BRIEFING SLIDES

COMMISSION MEETING

DISCUSSION OF SECURITY ISSUES

JANUARY 12, 2006

IT Systems Certification and Accreditation

January 12, 2006

AGENDA

- Background
- IG Review Results
- Progress to Date
- Chairman's Tasking Memo
- Lessons Learned
- Path Forward
- Challenges

BACKGROUND

- System Accreditation Activities
- FY 2005 OIS Program Brief
- Closed Commission Brief on IT Security
- Commission Paper on IT Security

SYSTEM ACCREDITATION ACTIVITIES

- An assessment of system for Privacy Act information
- NRC Electronic Information Systems Records Scheduling Survey (NRC Form 637)
- An assessment of the sensitivity of the information being processed by the system
- Assessment of the level of authentication required to access the system
- An assessment of the risk posed to the information being processed, to the NRC, and to the nation along with proposed risk mitigation

SYSTEM ACCREDITATION ACTIVITIES (Cont'd)

- Identification of the information system security controls
- Tests that ensure that the IT security controls are implemented as documented, operating as intended, and produce the desired outcome
- Contingency Plan, Contingency Test and Test Report
- All identified high risk issues have been resolved
- A plan and schedule to resolve lower risk security issues

IG REVIEW RESULTS

- Evaluation of Certification and Accreditation Efforts
- Evaluation of Implementation of FISMA
- Evaluation of Security Controls for Stand-alone Laptops For Handling Unclassified, Safeguards, or Classified Information

FEEDBACK FROM OMB

- Scores on OMB Exhibit 300s lower than last year
- Security is one of the primary reasons
- Interim Authority To Operate (IATOs) now penalized in scoring by OMB (change from previous years)
- Caused staff to propose change in approach to Certification and Accreditation (C&A)

PROGRESS TO DATE

- Information System Security (ISS) Program
- Status of C&A
- Resolved vulnerabilities
- Testing of security

Information Systems Security Program

- Completing templates for C&A documents (Artifacts)
- Documenting instructions for developing C&A information and completing templates
  - using RPS as pilot
  - ensuring repeatable process
- C&A activities focused on highest priority systems
  - SafeSource -- WBL (internal and external) & NSTS
  - Financial systems – Cost Accounting System, FEES, legacy HRMS
  - Agency's infrastructure components supporting these high priority systems

STATUS OF C&A

- Financial systems (estimated ATO date: FY 2006 Q2)
- WBL (estimated ATO date: FY 2006 – Q3)
- NSTS (estimated ATO date: FY 2007 – Q1)
- Infrastructure (LAN/WAN) (estimated ATO date: FY 2007 – Q1)
- RPS (estimated ATO date: FY 2006 – Q2)

RESOLVED VULNERABILITIES

Examples

- Transmission of usernames and passwords encrypted
- Stored sensitive employee information encrypted
- Password expiration periods enforced

CHAIRMAN'S TASKING MEMO

- Approved change in focus of C&A effort
- Approved Independent Study
- Provided additional funding

LESSONS LEARNED

- IT security needed more attention, support, and decisions from senior OIS and agency management
- Enterprise approach (agency-wide) to security necessary
- Security has to be built in during development
- Previous testing was not comprehensive, focused on external threats
- Improved communication on IT Security necessary within OIS and with system owners

PATH FORWARD

- Established OIS SES Lead for ISS Program
- Dedicated staff to completing and documenting ISS Program
- Established two dedicated teams for C&A
  - One dedicated to the WBL and NSTS
  - One dedicated to the financial systems
  - Each team responsible for the respective underlying Agency's infrastructure components supporting the high-priority systems

CHALLENGES

- NIST 800-53 is significantly more prescriptive in controls and documentation
- Limited knowledgeable resources available inside and outside NRC
- Competing workload
- Providing appropriate training to staff
- Resistance to change
- Acknowledgment of potential risk

NEXT STEPS

- OIS will work with the offices to extend IATO's for existing systems – expired or expiring within the next 12 months
- OIS will work with the offices to identify priorities based on their business needs for the remaining systems
- Information Technology Advisory Council will be asked to ensure that the prioritization of C&A activity for the remaining systems supports the agency's business needs
- OIS will communicate impacts on remaining systems as a result of supporting the agency's path forward
  - Delay in review of business cases for new systems
  - Delay in review of C&A artifacts for lower priority systems
  - Limited OIS support for review during development of C&A artifacts
  - Possibility that C&A artifacts developed for the remaining systems may need further revision to meet security and documentation requirements