - Simplify (or eliminate) test and registration requirements
  - Increase registration capacity with OPM
  - Evaluation and planning will begin after SWFT 2.0 deployment
- Coordinate with DMDC to plan for SWFT transition

References

- **Documentation / References**
  - http://www.dss.mil/
  - SWFT 2.0 Memorandum (in draft)
  - SWFT User Guide
  - Registration & Access Procedures
  - Machine Basic Configuration Guide
  - System Access Request (SAR)

Questions

Questions?

Appendix 4
Mr. Pannoni’s FOCI Working Group Presentation

NISP Implementing Directive

(Summary of Proposed Changes)

National Interest Determinations (NIDs)

- Specifies Requirement
- Application of the Requirement
  --- Precontract activity, new contracts, and existing contracts
- Delineation of U.S. Government Responsibilities
  --- CSO, GCA, other departments and agencies
- Provides for Timelines to Render NID Decisions and Follow-Up
  --- 30 and 60 days
- Defines NID, CSO and Proscribed Information

Appendix 5
Mr. Farley’s Certification and Accreditation Working Group Report

Defense Security Service

Industrial Security Field Operations
Office of the
Designated Approving Authority
(ODAA)

July 2009

Defense Security Service

Overview

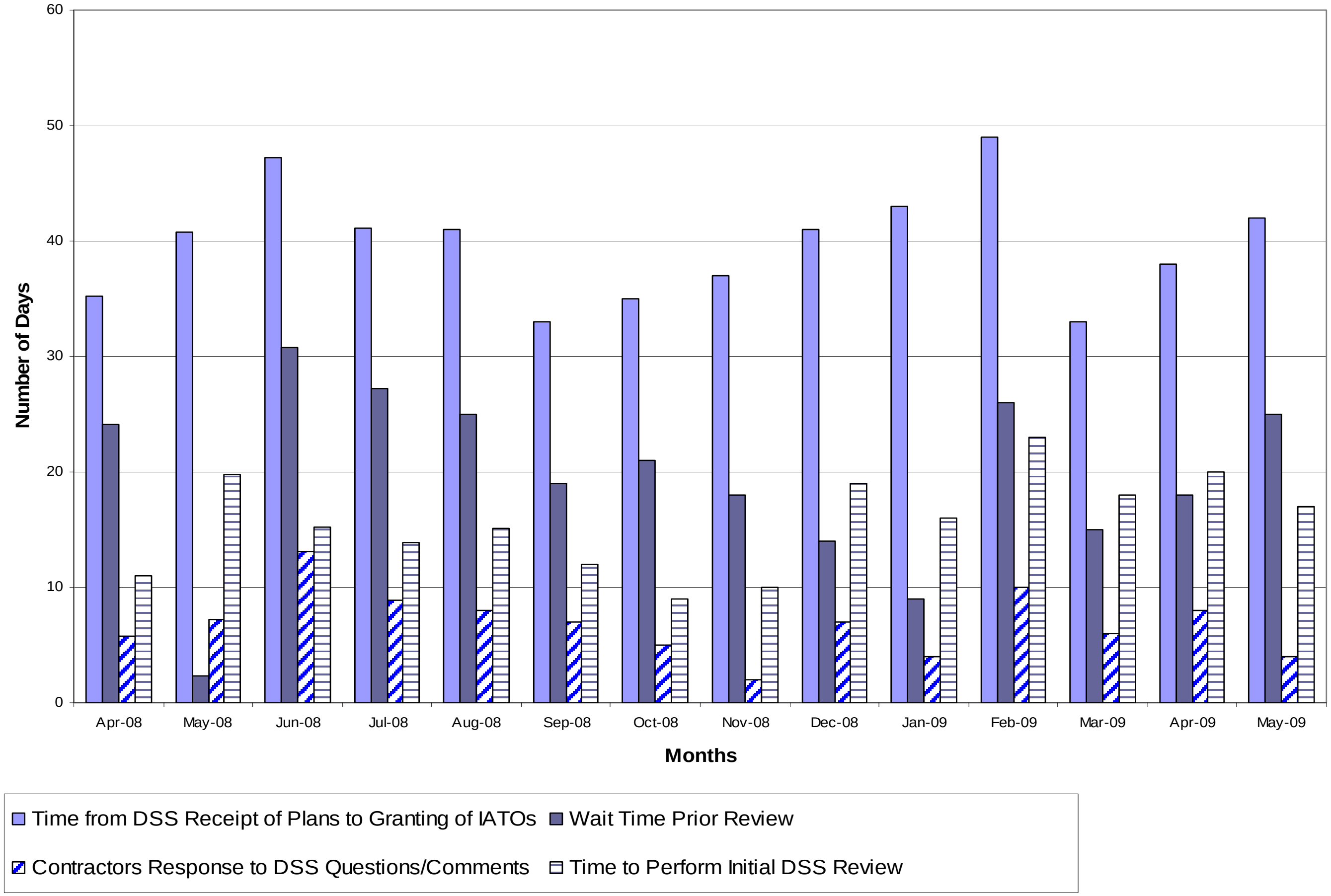
- Certification & Accreditation (C&A)
- C&A Metrics

Certification & Accreditation

- DSS is the 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

ODAA Metrics for # Days to Process Plan Submissions

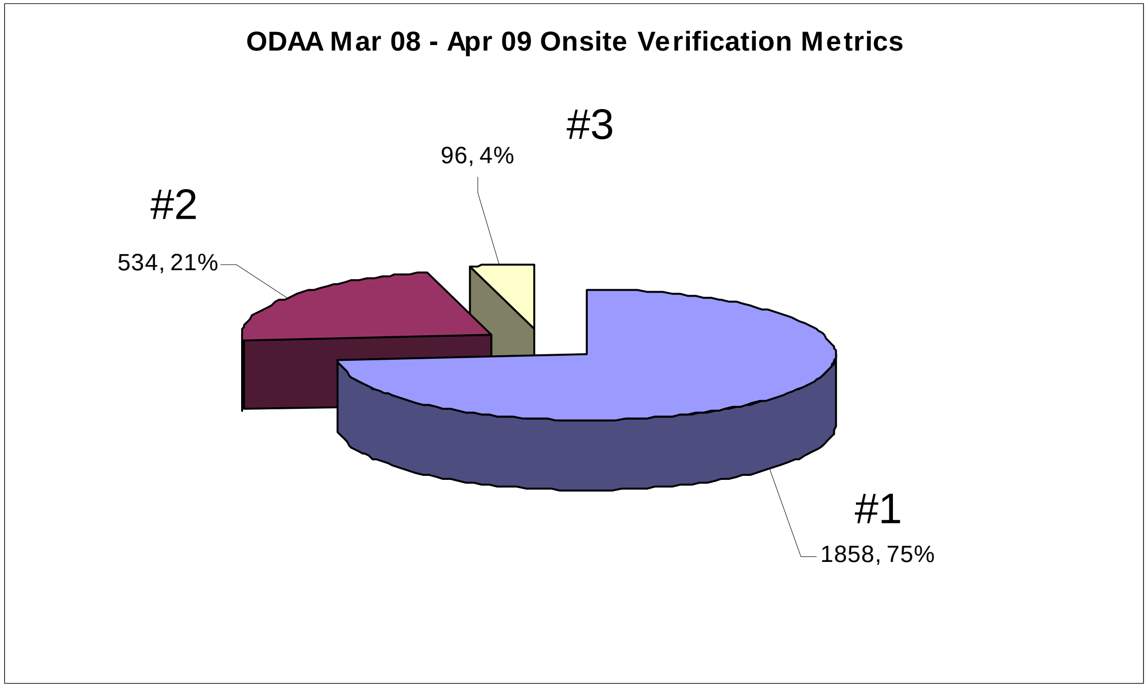


During the Past Year Apr 2008 – May 2009

- Average number of days to receive an IATO after receipt of a submission is 40 Days
- Average waiting time before a review process is initiated is 20 Days
- Average number of days for the review time to be completed is 16 Days

ODAA Metrics and Organization

On-site Verification Stats (26% Required Some Level Modifications)



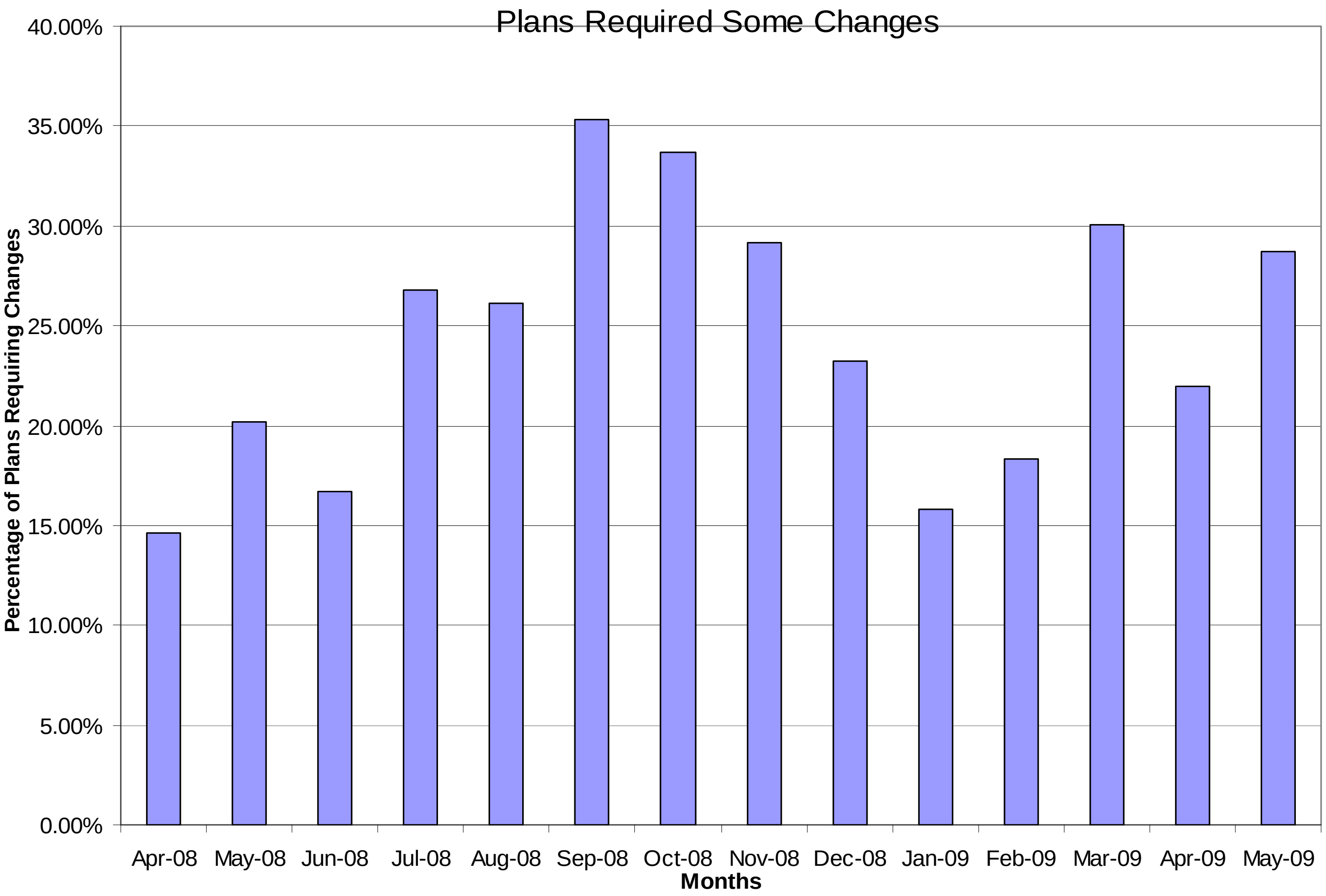
#1. No discrepancies discovered during on-site validation.

#2. Minor discrepancies noted and corrected during on-site validation.

#3. Significant discrepancies noted which could not be resolved during on-site validation.

ODAA Metrics
Security Plan Reviews

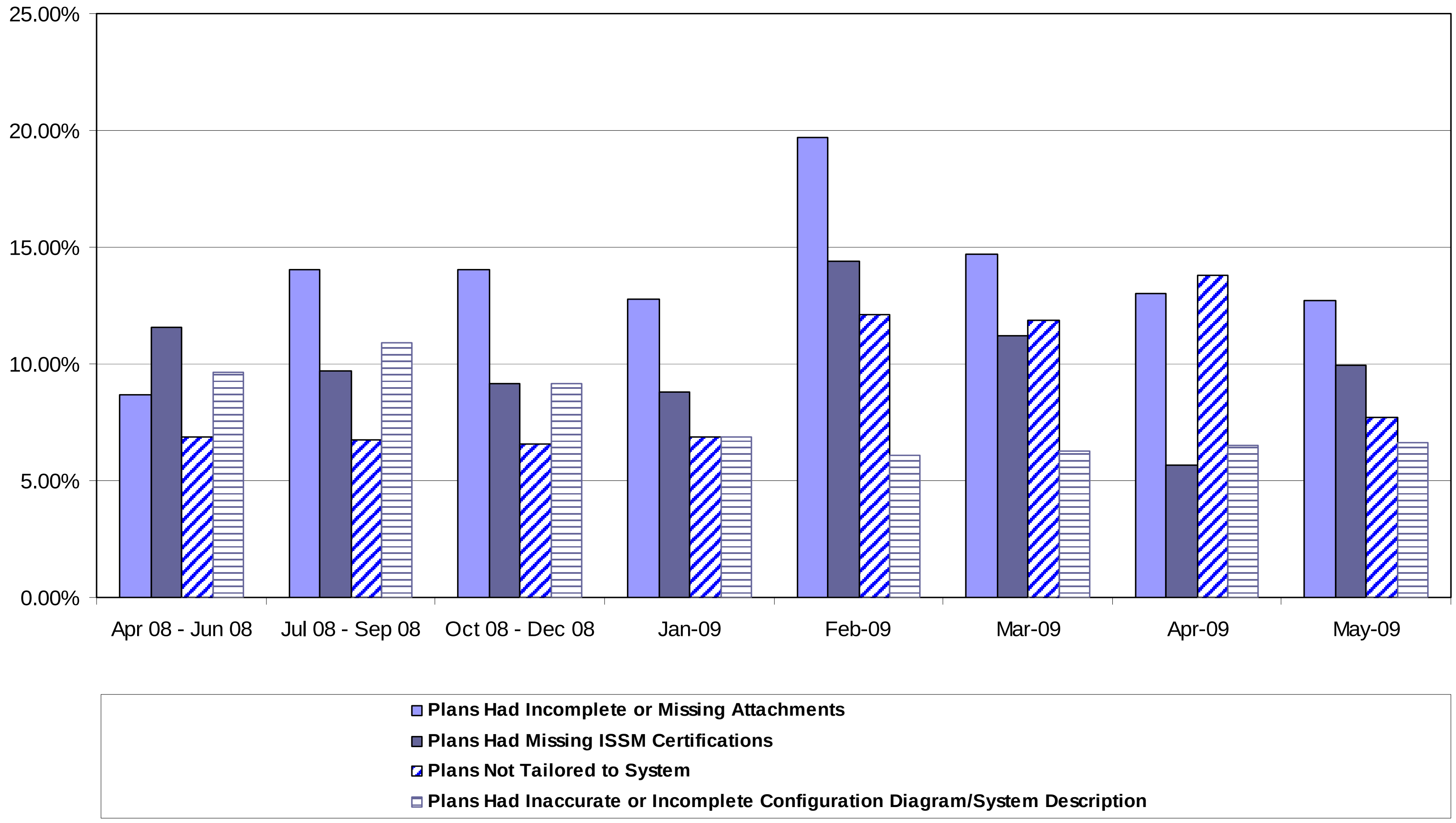
Review Questions and/or Comments, Errors and Corrections Noted



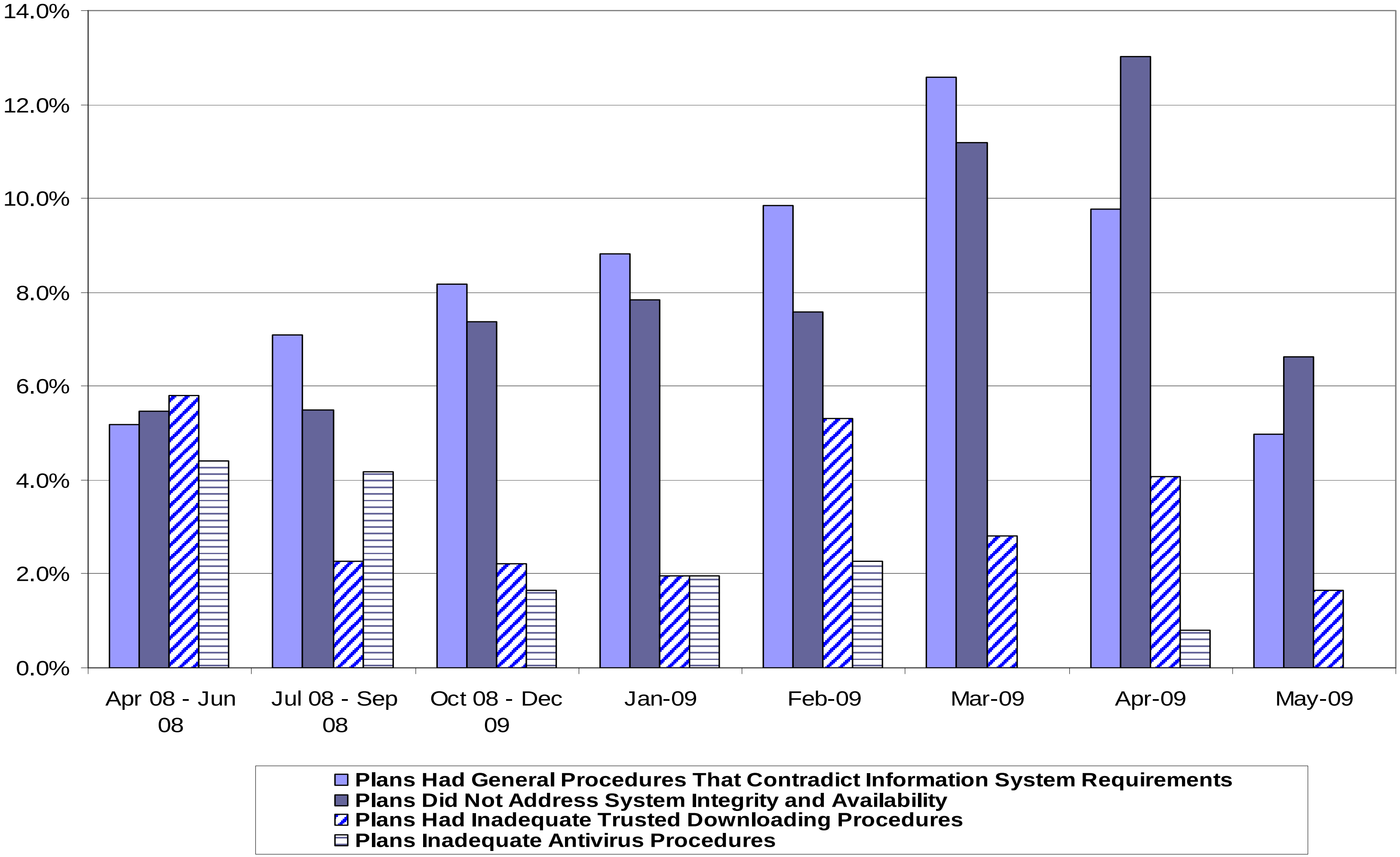
Of the 1898 plans received from Apr 08 – May 09:

- On average 24.3 % of all plans submitted required changes prior to the On-site Verification for ATO

ODAA Metrics
Security Plan Reviews Common Errors
Part One



ODAA Metrics
Security Plan Reviews Common Errors
Part Two



Appendix 6
Ms. Shoup-Stirlen, Mr. Chambers, and Mr. Lawrence’s Security Operations Curriculum Development Presentation

Office of the Director of National Intelligence Special Security Center

Security Operations Curriculum Development

Overview

- Security Education and Training Program Objectives
- IC Security Education and Training Council
- Why Develop a Security Operations Curriculum
- Educate not Train
- Summary

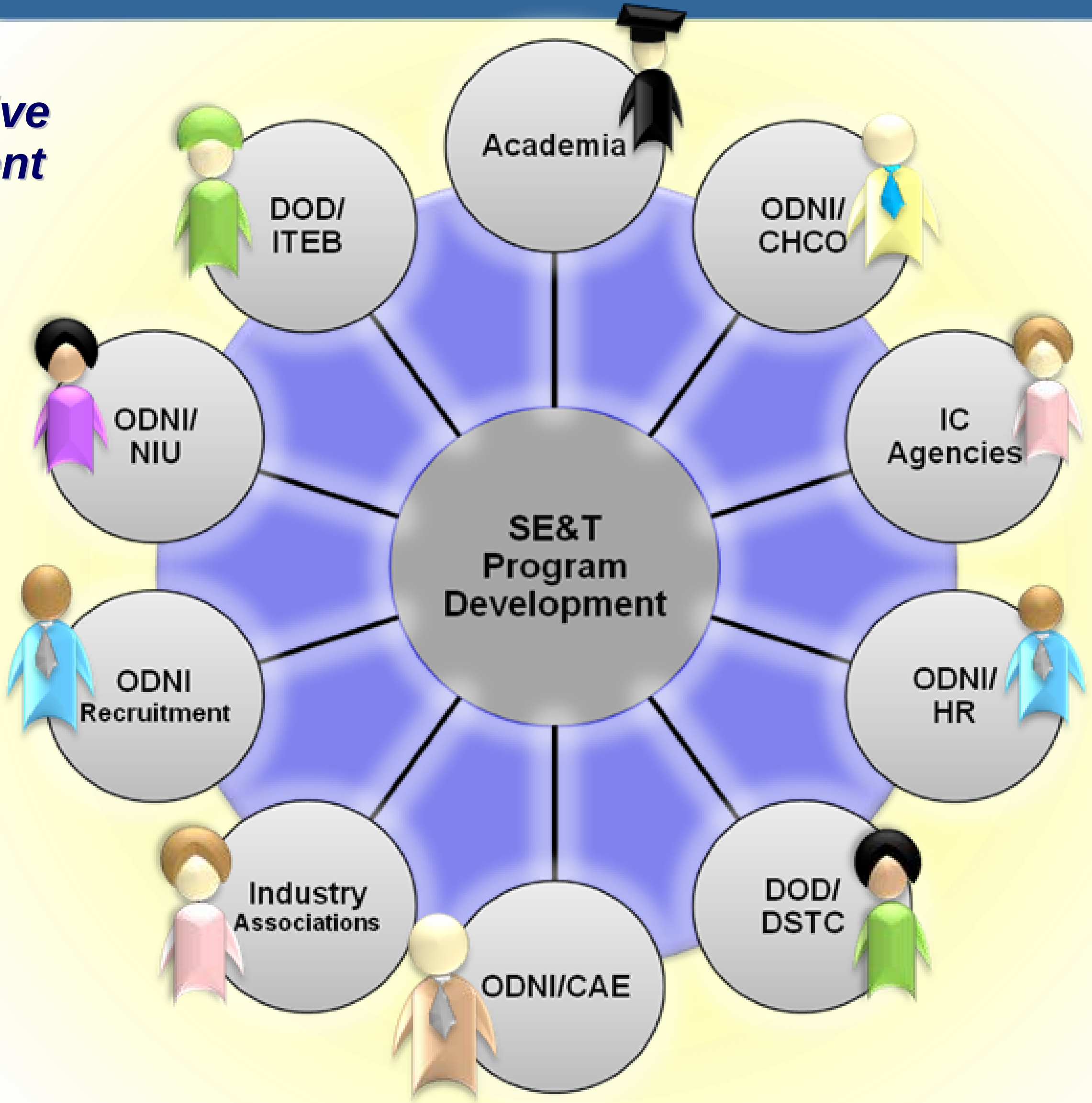
IC Security Education & Training Program

Objectives

- Support common, uniform, and reciprocal security practices as directed by the National Intelligence Strategy
- Make the IC be the security professionals' "'employer of choice' able to *attract* and *retain* the very best and brightest to our ranks"
- Facilitate greater integration and collaboration within the security profession across agencies
- Professionalize the security profession through education and training
- Make the whole of the Intelligence Community greater than the sum of its parts

IC Security Education & Training Program

Collaborative Environment



IC Security Education & Training Council

- Membership, Objectives and Scope
  - IC Agency Security Education/Training Chiefs
  - The SE&T Council will **assess, enhance** and **sustain** the IC SE&T Program in accordance with appropriate authorities and directives
  - Establish a training infrastructure that can easily adapt to future training requirements and opportunities
  - Increase IC agencies' collaboration on
    - Training requirements, methodologies, curriculum
    - Career development, mentoring, and certification programs

Combined Vision

To collaborate with academia to develop a
Security Operations Baccalaureate Degree Program
allowing the USG and Industry to grow future security professionals

Why a Security Operations Curriculum?

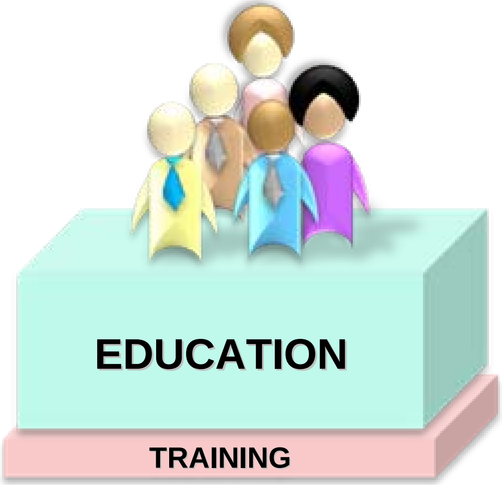
- More focused, formal degree program will enable security "practitioners" to become even more effective as "professionals"
- No traditional higher education institution has a baccalaureate program that focuses on our definition of Security
- The competition for talent will increase proportionally, not just between government and industry, but also between security disciplines
- The Security Profession will be competing for talent with our counterparts in Analysis, Finance, Operations, etc.

Educate not Train

- Use existing academic courses as a foundation to build a Security Operations
- Education emphasizes principles;

  training emphasizes application
- Education focuses on building the mind;

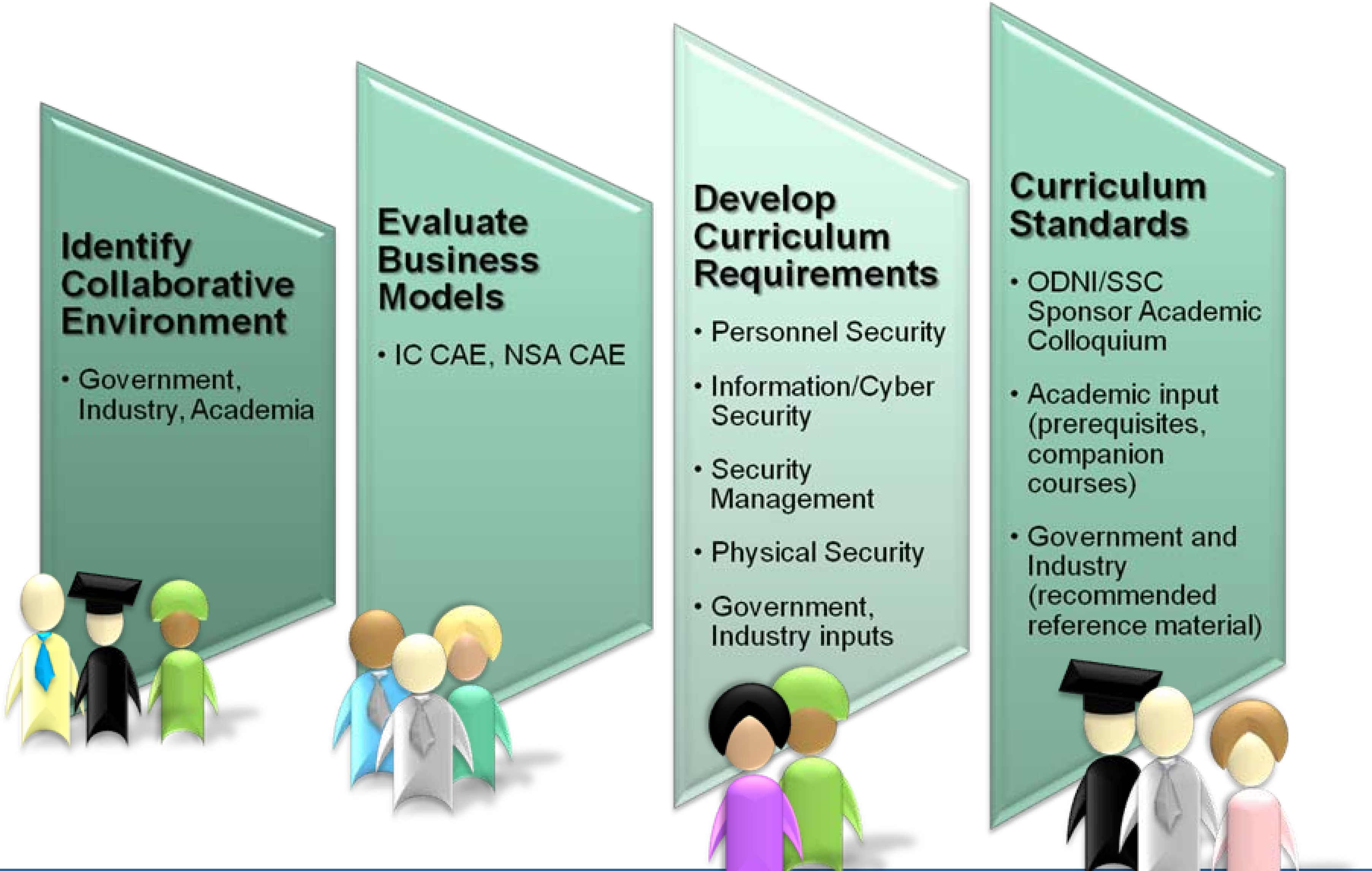
  training on building skills
- Educate future security professionals that will be trained by their future agency or company



Education is not the filling of a pail, but the lighting of a fire.

William Butler Yeats

Development Process



Identify Collaborative Environment

- Government, Industry, Academia

Evaluate Business Models

- IC CAE, NSA CAE

Develop Curriculum Requirements

- Personnel Security
- Information/Cyber Security
- Security Management
- Physical Security
- Government, Industry inputs

Curriculum Standards

- ODNI/SSC Sponsor Academic Colloquium
- Academic input (prerequisites, companion courses)
- Government and Industry (recommended reference material)

Advertise and Recruit

- Advertisement
  - National Academic Colloquium
  - Professional Media

- Recruitment
  - Exploit Current Scholarship and Internships
  - Explore and support new opportunities
    - ➢ Agency/university partnerships
    - ➢ Industry/university partnerships
    - ➢ Adjunct instructors
    - ➢ Scholarships/Internships
  - Forecast specifics of human talent requirements
  - ID Security professionals to participate in recruiting events
  - Develop an Agency/Industry coordinated recruiting calendar
  - Recruit

Summary

- Government and industry leaders of the Security Profession should no longer rely on talent to be delivered, but must be actively involved in the talent management process
- One solution is to grow our own talent—that growth begins in academia

Collaborative Environment

INDUSTRIAL SECURITY WORKING GROUP

IC Security Education & Training

Mitch Lawrence

Chairman, ISWG

Introduction

- ISWG brief overview
- Background information
- Why is ISWG interested?
- The ISWG commitment

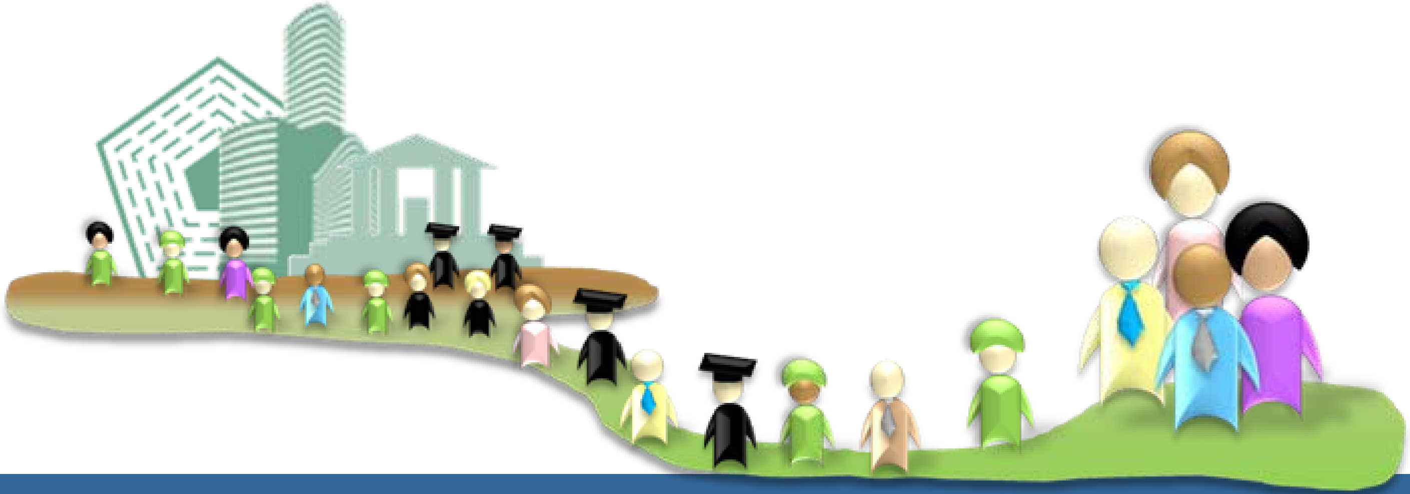
Why Should Industry Support?

- Return on security investment –
  - Attract, train and hire individuals who have been given the foundation of our profession PRIOR to joining our organizations.
  - Validating the security professional career path:

“It just isn't for them"

Why Should Industry Support?

- It’s the right thing to do for our profession –
  - Gives credibility to the government/industry security profession
  - Gives us a credible "supply chain" to pull from into the profession
  - Continuity of the security professional career



How Can Industry Support?

- Engagement at every level
  - Subject matter expertise in curriculum review/development and serving as guest speakers or adjunct professors
  - Internships for students at participating companies & possibly our Government agency partners
  - Industry organizations assisting graduates of this degree program with their job search after graduation

Summary

Bottom Line:

- The security (government and industry) profession needs to grow their own future security professionals

- This opportunity is our chance to make an impact to our profession now and for years to come.

Backup Slides

Security Operations Curriculum

- Introduction to Psychology
- Social Psychology
- Psychology of Human Sexuality
- Introduction to Sociology
- Social Problems
- Deviance
- Criminal Investigation
- Research Methods in Criminal Justice
- Interpersonal Communication
- Research and Critical Writing
- Workplace Writing
- Technical Writing
- Expository English Composition
- Public Speaking
- Business and Professional Communication

Security Operations Curriculum

- Personnel Security (4xxx-level course)
  - Week 1-7: Academics: ICD 704 and associated ICPGs
  - Begin background investigation (using mock cases)
  - Mid-term: Knowledge test
  - Week 7-15: Practical Application Classes and Lab
  - Case development, documentation, following leads, interviewing, consolidation, report writing
  - Final: Presentation of investigation, adjudicated case with recommendation to Adjudications Board (chair, members TBD)

Security Operations Curriculum

- Information Security, Information Systems Security, Communications Security (3xxx-4xxx-level course)
  - Course: Develop knowledge based policy course using USG Directives as educational tool, i.e., ICD 503
    - ➢ Introduction to Computer Science
    - ➢ Advanced Object-Oriented Programming
    - ➢ Computer Security
    - ➢ Computer Networks

Security Operations Curriculum

- Introduction to Public Administration
- Public Policy Process
- Introduction to Management and Organizational Behavior
- Advanced Organizational Development
- Project Management
- Business Finance
- Management Accounting
- Criminal Justice Organization and Management

Security Operations Curriculum

- Security Management (4xxx-level course)
  - What is it? Manages security implications (e.g., strategic, personnel, infrastructure, policy enforcement, emergency planning, and other resources) for a program or other area of responsibility. Source: ICD 610, Annex R (Competency Directory for Security)
  - Accomplished through blended education (course work, online studies, seminar attendance, and guest speaker series) throughout semester or academic year similar to an honors program, culminating with a written project and presentation. Project sponsorship possible; internships.

Security Operations Curriculum

- Physical Security (Two courses taken in sequence)

- Physical Security I: Analytical Risk Management (ARM) (3xxx/4xxx-level)

  - Week 1-7: Academics ARM Course
  - Mid-term: Knowledge test
  - Week 7-15: Practical Application Classes and Lab (Vulnerability Assessment, Threat Assessment, Countermeasure recommendations)
  - Final: Publication and presentation of report with findings

Security Operations Curriculum

- Physical Security II
- Policy, Equipment and Technology (PET) Project (4xxx-level)
  - Academics (DCID 6/9 and associated annexes)
  - Research and Application: Using ARM class report’s recommended countermeasures, develop policy, identify and integrate equipment and technology with policy to most effectively fill countermeasure requirements.
  - Understand relationships at the tactical level (security is not the mission, the mission is the mission) and at the operational and strategic levels (interoperability of equipment and technology between agencies).
  - Mid-term: knowledge level test. Final: Application level presentation

Appendix 7
Mr. Jarvie’s Combined Industry Presentation

NISPPAC
Industry Presentation

22 July 2009

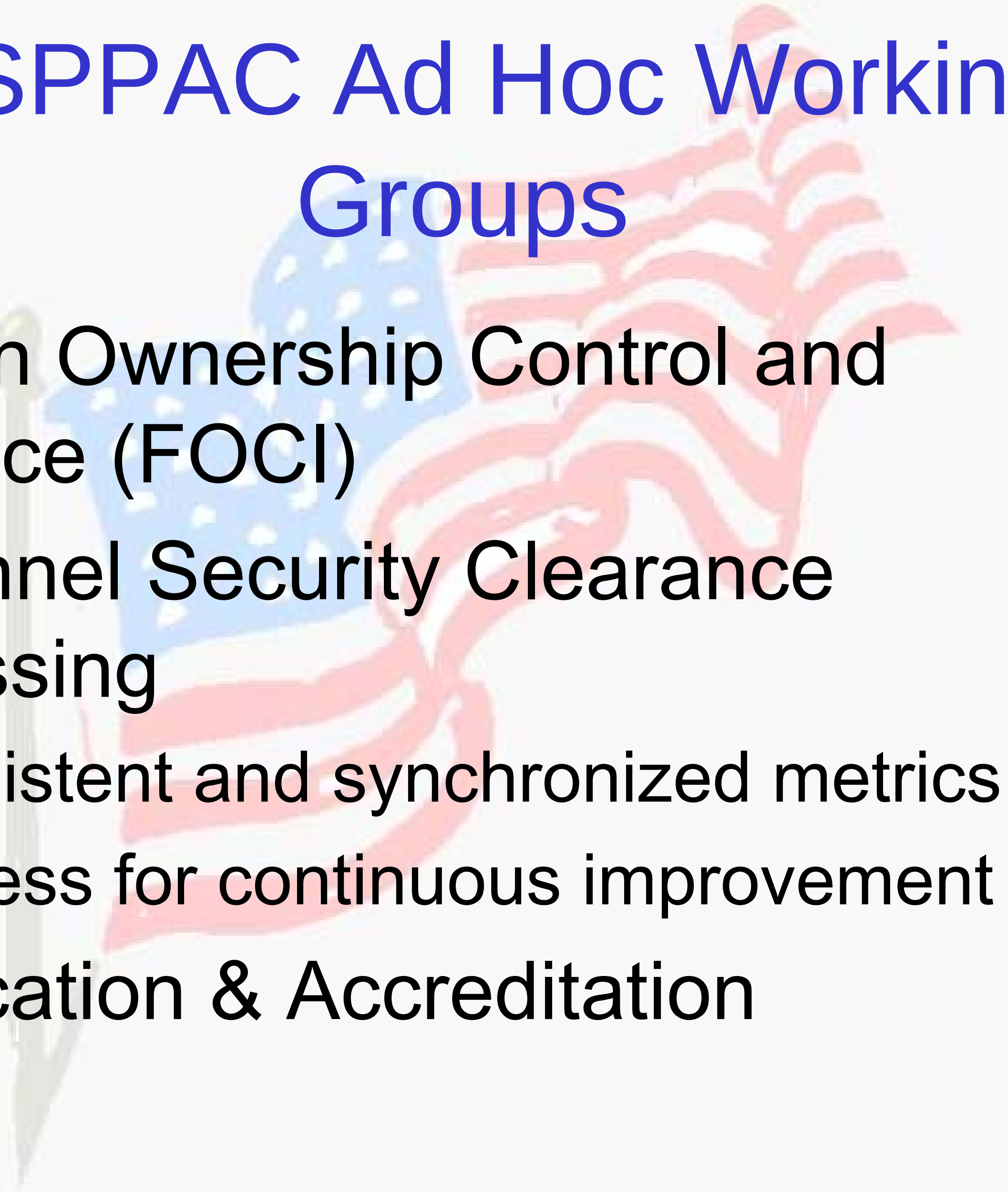
Industry Members/NISPPAC

Member	Company	Term Expires
Tim McQuiggan	Boeing	2009
Doug Hudson	JHU/APL	2009
“Lee” Engel	BAH	2010
Vince Jarvie	L-3	2010
Sheri Escobar	Sierra Nevada	2011
Chris Beals	Fluor Corporation	2011
Scott Conway	Northrop Grumman	2012
Marshall Sanders	SRA	2012

Industry Members/MOU

AIA	Scott Conway
ASIS	Ed Halibozek
CSSWG	Randy Foster
ISWG	Mitch Lawrence
ITAA	Richard “Lee” Engel
NCMS	Paulette Hamblin
NDIA	Fred Riccardi

NISPPAC Ad Hoc Working Groups

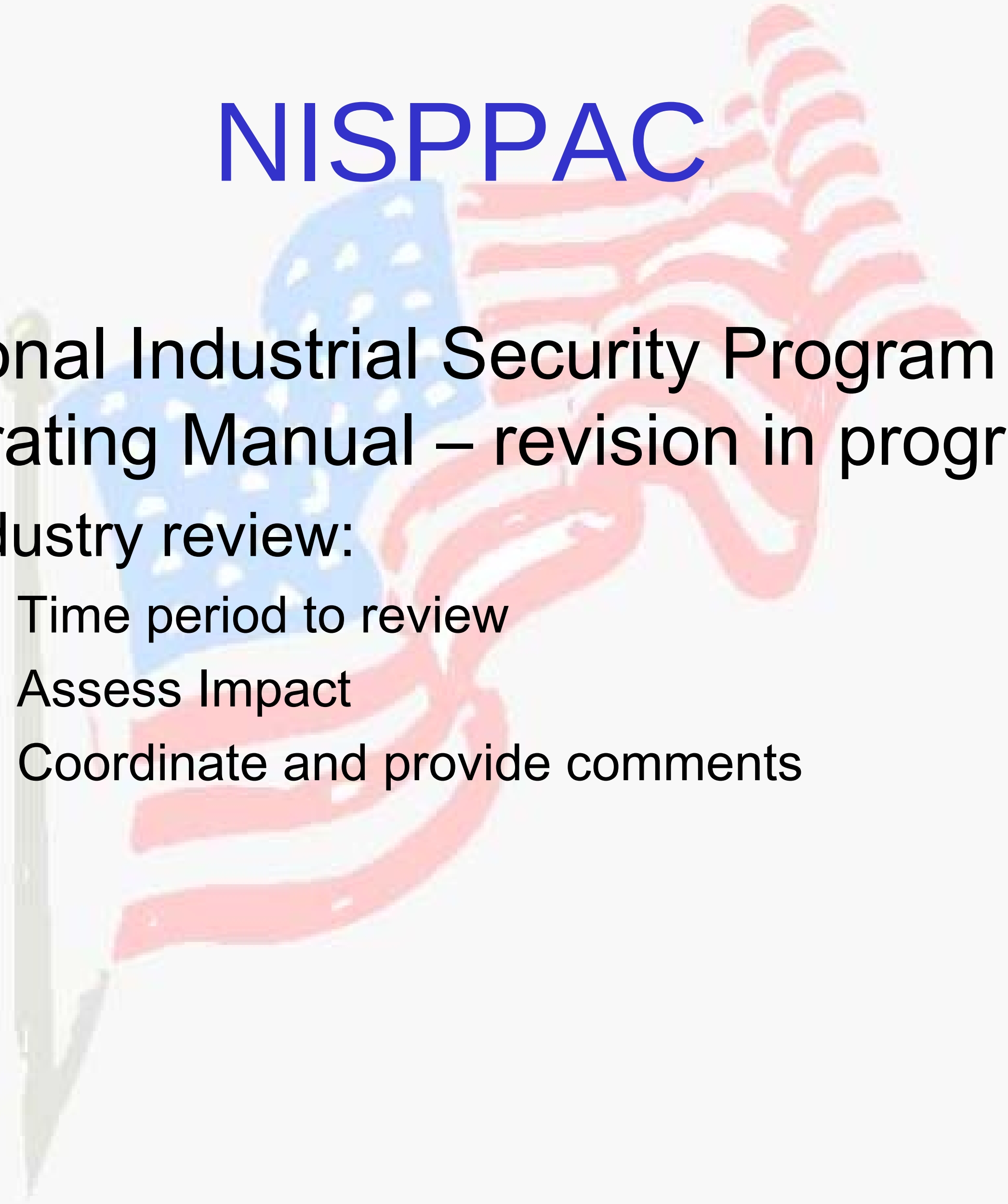


- Foreign Ownership Control and Influence (FOCI)
- Personnel Security Clearance Processing
  - Consistent and synchronized metrics
  - Process for continuous improvement
- Certification & Accreditation

NISPPAC

- National Industrial Security Program (NISP)
  - Industrial Security Letter Implementation
    - Office of the Designated Approval Authority
  - Industrial Security Letter 2009 - 02
    - Clarification - items 2 and 3
      - 2) Pre employment clearance action
      - 3) Negotiating an acceptable FOCI mitigation

NISPPAC



- National Industrial Security Program Operating Manual – revision in progress
  - Industry review:
    - Time period to review
    - Assess Impact
    - Coordinate and provide comments

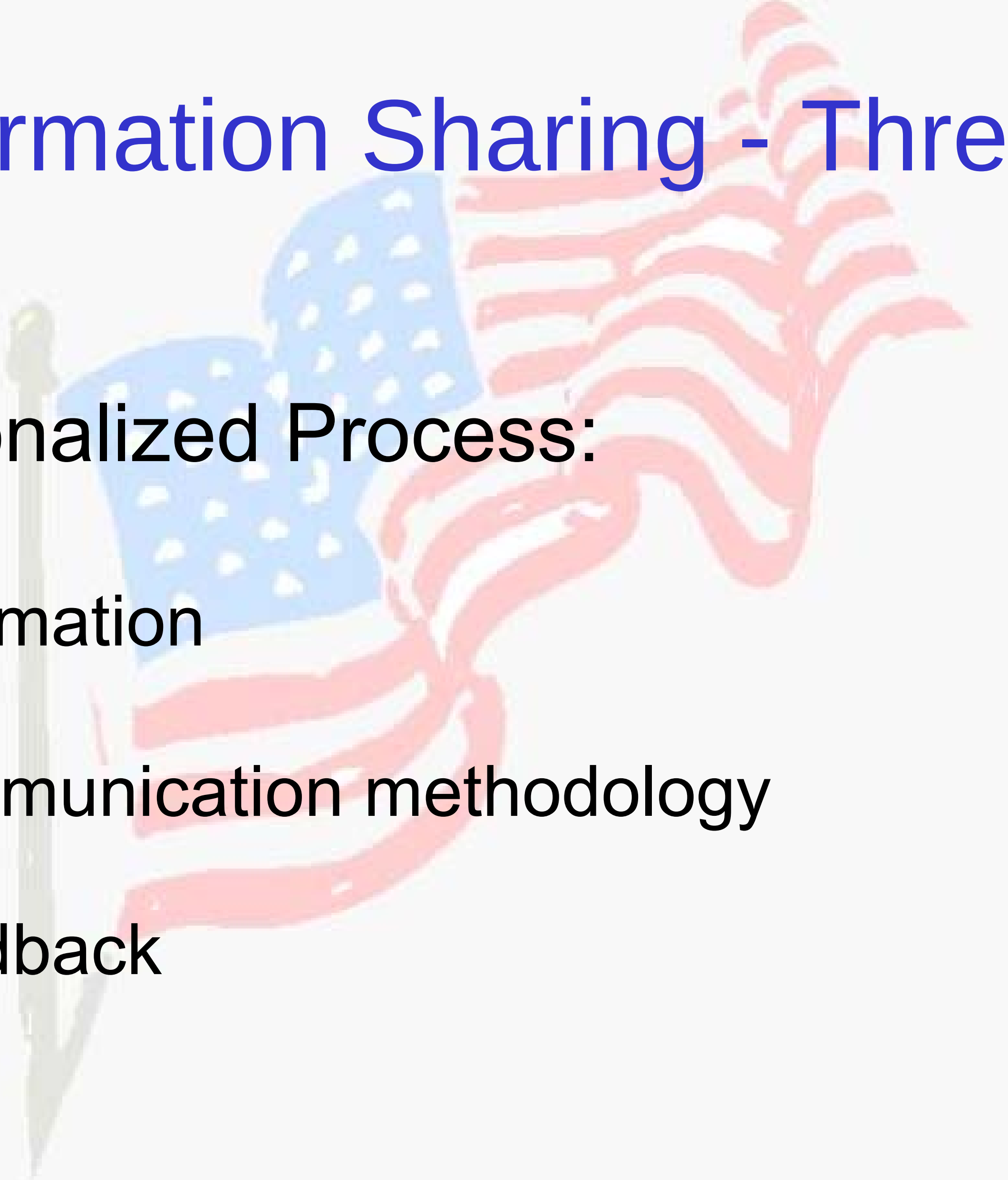
NISPPAC

(Industry concerns 15 May 2008/ 20 November 2008/ 07 April 2009))

- Information Sharing - Threat
- Controlled Unclassified Information*
- Foreign Ownership Control & Influence (FOCI) *
- Personnel Security Clearance Processing*

*previously discussed

Information Sharing - Threat



Institutionalized Process:

- Information
- Communication methodology
- Feedback