



Information Security Issues

Rob McKinney



Topics

- Certification & Accreditation
- Ongoing Requirements – FISMA / HIPAA Compliance
- Support
- Projects / Pilots / Initiatives
- Maximize Resources



Certification and Accreditation Status

- C&A's complete for RPMS and NPIRS through June 2009
 - RPMS -> Type C&A: if local RPMS implementations conform to the configuration "national" C&A'd then the national C&A can be used locally with slight changes to address locally focused controls such as physical access controls
 - TeleHealth
- IOAT C&A -> 8 of 11 Areas, HQ, and OIT Abq are complete; expect remaining three Areas to be done by the end of December
 - HR Applications
 - Everything not RPMS or NPIRS



Ongoing Requirements – FISMA / HIPAA Compliance

- Penetration Testing
- Vulnerability Testing
- Control Testing
- POA&M's
- Minimum Security Configurations
- Self-assessments
- Life-cycle Integration
- CPIC Process Integration



Support

- Assist Team
 - 12 Site Visits
- Incident Response
 - 159 Suspected Incidents; 25 Incidents Investigated Evaluations
 - Coordinating – OIT Team, NOSC, Local Personnel
- Monitoring
 - Network
 - IDS / IPS / FW / Router
 - Baseline Configuration Development – Phoenix AO
 - Network Policy – Securify
 - Websense
 - High Value Servers (RPMS, AD, DNS, Web)
 - Performance Parameters
 - Security Events
- Interconnection Partners / Agreements



Projects / Pilots / Initiatives

- Network Admission / Information Flow Control – Citrix, Cisco, Microsoft
 - Remote Users
 - Guests
 - All Users
- WLAN Standard Development
 - Joint Effort W / Oklahoma AO
- Significant Security Responsibilities Training Program
- Laptop and Removable Media Protection – HHS Funded
- Agency-wide Automated Patching / Application Deployment System



Maximize Resources

- **Centralized capability**
 - Spread over three-year period
 - Provides additional services, e.g.:
 - Infosec / adhoc systems training
 - Vulnerability remediation
 - Audit
- **Use of *common information security controls* that can be applied to one or more Agency information systems**
 - Assessments of common controls can be used to support C&A's of agency information systems where those controls have been applied
 - Example: RPMS – “type” C&A
- **Possibility at the facility level:**
 - Implement standards according to representative facilities
 - Conduct C&A's on representatives and apply to others



Maximize Resources

- **Common Infosec Controls: Facility Perspective**
 - Would require development and implementation of standards / standard infosec controls; e.g., OS's, security appliances, applications, configurations
 - Cons: some initial costs of migrating to standards, loss of some autonomy with IT systems
 - Pros: meeting standards requirement, cost reductions through bulk purchases, sharing IT expertise, reduced maintenance and implementation costs, supports move to centralized automated patch management system and NOSC, significantly reduces costs associated with C&A's, e.g., conducting 4-12 C&A's every three years vs. hundreds



Mature Program

The consideration of information security is pervasive in the culture. A proven life-cycle methodology is implemented and enforced, and an ongoing program to identify and institutionalize best practices has been implemented. There is active support from senior management. Decisions and actions that are part of the system life cycle include:

- Improving security program,
- Improving security program procedures,
- Improving or refining security controls,
- Integrating security within existing and evolving IT architecture, and
- Improving mission processes and risk management activities.

Each of these decisions results from a continuous improvement and refinement program instilled within the organization. The understanding of mission-related risks and the associated costs of reducing these risks are considered with a full range of implementation options to achieve maximum mission cost-effectiveness of security measures.



Summary

- C&A's Progressing
- Continual Effort Required – FISMA / HIPAA Compliance
- Centralized Support
 - Assists; Incident Response; System Monitoring; Interconnection Agreements / Reviews
- Projects / Pilots / Initiatives
 - Access / Policy Enforcement; Laptop / Media Protection; Training Program; Wireless Standard; Agency-wide Patching / Application Deployment
- Maximize Resources
 - Develop and implement standards
 - Conduct a few representative C&A's