**NATIONAL INDUSTRIAL SECURITY PROGRAM**
**POLICY ADVISORY COMMITTEE (NISPPAC)**

**SUMMARY MINUTES OF THE MEETING**

The NISPPAC held its 34th meeting on Thursday, October 8, 2009, at 10:00 a.m., at the National Archives Building, 700 Pennsylvania Avenue, NW, Washington, DC 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 January 11, 2010.

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)
- Richard Hohman (Office of the Director of National Intelligence)
- Richard Donovan (Department of Energy)
- Jose Salazar (Department of Homeland Security)
- Dennis Hanratty (National Security Agency)
- Kimberly Baugher (Department of State)
- Richard Lee Engel (Industry)
- Douglas Hudson (Industry)
- Timothy McQuiggan (Industry)
- Vincent Jarvie (Industry)
- Scott Conway (Industry)
- Marshall Sanders (Industry)
- Frederick Riccardi (Industry)
- Shawn Daley (Industry)
- Darlene Fenton (Nuclear Regulatory Commission)
- Kathleen Branch (Defense Security Service)
- Kisha Braxton (Department of Commerce)
- Colleen Crowley (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 10:08 a.m. The Chair recognized Frederick Riccardi, Industry, and Shawn Daley, Industry, as the newest incoming members of the NISPPAC. The Chair also recognized Timothy McQuiggan, Industry, and Douglas Hudson, Industry, as outgoing members of the NISPPAC and presented them with a token of appreciation for their service. The Chair requested that comments to the minutes from the July 22, 2009, be provided by October 17, 2009.

## II. Old Business

The Chair requested that Greg Pannoni, ISOO, review the action items from the last meeting.

*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.*

Mr. Pannoni stated that the amended NISPPAC Bylaws were now posted to the ISOO website, and that a related issue will be discussed under new business.

*ACTION: The Chair stated that the Foreign Ownership, Control, or Influence (FOCI) Working Group would suspend operations, as its main initiative has been completed and is in final coordination. The Personnel Security Clearance (PCL) and the Certification and Accreditation (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.*

Mr. Pannoni stated that the FOCI Working Group completed work on a revision to the National Industrial Security Program (NISP) Directive No. 1 with regard to National Interest Determinations. The document was forwarded to the National Security Council Interagency Policy Committee on Records Access and Information Security, and the committee recommended that it be formally coordinated as written. Mr. Pannoni indicated the revision was being prepared for publication in the Federal Register so that it could be formally coordinated for a review. He advised that once the revision is published there will be a 60-day comment period, and all NISPPAC members would be notified. Mr. Pannoni stated that updates for the PCL and C&A Working Groups would be provided after the review of old business.

*ACTION: ISOO will host a meeting with Industry to provide the opportunity for Industry to make recommendations for changes to the National Industrial Security Program Operating Manual (NISPOM).*

Mr. Pannoni stated that a NISPOM listening session was conducted on August 27, 2009, and Industry provided a robust set of comments and suggestions. He advised that Industry would be given ample time to review any proposed changes to the NISPOM. He also indicated that Stephen Lewis, Department of Defense (DoD), would provide more on this topic during his presentation.

*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.*

The Chair spoke to the final action item concerning smaller NISP companies stating that there was a request to examine how to better support smaller companies. There are two options: (1) use one of the three NISPPAC meetings as a focus meeting for small company solutions and solicit issues of concern from small companies; or (2) hold a NISPPAC meeting outside of the Washington, DC, area to create greater involvement from smaller companies. The Chair stated that these two options would be pursued within the provisions of the Federal Advisory Committee Act (FACA).

## III. Working Group Updates

### A) Personnel Security Clearance (PCL) Working Group Report[1]

Deborah Smith, Office of Personnel Management (OPM), and Kathleen Branch, Defense Security Service (DSS), provided the PCL Working Group Report. Ms. Smith stated that the end-to-end metrics for DoD industry personnel represented the adjudicative decisions as reported by DSS to OPM through a daily upload to the Personnel Investigative Processing System. Ms. Smith provided metrics for end-to-end timeliness for all levels of initial clearances plus Secret and Confidential Periodic Reinvestigations (PRs) for the third quarter of fiscal year (FY) 2009, which were 30,263 cases that averaged 106 days, and the fastest 90 percent of these decisions averaged 77 days. Ms. Smith also provided end-to-end timeliness data for third quarter FY 2009 Top Secret clearances, which were 6,554 cases that averaged 134 days, and the fastest 90 percent of these decisions averaged 107 days. The data for end-to-end timeliness for third quarter FY 2009 initial and PRs for Secret and Confidential clearance decisions consisted of 23,696 cases that averaged 98 days and the fastest 90 percent of these decisions averaged 69 days. Ms. Smith provided data for end-to-end timeliness for third quarter FY 2009 Top Secret PRs, which consisted of 5,965 cases that averaged 163 days, and the fastest 90 percent of these decisions averaged 121 days. She emphasized that these metrics included both collateral and Sensitive Compartmented Information (SCI) adjudications.

Ms. Smith presented average end-to-end timeliness for the fastest 90 percent of all levels of initial clearances plus Secret and Confidential PRs for July and August 2009, which were 82 days and 84 days respectively. Ms. Smith stated that on August 20, 2009, Defense Industrial Security Clearance Office (DISCO) began receiving cases electronically from OPM, which means that the estimated 10-day mail time will be replaced with actual transmission time, thus significantly reducing end-to-end timeliness of clearance decisions. Ms. Smith presented the average end-to-end timeliness data for the fastest 90 percent of initial Top Secret clearance decisions for July and August 2009, which were 119 days and 118 days respectively. Ms. Smith presented the average end-to-end timeliness data for the fastest 90 percent of initial and PRs for Secret and Confidential clearance decisions for July and August, which were 76 days and 75 days respectively. Ms. Smith also presented the average end-to-end timeliness data for the fastest 90 percent of Top Secret PR clearance decisions for July and August, which were 128 days and 131 days respectively.

Ms. Smith stated that a revised Standard Form 86, "Questionnaire for National Security Positions" (SF 86), has been published in the Federal Register for comment and probably will be effective in 2010. The Chair thanked Ms. Smith and introduced Ms. Branch.

Ms. Branch provided metric data for DISCO adjudicative activity. Ms. Branch stated that there was a 9 percent decrease in adjudicative workload from the end of the first quarter of FY 2009 to the end of July 2009. Ms. Branch stated that there were 27,522 Industry cases pending at OPM as of the end of July 2009, which represents a 5 percent reduction from the end of the first quarter of FY 2009. The Chair asked Ms. Branch if the decrease

[1] See appendix 1 for Ms. Smith's presentation and appendix 2 for Ms. Branch's presentation.

in inventory was due to challenging economic times resulting in less requests for clearances. Ms. Branch responded by presenting data that compared clearance submissions to projections based on a survey sent to Industry by DSS. At the close of July 2009, clearance submissions were about 2 percent below overall projections. Vincent Jarvie, Industry, commented that the reduction in caseload belies a probable decrease in submissions. Ms. Smith commented that there was a 3 percent decrease in cases from FY 2008 to FY 2009; however, there was a 13 percent increase in Special Background Investigations and a decrease in Top Secret PRs from FY 2008 to FY 2009. The Chair thanked Ms. Branch and introduced Michael Farley, DSS.

### B) Certification and Accreditation (C&A) Working Group Report[2]

Mr. Farley provided a report on the Working Group's progress. Mr. Farley stated that it was DSS' goal to ensure the implementation of security measures that are consistent with national level policy. He stated that the entire C&A process from the submission of the system security plan (SSP) to the issuance of an Interim Approval to Operate (IATO) averaged 38 days for FY 2009. He also stated that 77 percent of SSPs reflected the actual system deployed based on DSS's on-site inspections. Mr. Farley stated that 18 percent of the 23 percent of the SSPs with discrepancies were minor errors. For example, password length was only eight characters, but the requirement was for 12 characters. The remaining 5 percent were "significant" discrepancies that could not be resolved during the on-site inspection. Mr. Farley stated that once an on-site inspection is completed without significant discrepancies, the IATO is superseded by an Approval to Operate, which is valid for three years. He stated that there has been a recent increase in the rejection of SSPs, which could be a result of a majority of the Information System Security Professionals attending training, which meant few systems were being reviewed for an IATO. Richard Engel, Industry, asked if problems on a particular information system reflect the overall status of the information system program. Richard Lawhorn, DSS, stated that usually it is not a reflection of the overall program.

## IV. New Business

The Chair stated that the review of Executive Order 12958, as amended, "Classified National Security Information," (the Order) and Controlled Unclassified Information (CUI) policy had largely concluded. The Chair stated that an interagency group met with regard to the Order, and the draft revisions to the Order were in final coordination.

The Chair stated that the NISPPAC Charter has been renewed and the bylaws will require further amendment. The Chair stated that through the FACA review process, which is managed by the General Services Administration (GSA), it was determined that the Chair should not serve as the Designated Federal Officer (DFO) of the NISPPAC. The new DFO will be Mr. Pannoni and the alternate DFO will be David Best, ISOO. An updated version of the bylaws to reflect this change will be provided to the members and subsequently a vote will be taken.

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

The Chair stated that he would send a letter to the heads of Government agencies requesting appointment letters designating their Government representative to the NISPPAC. He stated that if a response has not been received by the next NISPPAC meeting, the Government agency would be downgraded to "Observer" status. The Chair requested that members respond within the next two weeks with contact information and courtesy copy information.

The Chair moved discussion on to the October 1, 2012, deadline for discontinuing the use of non-GSA approved security containers for the storage of classified information, and stated that ISOO received a letter from Congress on the issue. The Chair stated that ISOO sent out a letter to executive branch agencies and Industry to gather preliminary data on non-GSA approved containers still in use. The Chair stated that since the NISPPAC has been requested by Congress to assist in ensuring the transition to GSA-approved containers, a new ad hoc working group would be created to address the issue. The Chair yielded to Stan Sims, DoD, and Mr. Jarvie for comments. Mr. Sims commented that the requirement was for both Industry and executive branch agencies. Mr. Jarvie commented that he looked forward to seeing accurate data generated by Industry on the number of containers needing to be replaced. The Chair thanked both members for their comments and stated that there needs to be full cooperation and coordination to ensure the 2012 deadline is met.

The Chair introduced Mr. Lewis and Greg Torres, DoD, for the DoD update.

**A) DoD Update**

Mr. Lewis and Mr. Torres provided the update. Mr. Lewis discussed FOCI mitigation and the development of a material change matrix. He mentioned the NISPOM update and stated that a meeting regarding Industry's input was conducted. He stated that DoD would work with the cognizant security agencies of the NISP and ISOO in addressing the changes to the NISPOM. Mr. Lewis yielded to Mr. Torres for the remainder of the update.

Mr. Torres thanked Mr. Lewis and the Chair and stated that at the last Aerospace Industry Association meeting, he observed that Industry was having difficulties in filling positions that required a security clearance. Mr. Torres discussed the "Wounded Warrior" program as a means to increase the supply of cleared professionals. He stated that the program has received positive feedback and targets specific categories of veterans to assist in the workforce. He stated that presently Lieutenant General James Clapper, USAF, Ret., DoD, is proceeding with a memo changing policy regarding clearance investigations and separation from service for wounded warriors. The program is entitled "Operation Warfighter", and General Clapper wants agencies to sponsor a Wounded Warrior. Mr. Torres stated that the program also wants Industry to become involved by reviewing their unfilled positions that require a Top Secret security clearance with SCI access. The Government would then assess whether there is a wounded veteran in the local area who can do the job. Mr. Torres reiterated that the program definitely would like Industry's assistance and support.

**B) Committee on National Security Systems (CNSS) – Intelligence Community Certification and Accreditation (C&A) Transformation**[3]

Mr. Caslow provided a presentation on the C&A Transformation of Government information systems. Mr. Caslow presented the three strategies and the seven transformational goals of the Government for the change of the C&A of information systems. Mr. Caslow stated that the change would become a holistic risk approach. Mr. Caslow stated that National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 is the risk management approach, and NIST SP 800-39 is the executive risk function. Mr. Lewis commented on the NISPOM that DoD's rewrite would be consistent and point towards the CNSS and NIST policy documents.

**C) Industry Update**[4]

Mr. Jarvie presented the Industry update. Mr. Jarvie thanked all the presenters of working group updates for the hard work accomplished by each. Mr. Jarvie stated that the NISPOM listening session was successful and that Industry delivered a substantial amount of comments and suggestions with regard to the proposed NISPOM changes. Mr. Hudson stated that he had finished prioritizing the suggested NISPOM changes. Mr. Jarvie presented Industry's top concerns, which were Information Sharing-Threat, CUI, FOCI, PCL processing, and C&A. He stressed the necessity of having policy matter experts involved for the success of working groups. He stated that Information Sharing-Threat was the most important initiative and concern of Industry, especially with regard to the secure communication systems and how to address the threat to information systems from data compromise and attack. He also expressed thanks to the Federal Bureau of Investigation and collaboration on access to the Secure Internet Protocol Router Network "SIPRNet".

**D) NISP Signatories Update**

No updates were reported.

**E) General Forum and Open Discussion**

No items were discussed.

## V. Closing Remarks and Adjournment

The Chair expressed his sincere thanks to all the members and staff of the NISPPAC and its working groups for all of the hard work completed. The Chair stated that March 24, 2010, July 21, 2010, and November 17, 2010 were the dates for the next three NISPPAC meetings. The meeting was adjourned at 12:12 p.m.

**Summary of Action Items**

[3] See appendix 4 for Mr. Caslow's presentation.
[4] See appendix 5 for Mr. Jarvie's presentation.

**A) The Chair stated that there was a request to examine how to better support smaller companies. There are two options: (1) use one of the three NISPPAC meetings as a focus meeting for small company solutions and solicit issues of concern from small companies; or (2) hold a NISPPAC meeting outside of the Washington DC area to create greater involvement from smaller companies. The Chair stated that these two options would be pursued within the provisions of the FACA.**

**B) The Chair stated that the NISPPAC Charter has been renewed and the bylaws will require further amendment. The Chair stated that through the FACA review process, which is managed by the General Services Administration, it was determined that the Chair should not serve as the Designated Federal Officer (DFO) of the NISPPAC. The new DFO will be Mr. Pannoni, and the alternate DFO will be David Best, ISOO. An updated version of the bylaws to reflect this change will be provided to the members and subsequently a vote will be taken.**

**C) The Chair stated that he would send a letter to the heads of Government agencies requesting appointment letters designating their Government representative to the NISPPAC. He stated that if a response has not been received by the next NISPPAC meeting, the Government agency would be downgraded to "Observer" status. The Chair requested that members respond within the next two weeks with contact information and courtesy copy information.**

**D) The Chair stated that a new ad hoc working group would be formed to address the issue of non-GSA approved containers still in use by Government and Industry and their plans for ensuring that the October 1, 2012, deadline for discontinuing the use of these containers is met.**

**List of Appendices**

Appendix 1 – Ms. Smith's PCL Working Group Report Presentation
Appendix 2 – Ms. Branch's PCL Working Group Report Presentation
Appendix 3 - Mr. Farley's Certification and Accreditation Working Group Report Presentation
Appendix 4 - Mr. Caslow's Intelligence Community Certification and Accreditation (C&A) Transformation Presentation
Appendix 5 - Mr. Jarvie's Combined Industry Update Presentation

Appendix 1
Ms. Smith’s PCL Working Group Report Presentation

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

## Reported Clearance Decisions Made During the 3rd Qtr FY 09

- All levels of Initial clearances – 30,260 cases average 106 days End-to-End time (Initiation through Adjudication)
  - Fastest 80% average 70 days
  - Fastest 90% average 77 days

    – Top Secret Initial – All 6,564 cases: 134 day average cycle time
      - » Fastest 80% average 100 days
      - » Fastest 90% average 107 days

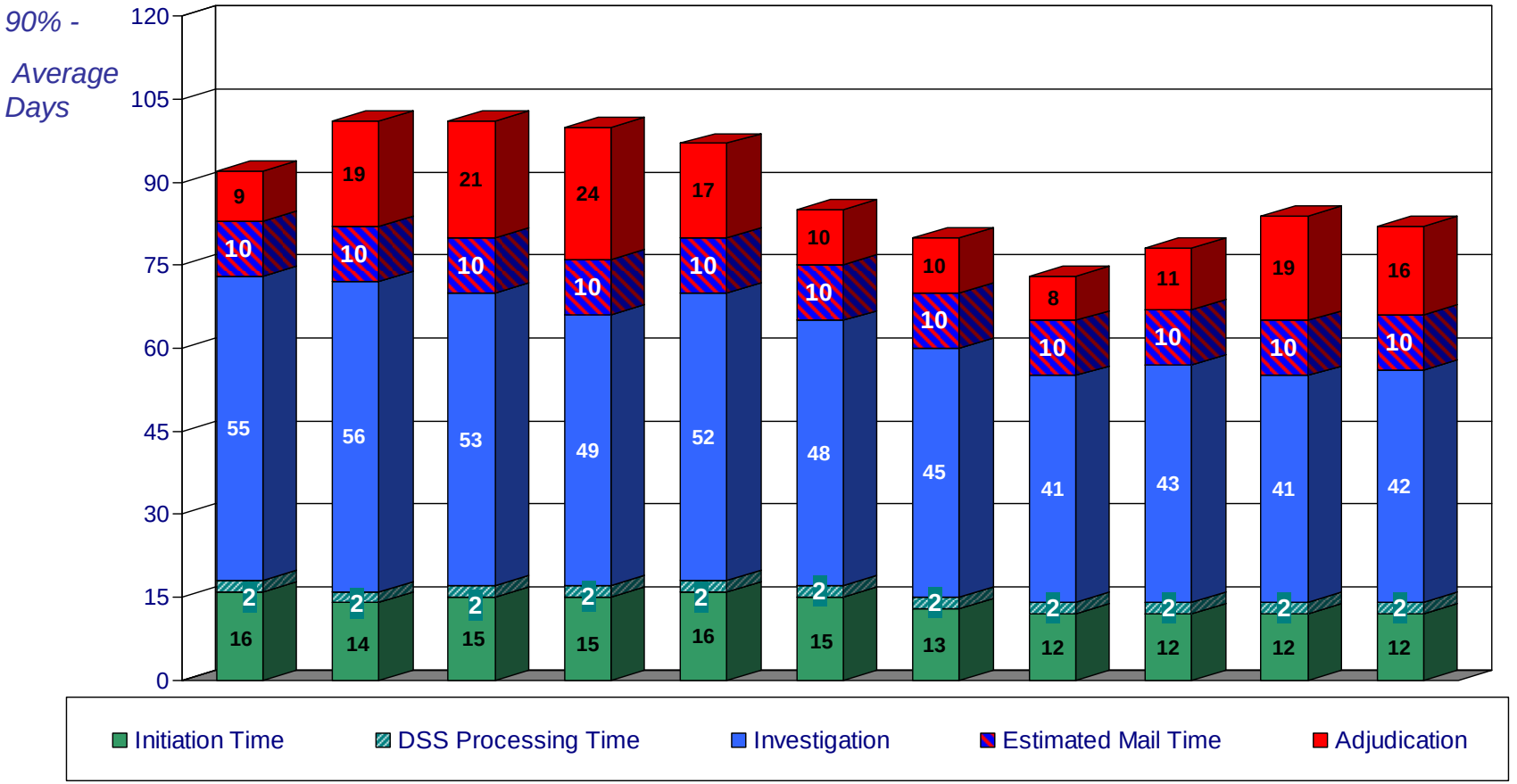
    – All Secret/Conf – All 23,696 cases: 98 day average cycle time
      - » Fastest 80% average 62 days
      - » Fastest 90% average 69 days

- TS Periodic Reinvestigation – All 5,965 cases: 163 day average cycle time
  - Fastest 80% average 111 days
  - Fastest 90% average 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

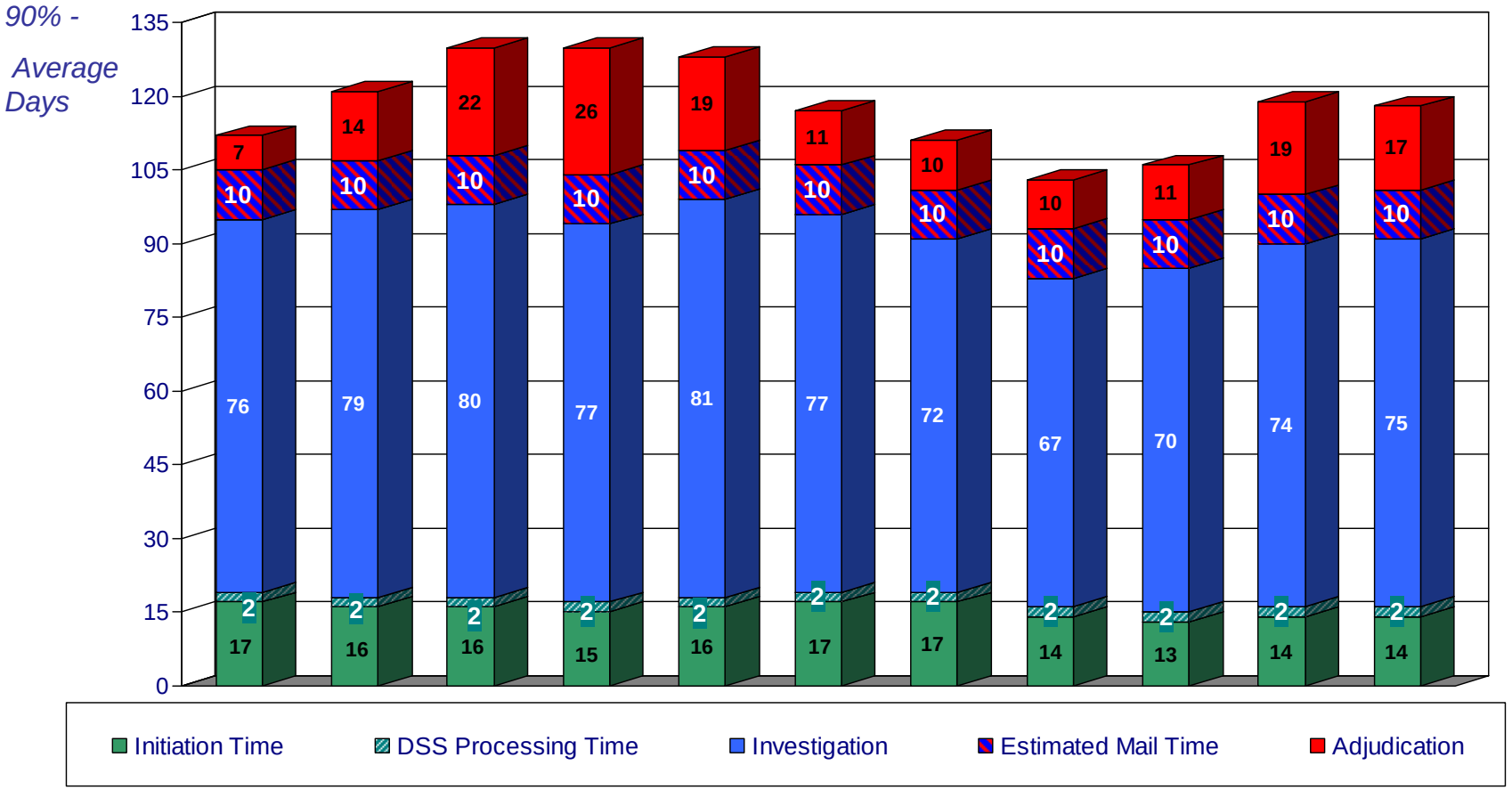
# Industry's Average Timeliness Trends for 90% Initial Top Secret and All Secret/Confidential Security Clearance Decisions




| Adjudications actions taken: | Oct 08 | Nov 08 | Dec 08 | Jan 09 | Feb 09 | Mar 09 | Apr 09 | May 09 | Jun 09 | Jul 09 | Aug 09 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 100% of Reported Adjudications: | 11,868 | 6,741 | 9,208 | 10,318 | 9,875 | 12,957 | 10,577 | 10,059 | 9,470 | 9,582 | 10,324 |
| Average Days for the fastest 90% | 92 days | 101 days | 101 days | 100 days | 97 days | 85 days | 80 days | 73 days | 78 days | 84 days | 82 days |

Slide has been updated with reported adjudicative decisions made during March 09 through August 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 may not be included in the above metrics

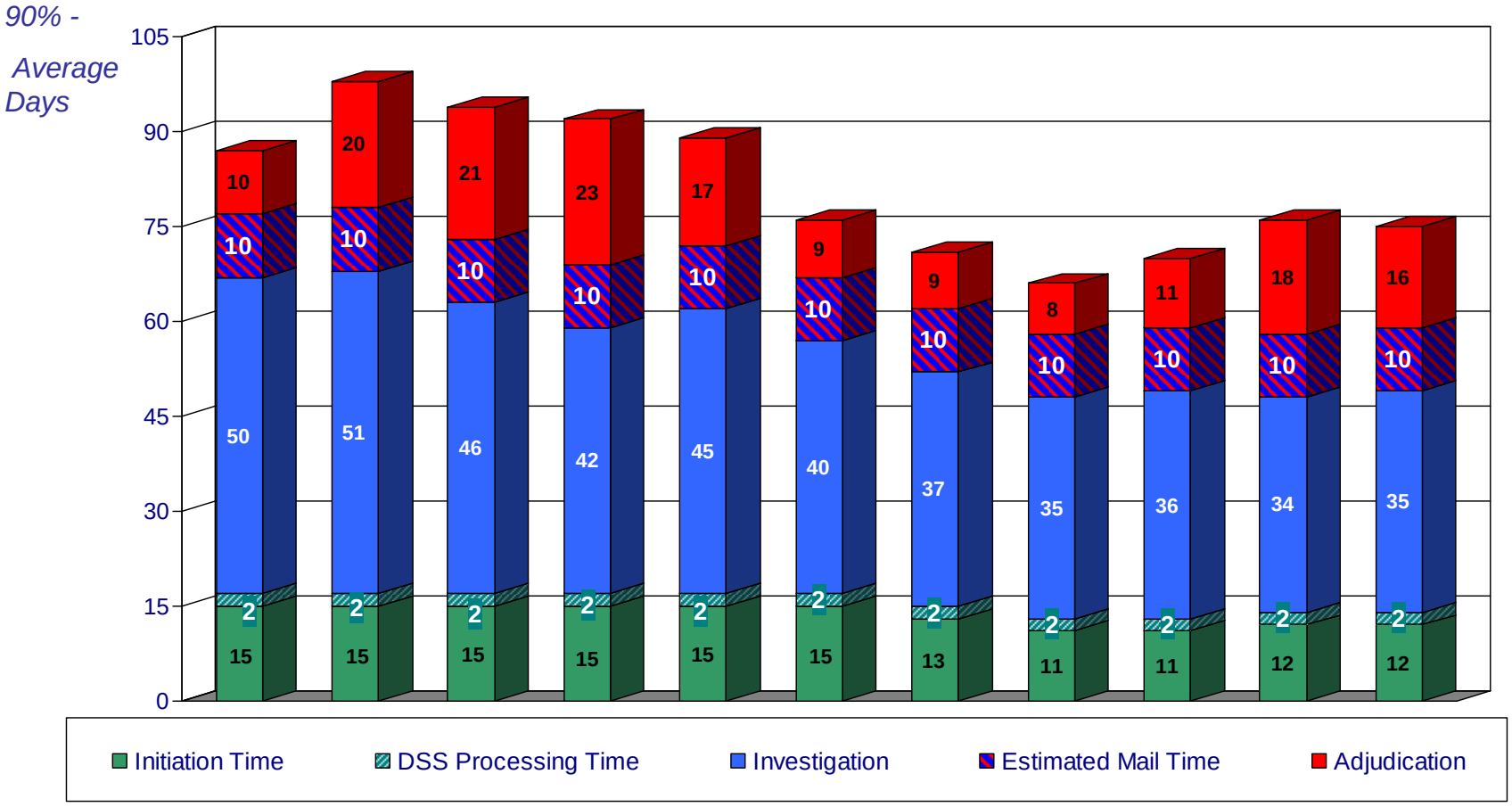
# Industry's Average Timeliness Trends for 90% Initial Top Secret Security Clearance Decisions




| Adjudications actions taken: | Oct 08 | Nov 08 | Dec 08 | Jan 09 | Feb 09 | Mar 09 | Apr 09 | May 09 | Jun 09 | Jul 09 | Aug 09 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 100% of Reported Adjudications: | 2,450 | 1,086 | 1,778 | 2,231 | 2,134 | 3,092 | 2,409 | 2,136 | 1,998 | 1,873 | 1,936 |
| Average Days for the fastest 90% | 112 days | 121 days | 130 days | 130 days | 128 days | 117 days | 111 days | 103 days | 106 days | 119 days | 118 days |

Slide has been updated with reported adjudicative decisions made during March 09 through August 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 may not be included in the above metrics

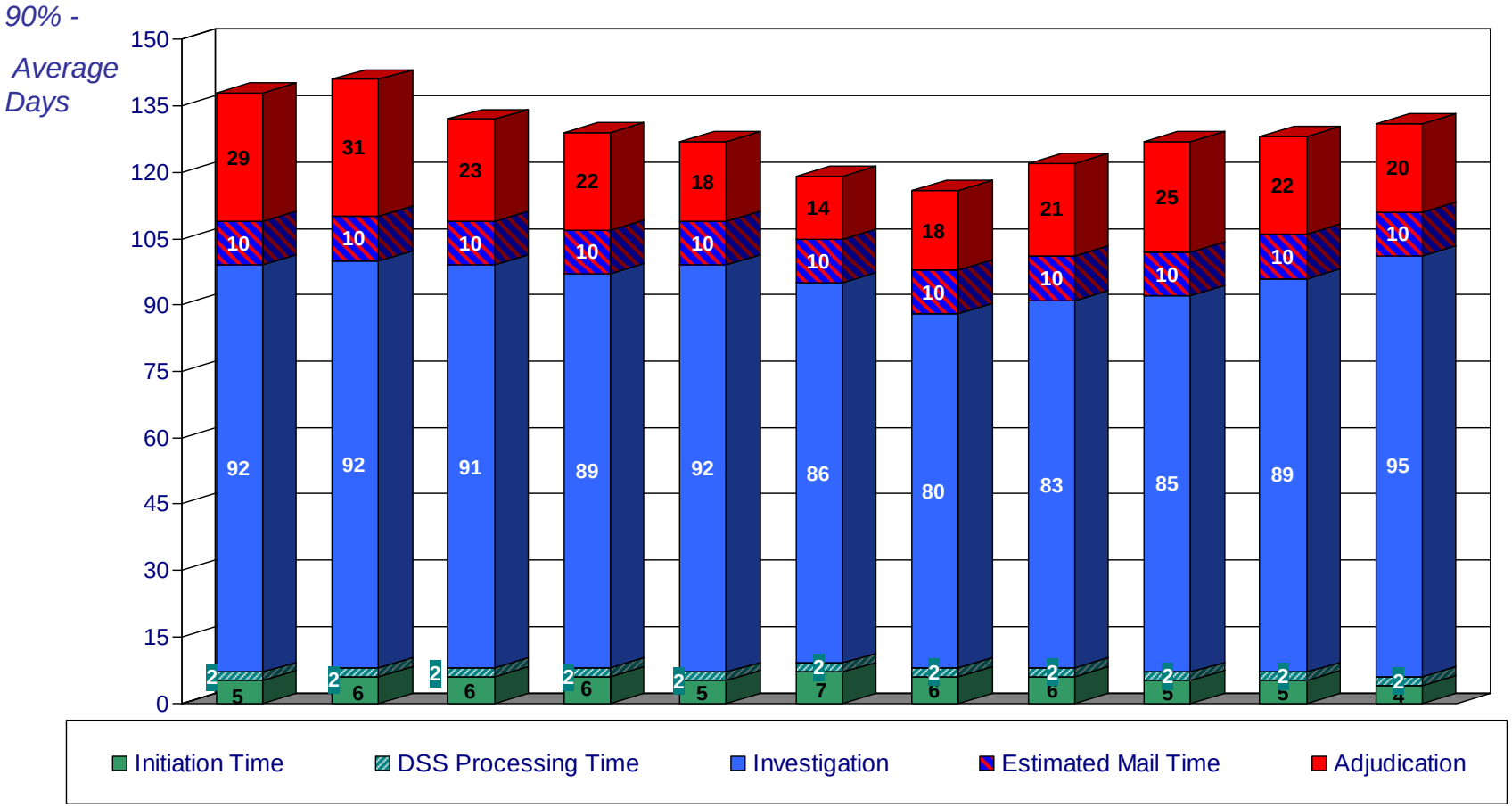
# Industry's Average Timeliness Trends for 90% Secret/Confidential Security Clearance Decisions




| Adjudications actions taken: | Oct 08 | Nov 08 | Dec 08 | Jan 09 | Feb 09 | Mar 09 | Apr 09 | May 09 | Jun 09 | Jul 09 | Aug 09 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 100% of Reported Adjudications: | 9,418 | 5,655 | 7,430 | 8,087 | 7,741 | 9,865 | 8,168 | 7,923 | 7,472 | 7,709 | 8,388 |
| Average Days for the fastest 90% | 87 days | 98 days | 94 days | 92 days | 89 days | 76 days | 71 days | 66 days | 70 days | 76 days | 75 days |

Slide has been updated with reported adjudicative decisions made during March 09 through August 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 may not be 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 | Jul 09 | Aug 09 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 100% of Reported Adjudications: | 4,471 | 2,252 | 3,116 | 3,408 | 3,070 | 3,729 | 2,210 | 1,891 | 1,812 | 1,989 | 2,063 |
| Average Days for the fastest 90% | 138 days | 141 days | 132 days | 129 days | 127 days | 119 days | 116 days | 122 days | 127 days | 128 days | 131 days |

Slide has been updated with reported adjudicative decisions made during March 09 through August 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 may not be included in the above metrics

Appendix 2
Ms. Branch’s PCL Working Group Report Presentation

# DISCO

## FY09 ADJUDICATION INVENTORY

| CASE TYPE | FY 08 | | | | FY 09 | | | | FY09 Delta Q1FY09 vs July 09 |
|---|---|---|---|---|---|---|---|---|---|
| | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Jul-09 | |
| NACLC | 11,449 | 488 | 240 | 1,953 | 4,721 | 1,815 | 4,187 | 4,995 | 6% |
| SSBI | 9,337 | 5,625 | 30 | 354 | 1,448 | 634 | 1,102 | 1,487 | 3% |
| SSBI-PR | 4,899 | 3,752 | 5,973 | 757 | 974 | 340 | 756 | 1,089 | 12% |
| Phased PR | 8,945 | 4,923 | 4,210 | 330 | 1,690 | 495 | 346 | 452 | -73% |
| TOTAL PENDING | **34,630** | **14,788** | **10,453** | **3,394** | **8,833** | **3,284** | **6,391** | **8,023** | **-9%** |

**Overall reduction of 9% for NACLC, SSBI, SBPR and Phased PR case types from 1Q FY09 to July 09.**

Source: DISCO Manual Counts

# INDUSTRY CASES AT OPM

## FY09 INVESTIGATION INVENTORY

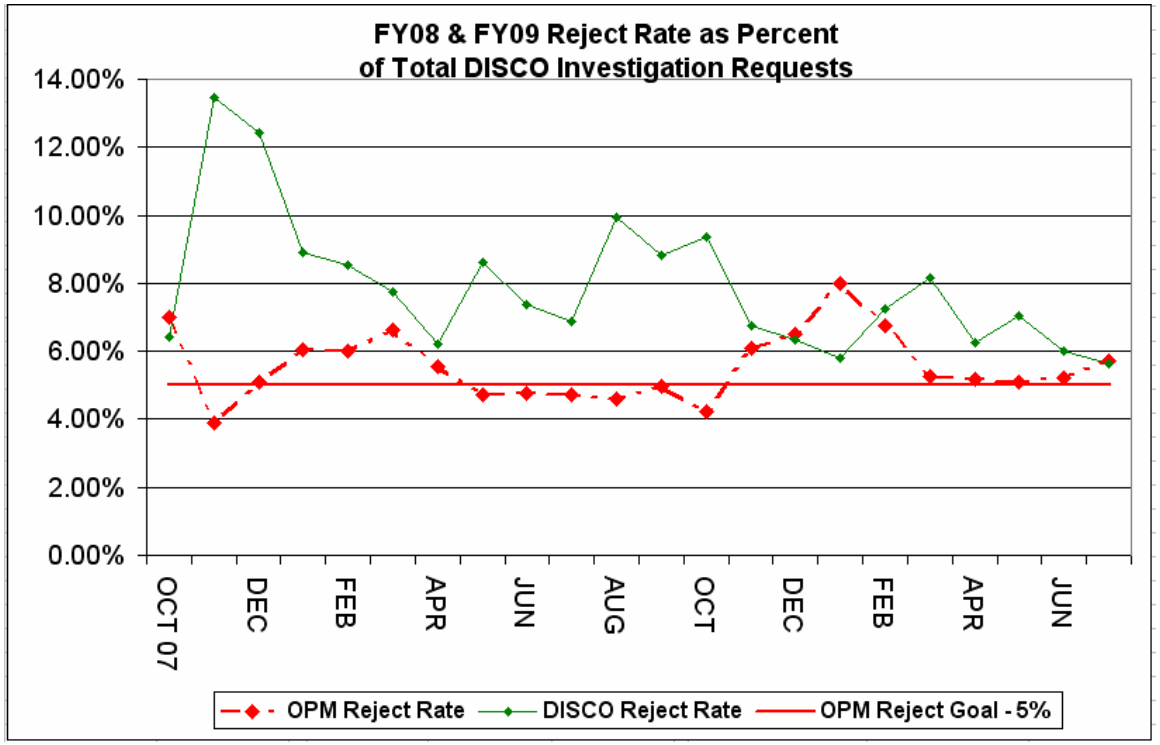
| Case Type | FY 08 | | | | FY 09 | | | | FY09 Delta Q1 vs July 09 |
|---|---|---|---|---|---|---|---|---|---|
| | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Jul-09 | |
| NACLC | 29,575 | 25,085 | 22,077 | 15,561 | 13,209 | 13,982 | 13,900 | 13,523 | 2% |
| SSBI | 14,110 | 8,796 | 7,404 | 6,720 | 6,626 | 6,687 | 6,944 | 6,968 | 5% |
| SSBI-PR | 11,761 | 9,943 | 5,639 | 4,167 | 3,772 | 4,160 | 4,692 | 4,308 | 14% |
| Phased PR | 7,711 | 7,749 | 6,734 | 6,408 | 5,430 | 2,771 | 2,476 | 2,723 | -50% |
| **TOTAL PENDING** | **63,157** | **51,573** | **41,854** | **32,856** | **29,037** | **27,600** | **28,012** | **27,522** | **-5%** |

**Overall reduction of 5% for NACLC, SSBI, SBPR and Phased PR case types from Q1 FY09 to July 09.**

Source: OPM Customer Support Group

# QUARTERLY REJECT RATES

(Initial & Periodic Reinvestigation Requests)




- **FY09 (As of July 31): DISCO received 141,195 investigation requests**
  - **Rejects -** Total of **19,276 (13.6%)** of incoming investigation requests rejected back to FSOs
    - DISCO rejected **11,168 (7.9%)** investigation requests to FSOs for re-submittal
    - OPM rejected **8,108 (5.7%)** 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.
- **Note – To further reduce NISP PSI request rejections, DSS will be publishing an updated *"Applicant Tips for Successful e-QIP Submission"* to the DSS.mil JPAS site as well as directly emailing the handout to facilities with a high rate of rejection.**



Source: JPAS / OPM IRTPA Monthly Reports

# FY09 INDUSTRY CLEARANCE SUBMISSIONS VS PROJECTIONS

- OMB performance goal is +/- 5%
  - July '09 Status: At the close of July, Industry clearance submissions were 2.3% below overall Industry/DSS projections.

| FY09 Projection | Weekly Projected | Year to Date | % of Projection |
|---|---|---|---|
| 182,315 | 3,506 | 3,425 | 97.7% |

Appendix 3
Mr. Farley's Certification and Accreditation Working Group Report Presentation

**Defense Security Service**

# Industrial Security Field Operations Office of the

# Designated Approving Authority (ODAA)

September 2009

# Defense Security Service

Overview

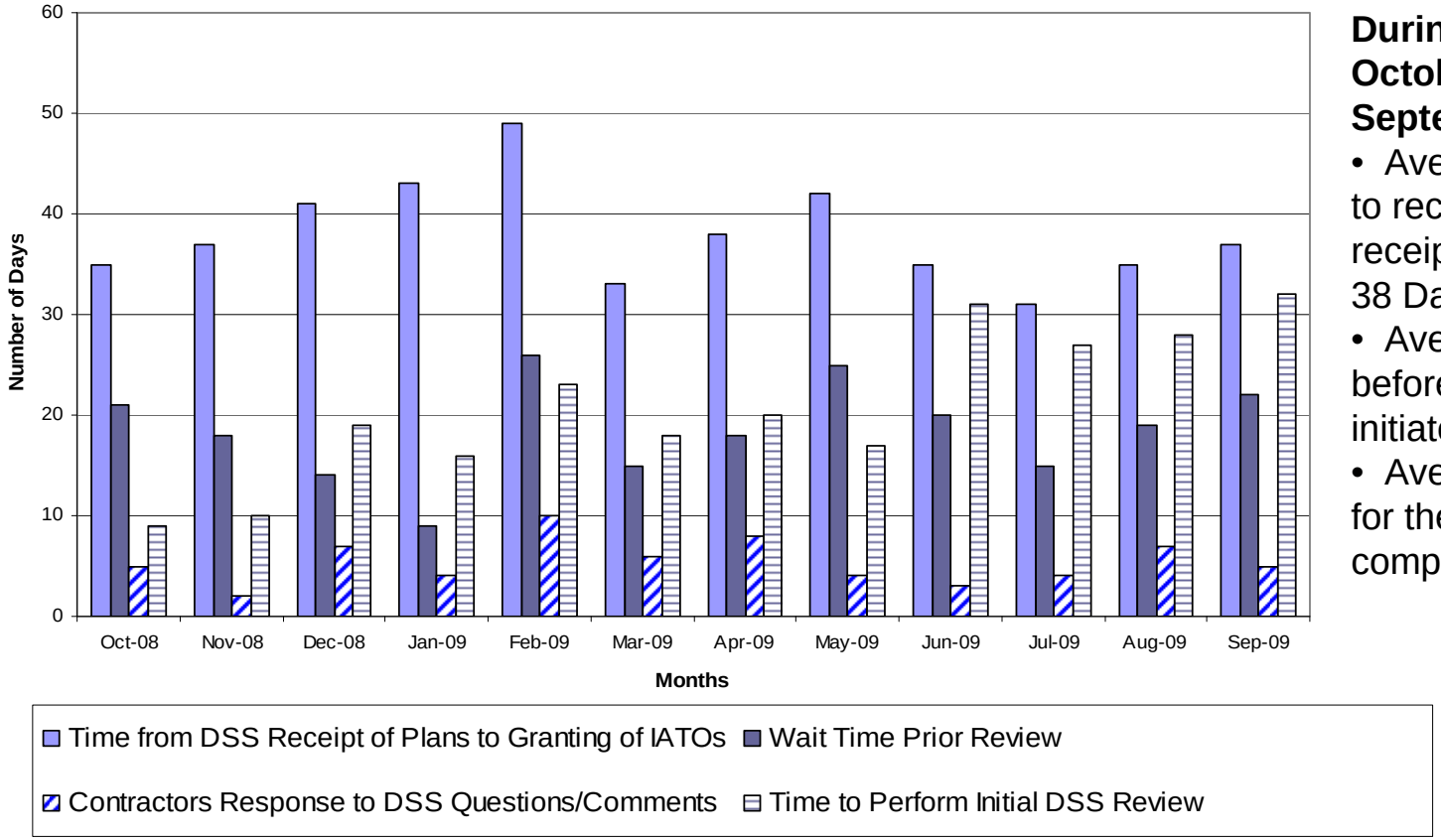
- Certification & Accreditation (C&A)
- C&A Metrics

# 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

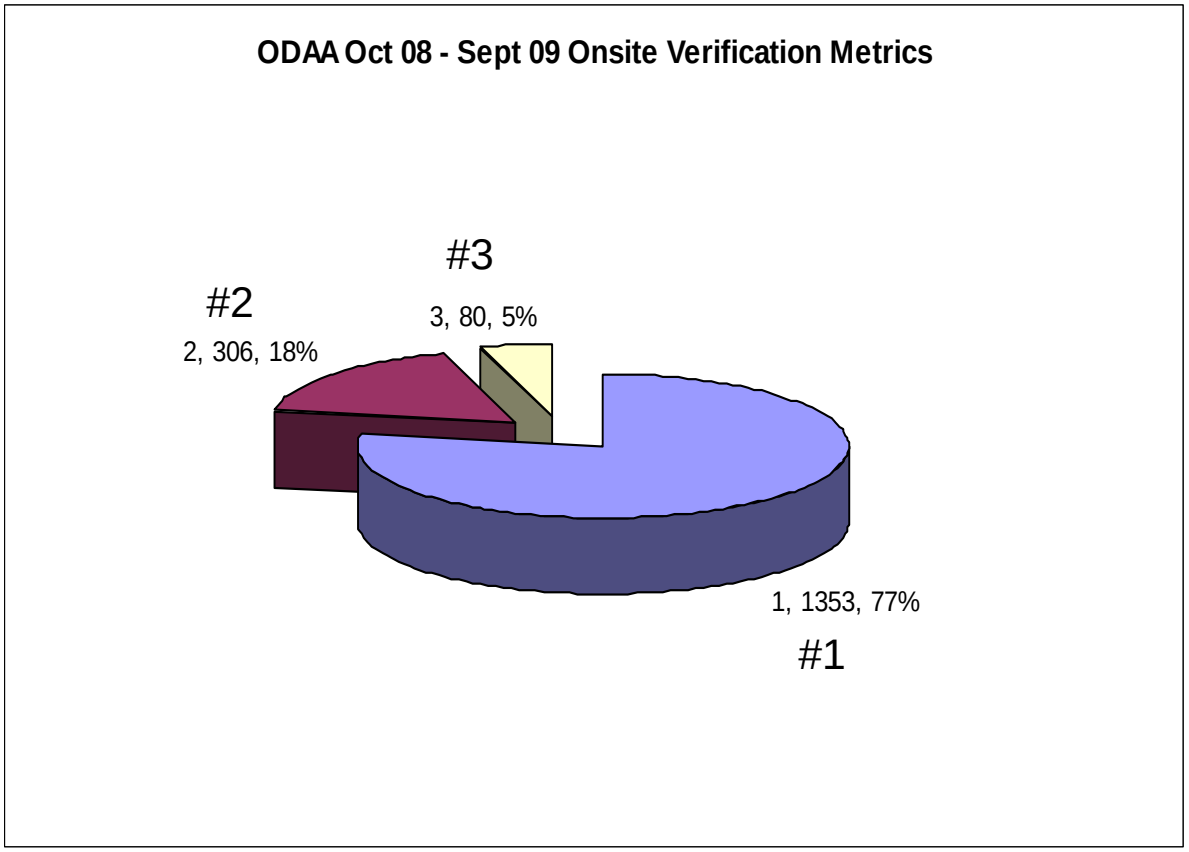



**During the Past Year October 2008 – September 2009**

- Average number of days to receive an IATO after receipt of a submission is 38 Days
- Average waiting time before a review process is initiated is 19 Days
- Average number of days for the review time to be completed is 21 Days

# ODAA Metrics and Organization

## On-site Verification Stats (18% Required Some Level Modifications)



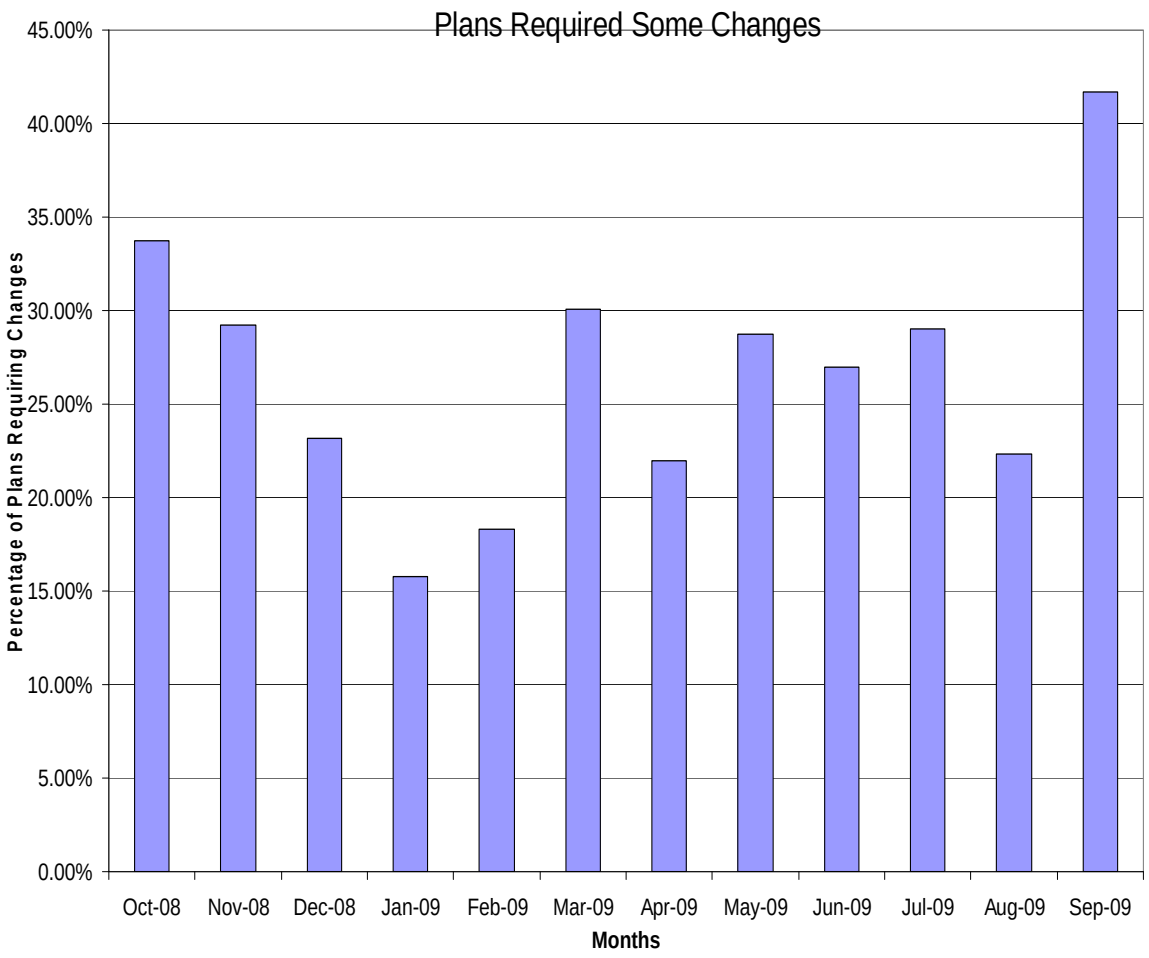

#1. No discrepancies discovered during on-site validation.

#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

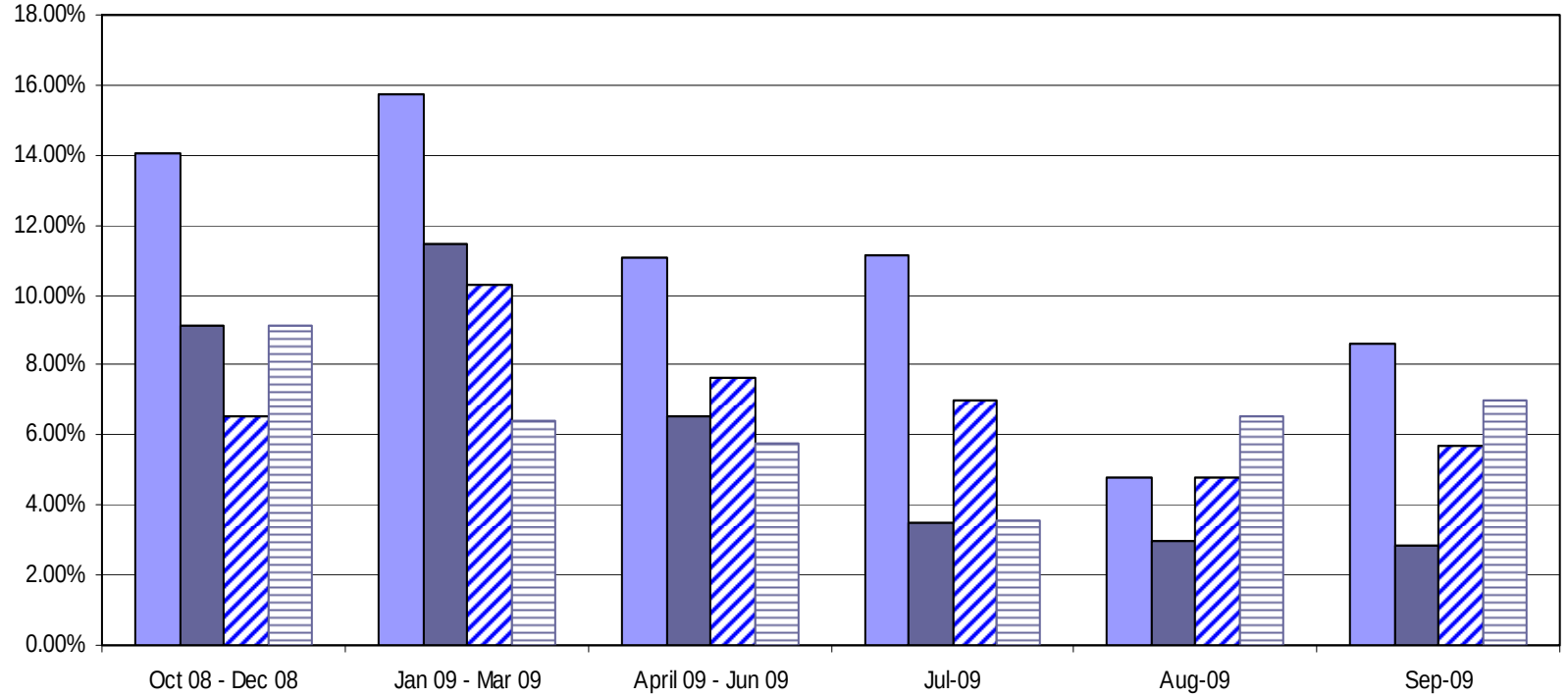
Review Questions and/or Comments, Errors and Corrections Noted



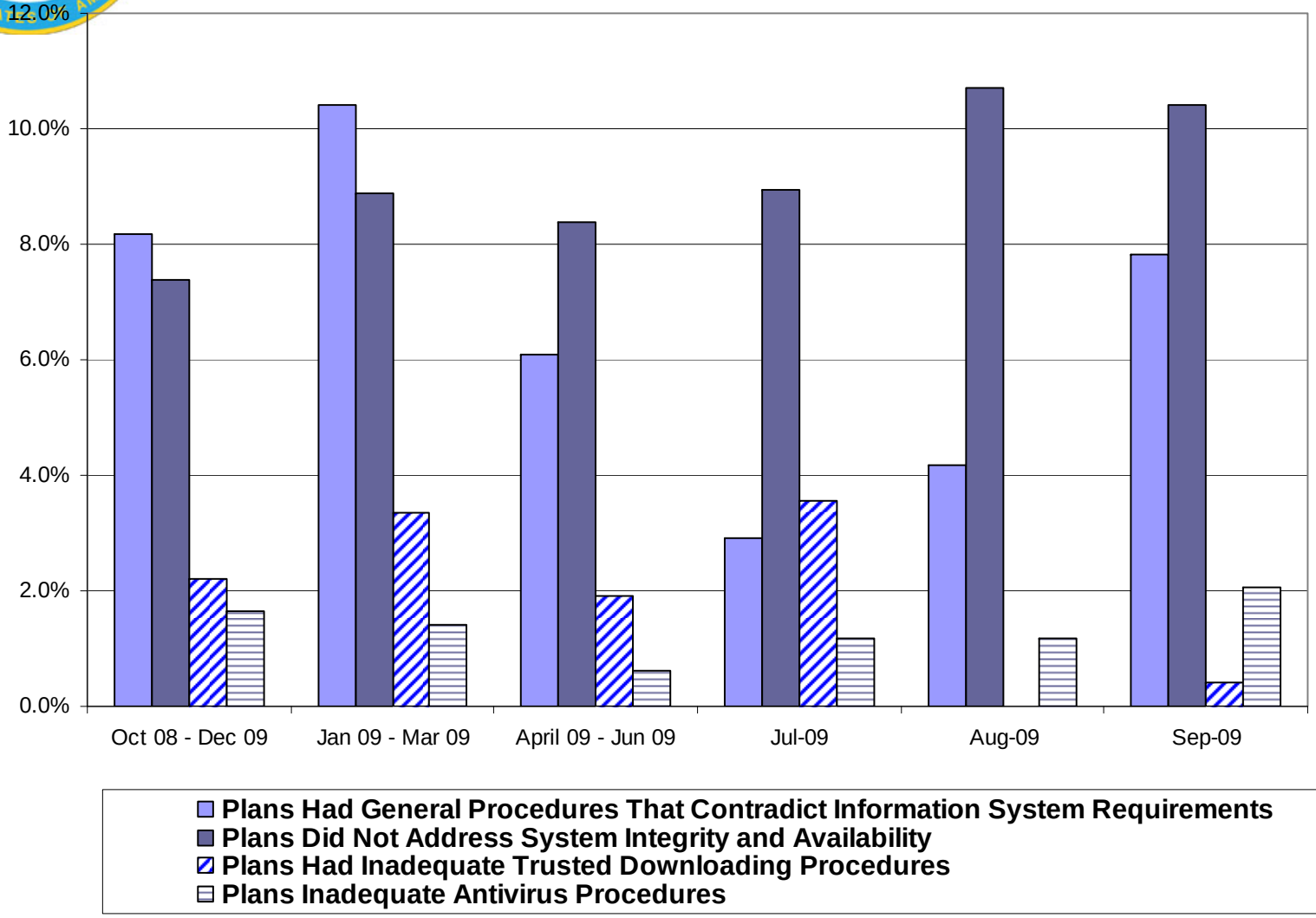

Of the 1799 plans received from Oct 08 – Sept 09:

- On average 26.7 % of all plans submitted required changes prior to the On-site Verification for ATO

# ODAA Metrics
# Security Plan Reviews Common Errors
# Part One

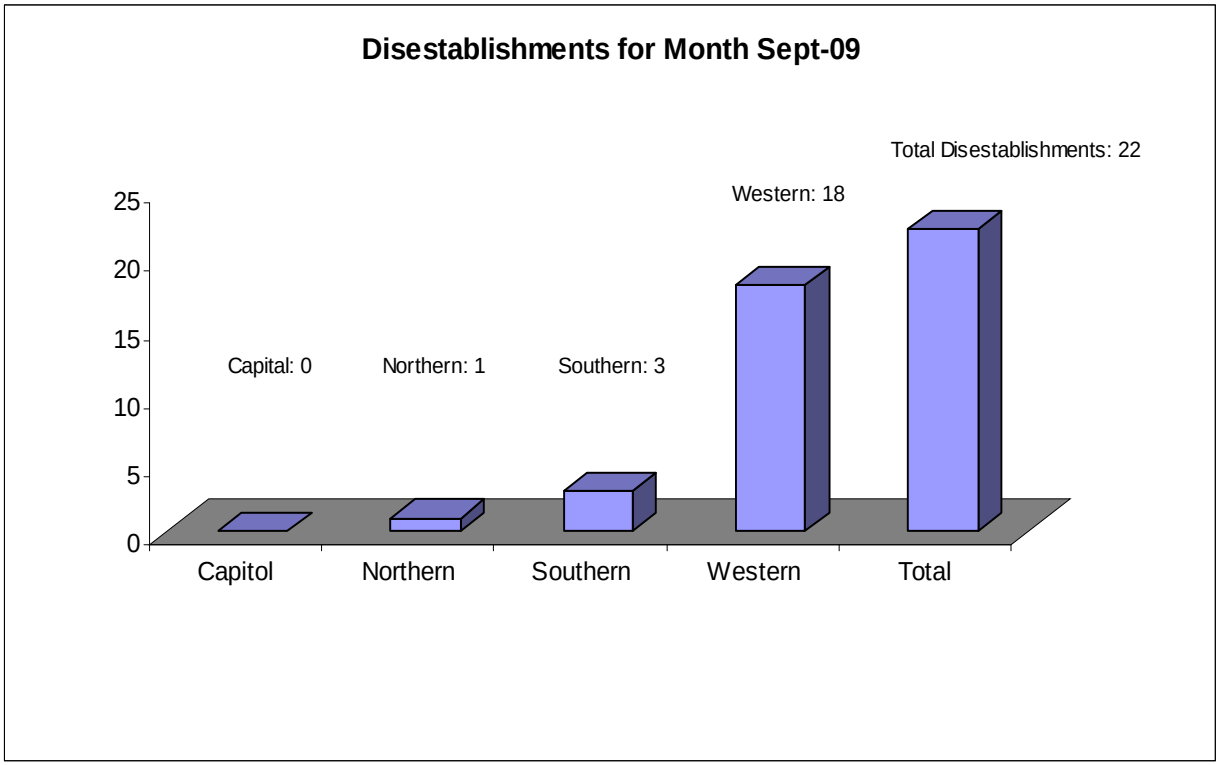


# ODAA Metrics
# Security Plan Reviews Common Errors
# Part Two



# ODAA Metrics and Organization

## Disestablishments for Month of Aug-09




Total Disestablishments for the month of Sept-09 were 22.

Capital Disestablishments for Month of Sept-09 were 0 or 0%

Northern Disestablishments for Month of Sept-09 were 1 or 4.54%

Southern Disestablishments for Month of Sept-09 were 3 or 13.63%

Western Disestablishments for Month of Sept-09 were 12 or 81.81%

*"No accreditation was revoked for cause during the month of August 2009."

Appendix 4
Mr. Caslow's Intelligence Community Certification and Accreditation (C&A) Transformation Presentation

# Intelligence Community Certification and Accreditation Transformation

Connect. Integrate. Collaborate.

## Certification and Accreditation/Risk Management Program

**IC CIO**

**Intelligence Community Information Assurance**

# The Bottom Line

- **The Intelligence Community is working towards an *innovative* and *efficient* way to perform Security Authorization (also known as Certification and Accreditation (C&A)) across the *National Security Community*, establishing a single approach by:**
  - Converging parallel efforts across the Federal Government
  - Leveraging partnerships

- **We are working to ensure our approach is integrated with current activities and supported by:**
  - Committee on National Security Systems (CNSS)
  - Department of Defense (DoD)
  - National Institute of Standards and Technology (NIST)
  - OMB Information Systems Security Line of Business (ISS LOB)
  - Program Manager-Information Sharing Environment (PM-ISE)
  - Unified Cross Domain Management Office (UCDMO)

# Strategy

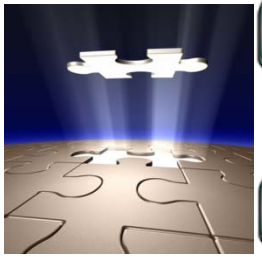
- **Incorporate security throughout the lifecycle**
- **Standardize the process and procedures**
- **Achieve reciprocity and reuse of documentation**

# Transformation Goals

- Establish a common set of trust levels
- Achieve reciprocity
- Define, document, and adopt common security controls
- Develop a common language for efficient communication among security professionals, program managers, developers, and acquisition officials
- Manage risk from an overall enterprise perspective addressing mission and budget as well as security
- Incorporate Information Assurance (IA) into enterprise architecture and deliver IA services as enterprise services
- Build security into the "lifecycle" so that it becomes adaptable to different development environments.

# Foundational Changes

## STRATEGY



| | | |
|---|---|---|
| Risk Management | System | Enterprise |
| Governance | Passive/Intuitive | Active and repeatable |

## PROCESS

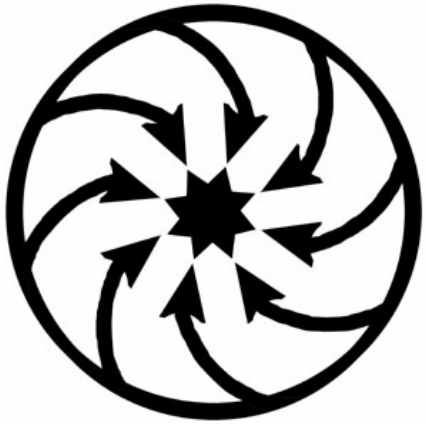
| | | |
|---|---|---|
| Standards and Guidelines | Inability to capture security-related costs | Integration and tracking of security costs |
| Budget | Multiple sets | Single set |
| Adaptability | Inflexible | Flexible |

## PEOPLE

| | | |
|---|---|---|
| Roles and Responsibilities | Functional stovepipes | Integrated competencies |
| Leadership | Lack insight | Informed decisions |
| Knowledge | Functional expertise | Broad understanding |

# Unifying Federal Government Efforts

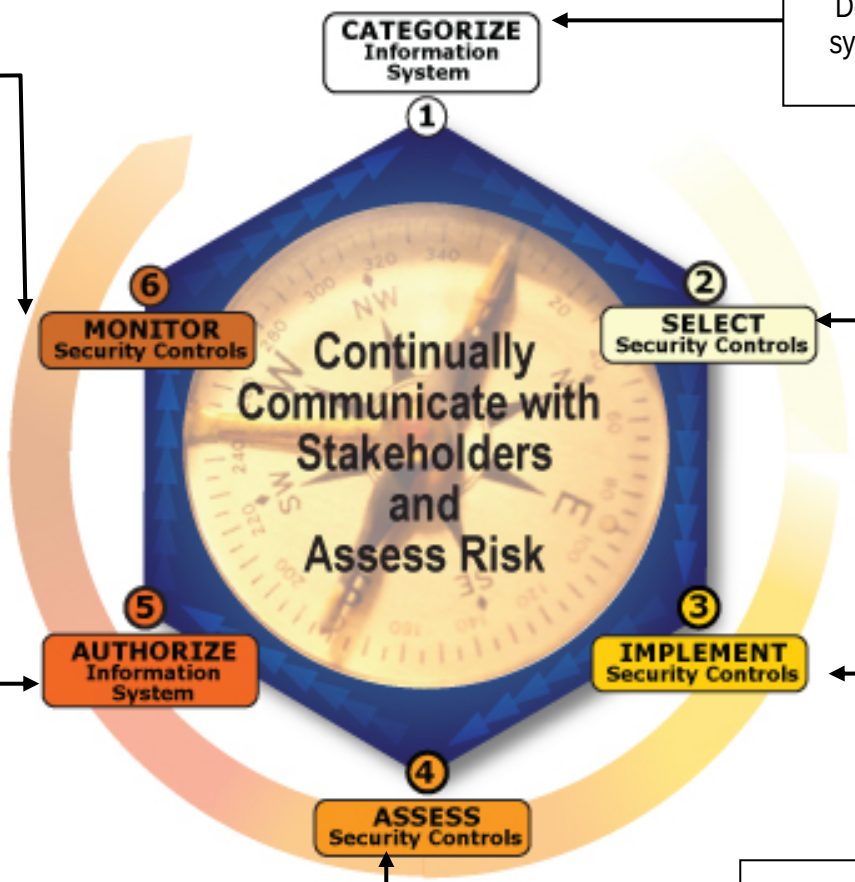
- **Certification and Accreditation is now a part of the Risk Management Framework**
  - Ensures security is built into the system lifecycle (SDLC)
  - Captured in both Civil and National Security-related documentation
- **IC and DoD Chief Information Officers (CIOs) reciprocity and reuse memorandum**
  - Allows DoD and IC entities to accept each other's C&A documentation
  - Reduces needless duplication of work and reformatting of documents
  - Supports mission success by emphasizing content vice format in making security-related decisions
- **NIST, IC, DoD and CNSS are working together**
  - Updating NIST SPs 800-39, 800-37, 800-30, 800-53, 800-53A to formulate a single federal approach
  - Revising the Risk Management Framework to a six step process
- **Program Manager - Information Sharing Environment (PM-ISE)**
  - Partner with IC, DoD
  - Extending work to the state, local, tribal level



# Risk Management Framework (RMF) Application

NIST 800-53A / NIST 800-37 / NIST800-30
Continuously track changes to information system that may affect security controls and reassess control effectiveness

NIST 800-37/ CNSSI 1253
Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.




NIST SP 800-53 / CNSSI 1253
Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk Assessment.

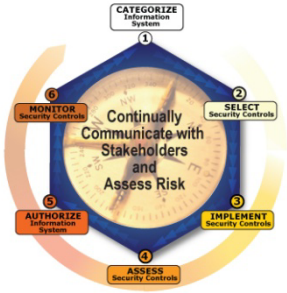
NIST 800-39 / NIST 800-37 / NIST 800-30
Determine risk to organizational operations, assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

NIST SP 800-53A / NIST 800-37
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

NIST 800-37
Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

# Need for New Policies and Guidance

- **Multiple policies for certification and accreditation of information systems among agencies, depending on information classification**
  - Director of Central Intelligence Directive (DCID) 6/3 for Sensitive Compartmented Information (SCI) systems
  - NISPOM, DITSCAP, or DIACAP for non-SCI classified systems
  - NIST for unclassified systems
  - Example: DCID 6/3
    - Different interpretation and implementation by each agency
    - Fixed security requirements, without regard to business/mission
    - Documentation intensive
    - Documentation often redundant among different agencies




- **Interpreting the diversity of requirements and processes across organizations increases the time needed to develop and implement systems**

# Policy Doctrine

## NIST

- Brings the national security community closer to FISMA requirements
- Assists with Inspector General (IG) audits, which are based on NIST standards
- Aligns with rest of Federal Government to support reciprocity

## Develop and use CNSS equivalents or supplements to NIST Publications

- Unifies DoD and Intelligence Community (IC) with common standards and processes
- Incorporates unique needs of national security community

## Craft IC Implementations to address IC unique missions and requirements

- Publication development time
- Use of draft publications
- Establish Intelligence Community Directives (ICD) and Standards (ICS)
- Where necessary, draft Intelligence Community Standard supplements to Federal Information Processing Standards and NIST Special Publications

# Intelligence Community Directive (ICD) 503

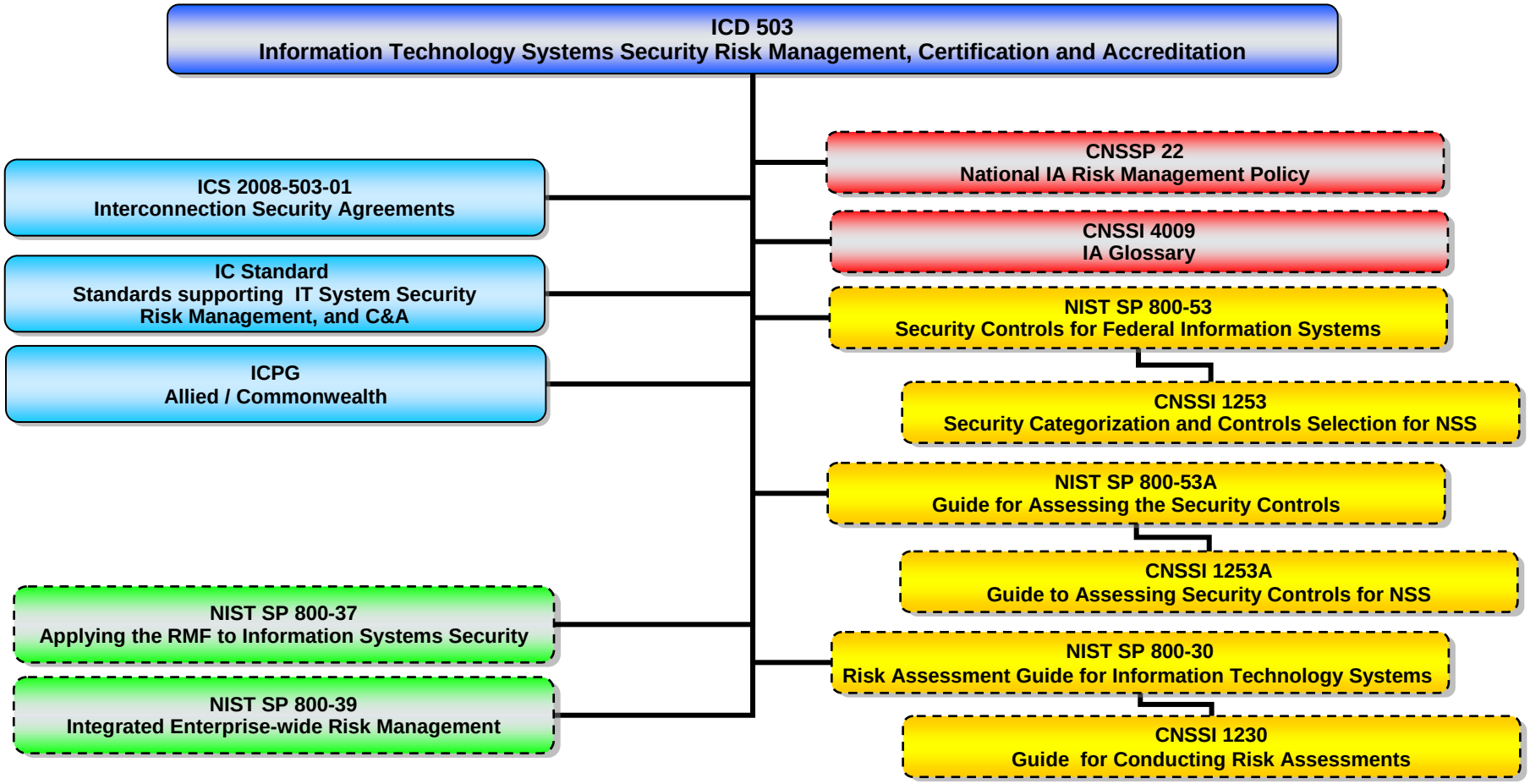
- ***ICD 503 "Information Technology Systems Security Risk Management, Certification and Accreditation"***
  - Signed by the DNI and effective on September 15, 2008
  - Rescinded DCID 6/3 Policy and Manual* and DCID 6/5 Manual
  - Addresses Policy for:
    - Risk Management
    - Accreditation
    - Certification
    - Reciprocity
    - Interconnections
    - Governance and Dispute Resolution

* Note: Appendix E remains in effect

# Key Elements of ICD 503

- Requires IC elements to determine level of acceptable risk based on a holistic perspective that considers Mission, Business and Security requirements
- Applies Consistent Standards for Risk Management
  - Promulgated by the IC CIO
  - Standards to include policies and guidelines approved by NIST and CNSS
- Calls for the application of a common security authorization process and standards for the IC Information Technology Enterprise
- Defines key roles in the C&A Process
  - Authorizing Official (AO)
  - Delegated Authorizing Official (DAO)
  - Certification Agent (CA)

# IC Policy Structure




***Policy architecture now leverages national-level documentation***

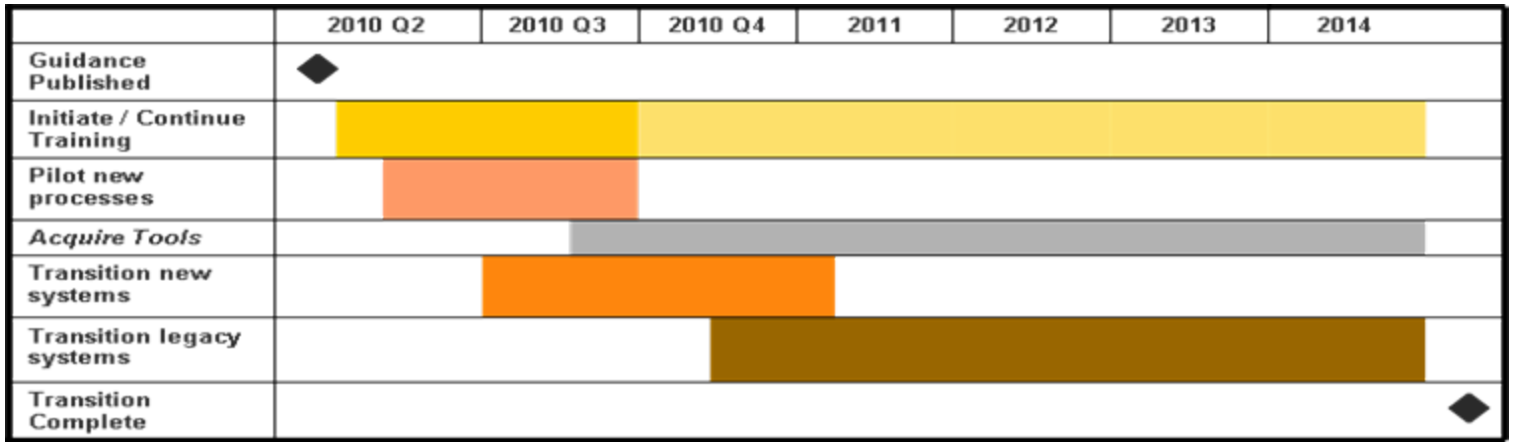
# Concerns on Transition

- C&A Guidance
- Policies/Standards
- Technical Staffing
- Resources
- Transition implementation timelines
- Performance Measures/Milestones
- New Concepts

# Transitioning…

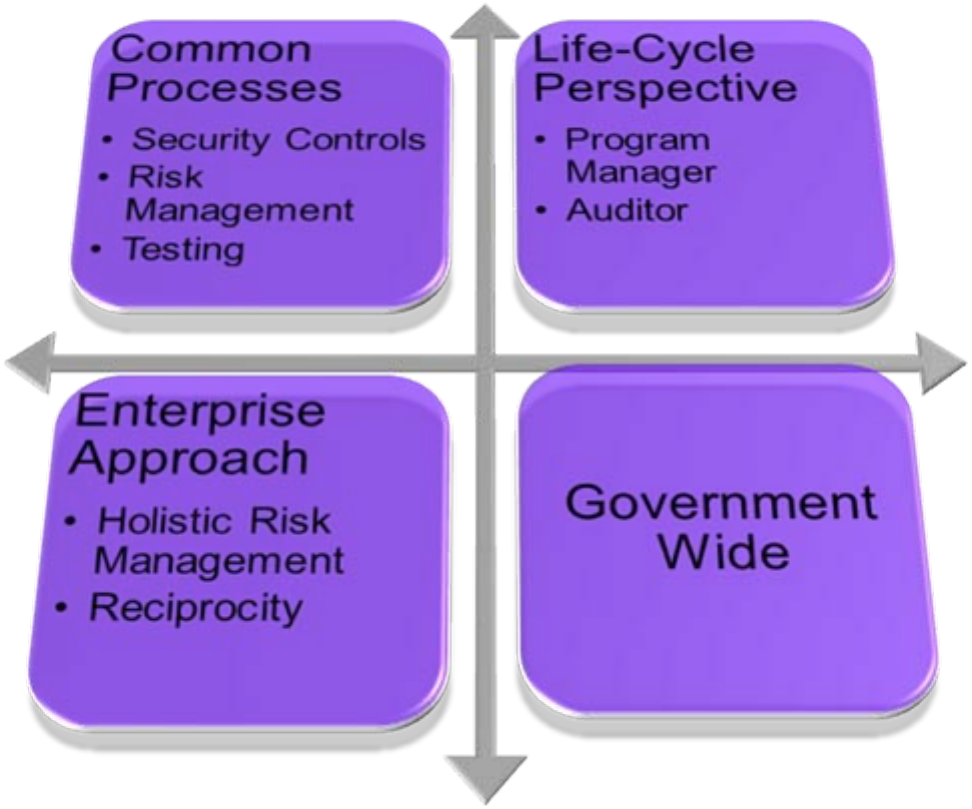
| Status (So What) | Now What | Then What |
|---|---|---|
| Valid accreditation (without liens) under DCID 6/3 that is less than three years old | Accreditation is “grandfathered” | Reaccreditation will be done under provisions of ICD 503 |
| C&A review under DCID 6/3 provisions but not yet accredited | Complete C&A under provisions of DCID 6/3 | Transition to ICD 503 and RMF where re-accreditation activities would normally begin |
| Accredited under DCID 6/3 with conditions (i.e., POA&M included) | Accreditation valid until approval expires or security relevant change triggers re-accreditation activities | Complete the POA&M actions as specified - Transition to ICD 503 for post-accreditation continuous monitoring |
| New system or scheduled for reaccreditation | Conduct certification under provisions of ICD 503 | Conduct certification and accreditation activities in accordance with ICD 503 and RMF methodology |

# Timeline




- **Timeline START begins with publication of ICD 503 implementation documents and assumes April 2010 start date**
- **Initiate Training: START + 2-6 months**
- **Pilot processes: START + 2-6 months (pilot should last approx 6 months)**
- **Transition of new systems (initiation phase of the lifecycle): Pilot + 6 months**
- **Acquire and apply automated tools (START + *availability*)**
- **Transition of legacy systems to ICD 503: Pilot + 3.5 years**
- **Transition complete: START + 4 years**

# *IMPACT…*


Common Processes
• Security Controls
• Risk Management
• Testing
Life-Cycle Perspective
• Program Manager
• Auditor
Enterprise Approach
• Holistic Risk Management
• Reciprocity
Government Wide

# Questions

# Contact Information

- **IC CIO Team:**
  - Roger Caslow, 703-983-3340
  - Jennifer Fabius Greene, 703-983-3449

- **Websites:**
  - Intelink-U website: https://www.intelink.gov/ICTG/ca.intel
  - Intelink-TS website: http://www.intelink.ic.gov/ICTG/ppd_ca.intel

Appendix 5
Mr. Jarvie’s Combined Industry Update Presentation

# NISPPAC
# Industry Presentation

08 October 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 |
| Frederick Riccardi | ManTech | 2013 |
| Shawn Daley | MIT Lincoln Labs | 2013 |

# Industry Members/MOU

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

# NISPPAC Ad Hoc Working Groups

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

# NISPPAC

- National Industrial Security Program Operating Manual – revision by USG in progress
  - August 27th 2009 – Initial discussion with Industry
    - Hosted by the ISOO
    - General outline of topics provided by OSD
    - Industry provided results of data call
      - Numerous items for consideration provided to USG
      - Industry working priorities

# NISPPAC

- National Industrial Security Program Operating Manual – revision by USG in progress
  - Industry review of revised language
    - Time period for review
    - Assess Impact
    - Coordinate and provide comments

# NISPPAC

(Industry concerns 15 May 2008/ 20 November 2008/ 07 April 2009/ 22 July 2009 )

- Information Sharing - Threat
- Controlled Unclassified Information
- Foreign Ownership Control & Influence (FOCI)
- Personnel Security Clearance Processing
- Certification& Accreditation (C&A)

# Information Sharing - Threat

Institutionalized Process:

- Information
- Communication methodology
- Feedback