



Protection of the IT Infrastructure and Related Topics (Open)

**Deputy Executive Director
for Corporate Management
December 15, 2008**

Agenda

- **Introduction**
- **Federal Information Security Management Act (FISMA) Update**
- **Information Technology (IT) Modernization**
- **Closing**

Federal Information Security Management Act Update

Paul Ricketts
Senior IT Security Officer
FISMA Compliance and Oversight
Branch
Computer Security Office

FISMA Update Overview

- **Past**
 - **Targeted implementation of the NRC IT Security Program through the newly created Computer Security Office (CSO)**
 - **Emphasis on FISMA compliance**

FISMA Update Overview (cont'd)

- **Present**
 - **Planning, directing, and overseeing implementation of the NRC IT Security Program**
 - **Maturing CSO capabilities**

FISMA Update Overview (cont'd)

- **Future**
 - **Mature the Program and seek efficiencies through effective risk management and enhanced technical capabilities, policy, training, and reporting**
 - **Conduct an enterprise risk assessment**
 - **Construct a viable situational awareness capability**

FISMA Update Overview (cont'd)

- **Future (cont'd)**
 - **Establish quarterly compliance review process**
 - **Expand the role-based training effort**
 - **Develop and integrate the security architecture**
 - **Document an Information Security Strategic Plan (ISSP)**

FISMA Update Overview (cont'd)

- **Future (cont'd)**
 - **Establish an Information Systems Security Officer (ISSO) framework, forum, and training program**

FISMA Update Accomplishments

- **Established Computer Security Office**
 - **CSO authorized by the Commission on 11/25/07**
 - **New office reports to the Deputy Executive Director for Corporate Management (DEDCEM)**

FISMA Update

Accomplishments (cont'd)

- **Established Computer Security Office (Cont'd)**
 - **Headed by the Chief Information Security Officer (CISO)**
 - **CISO assigned on 3/17/08**
 - **CSO now fully staffed with 14 personnel**

FISMA Update

Accomplishments (cont'd)

- **Material Weaknesses in the NRC IT Security Program Have Been Eliminated**
 - **Two significant deficiencies were identified in the FY07 FISMA Audit in the areas of certification and accreditation (C&A) and contingency planning**

FISMA Update

Accomplishments (cont'd)

- **Material Weaknesses in the NRC IT Security Program Have Been Eliminated (Cont'd)**
 - **The FY08 FISMA Audit reflects that:**
 - **Over 50% of NRC's FISMA-reportable systems are now authorized to operate (4 times the number completed in 2 previous fiscal years)**
 - **100% of NRC's FISMA-reportable systems now have tested contingency plans**

FISMA Update

Accomplishments (cont'd)

- **Other Advancements**
 - **100% of FISMA-reportable systems are now categorized**
 - **100% of NRC owned/operated systems have completed annual testing of security controls**

FISMA Update

Accomplishments (con't)

- **Other Advancements (cont'd)**
 - **Staff augmentation contract awarded to improve CSO processes and enhance capabilities**
 - **ISSP Steering Committee established and ISSP under development**

FISMA Update

Accomplishments (cont'd)

- **Other Advancements (cont'd)**
 - **Additional systems received authority to operate (ATO) since FY08 FISMA Audit**

FISMA Update

Fiscal Year 2009 Gaps

- **Certification and Accreditation**
 - **11 FISMA-reportable systems remaining**
 - **Funding C&A work for 8 systems in Quarters 2 & 3 FY09**

FISMA Update

Fiscal Year 2009 Gaps (cont'd)

- **Program Office Funding for Continuous Monitoring**
 - **Contingency plan testing**
 - **Annual security controls testing**
 - **Plan of action and milestones (POA&M) weakness remediation**

FISMA Update

Fiscal Year 2009 Gaps (cont'd)

- **Funding Continued Development**
 - **Enterprise security architecture**
 - **Digital forensic capability in conjunction with Infrastructure and Computer Operations Division (ICOD) and Support from the Office of Inspector General (OIG)**

FISMA Update

Fiscal Year 2009 Gaps (cont'd)

- **Funding Continued Development (cont'd)**
 - **Unissued policies and standards**
 - **Additional role-based training**

FISMA Update

Actions Taken to Meet Gaps

- **Certifying and accrediting 5 systems in Q1 FY09 under continuing resolution**
- **Requested program offices fund their continuous monitoring security needs**

FISMA Update

Actions Taken to Meet Gaps

(Cont'd)

- **Initiated outreach to other offices requesting funding of remaining C&A effort for FY09**
- **Consolidated 7 separate systems into a single infrastructure system**

FISMA Update

What Will be Different this Year?

- **Initiate Actions to Demonstrate Further Progress**
 - **Accredit remaining Major Applications and General Support Systems by 06/30/09**
 - **Complete contingency plan testing and updates by 6/30/09**

FISMA Update

What Will be Different this Year? (cont'd)

- **Initiate Actions to Demonstrate Further Progress (Cont'd)**
 - **Complete annual control testing by 6/30/09**
 - **Use of contractor support to augment CSO staff capability and to implement best practices**

FISMA Update

What Will be Different this Year? (cont'd)

- **Initiate Actions to Demonstrate Further Progress (cont'd)**
 - **Expand role-based training**
 - **Issue updated policies and standards**
 - **Enhance the POA&M process**

FISMA Update

What Will be Different this Year? (Cont'd)

- **Initiate Actions to Demonstrate Further Progress (Cont'd)**
 - **Update system inventory to include all security assets**
 - **Establish ISSO Forum to improve communication with program offices**

FISMA Update

What Will be Different this Year? (Cont'd)

- **These actions will enhance the NRC's security posture and improve its level of FISMA compliance**

Information Technology Modernization

**Thomas Rich, Director
Infrastructure and Computer Operations
Division**

**Joseph Holonich, Director
Information and Records Services
Division**

Office of Information Services

IT Modernization

- **Strategic and Tactical Plans**
 - **IT/IM Strategic Plan**
 - **Infrastructure Planning Team Report**
 - **IT Roadmap**

IT Modernization

- **Key Business Drivers**
 - **Working from anywhere**
 - **Getting access**
 - **Improving productivity**
 - **Maintaining a robust, efficient IT infrastructure**
 - **Getting information**
 - **Doing business during emergencies**

IT Modernization

Working from Anywhere

Staff can securely access the systems and information they need no matter where they're located

IT Modernization

Working from Anywhere

Accomplishments

- **Modernized video-teleconferencing**
- **Memory of remote access personal settings**
- **Outlook Web access**

IT Modernization Working from Anywhere (cont'd)

Short Term

- **Mobile communications expansion**
- **Secure wireless mobile computing**
- **Remote access application expansion**

IT Modernization Working from Anywhere (cont'd)

Planning for the Future

- **New IT infrastructure support contract**

IT Modernization

Getting Access

Users can securely access the IT systems and information they need through a single or minimal points of entry

IT Modernization Getting Access

Accomplishments

- **Increased communication bandwidth to remote locations**
- **Implemented Managed Public Key Infrastructure (MPKI)**

IT Modernization Getting Access (Cont'd)

Short Term

- **Single authoritative employee directory**

IT Modernization Getting Access (cont'd)

Planning for the Future

- **Identity management**
- **Single sign-on**

IT Modernization

Improving Productivity

Individuals and groups of staff can work efficiently to accomplish the agency's mission

IT Modernization Improving Productivity

Accomplishments

- **Enterprise SharePoint deployment**
- **Enterprise project management (NRO Pilot)**
- **Migration to Microsoft Outlook**

IT Modernization Improving Productivity (cont'd)

Short Term

- **SharePoint training and support program**

IT Modernization

Improving Productivity (cont'd)

Planning for the Future

- **Obtain voice mail through E-mail inbox**
- **Know how to contact your staff/manager wherever they are**

IT Modernization

Maintaining a Robust, Efficient IT Infrastructure

The agency continues to upgrade the IT Infrastructure to improve operational effectiveness and more efficiently support agency business needs

IT Modernization

Robust, Efficient IT Infrastructure

Accomplishments

- **Modernized telephone capabilities**
- **Data center efficiency enhancements**
- **Network refresh**

IT Modernization

Robust, Efficient IT Infrastructure (cont'd)

Short Term

- **More flexible network access controls**

IT Modernization Robust, Efficient IT Infrastructure (cont'd)

Planning for the Future

- **New IT infrastructure support contract**
- **Centralized IT operations**
- **Voice/data/video convergence**

IT Modernization

Getting Information

- **Staff can access the information they need to perform their work**
- **Stakeholders can access the information they need to participate effectively in the regulatory process**

IT Modernization Getting Information

Accomplishments

- **Kept information to staff and stakeholders available via ADAMS**
- **Began modernization of ADAMS**

IT Modernization

Getting Information (cont'd)

Short Term

- **Continue ADAMS modernization**
- **Obtain public Web content management services**
- **Acquire tools for public users of the NRC's Web site**

IT Modernization

Getting Information (cont'd)

Planning for the Future

- **Implement information management framework and complete modernization**
- **Redesign public Web site**

IT Modernization Challenges

- **Ensuring that the delivery of services is commensurate with agency expectations and resources available**
- **Identifying requirements to support a corporate view for acquiring and providing Services**

IT Modernization Challenges (cont'd)

- **Maintaining legacy systems and infrastructure versus modernizing**
- **Reducing customization**

Acronyms

- **ADAMS – Agencywide Documents Access and Management System**
- **ATO – Authority to Operate**
- **C&A – Certification and Accreditation**
- **CISO – Chief Information Security Officer**
- **CSO – Computer Security Office**
- **FISMA – Federal Information Security Management Act**
- **FY – Fiscal Year**

Acronyms (con't)

- **ICOD – Infrastructure and Computer Operations Division**
- **ISSO – Information Systems Security Officer**
- **IT – Information Technology**
- **MPKI – Managed Public Key Infrastructure**
- **NRC – Nuclear Regulatory Commission**
- **NRO – New Reactor Office**
- **OIG – Office of Inspector General**
- **OIS – Office of Information Services**
- **POA&M – Plan of Action and Milestones**
- **Q - Quarter**