NIH Security, FISMA and EPLC

Lots of Updates!
Where do we start?

Kay Coupe
NIH FISMA Program Coordinator
Office of the Chief Information Officer

Project Management Community Meeting
October 18, 2011

" OCIO - Enabling the NIH Research Mission"

Risk Management

No more 3 year ATOs????

NEAR

C&A is "GONE"

New terms, new concepts, questions

Vulnerability Management

No more DAAs?

Security Authorization

HEAR

Continuous Monitoring

NIST Updates

Updated Special Publications (SP)

- 800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations (Sept 2011)
- 800-128: Guide for Security-Focused Configuration Management of Information Systems (Aug 2011)
- 800-53 Appendix J: Draft Privacy Control Catalog (July 2011)
- 800-39: Managing Information Security Risk: Organization, Mission and Information System View (Mar 2011)
- 800-30: Draft Guide for Conducting Risk Assessments (Sept 2011)
- 800-37, Rev 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (Feb 2010)

New Terms

- Certification & Accreditation (C&A) is now:

  System Authorization

- Designated Authorizing Authority (DAA) is now:

  Authorizing Official (AO)

- Project Categorization is now:

  System Categorization

- System Certification is now:

  Security Control Assessment

- System Re-certification/Re-Accreditation is now:

  System Re-Authorization

New (and old) Emphasis

- Risk Management – *more involvement by the system owner and project manager*
- Continuous Monitoring – *new approaches and tools coming*
- “Continuous Authorization to Operate”
  - *More to come from HHS on this new concept*
- Cloud Computing – *new contract language*
- POAMs and validation of mitigation – *tracked in NIH Certification & Accreditation Tool (NCAT)*
- Remote Access and 2-factor authentication of moderate and high impact systems – *ensure it is built into new systems*

Acronyms

- FISMA – Federal Information System Management Act
- NCAT – NIH Certification & Accreditation Tool
- NEAR - NIH Enterprise Architecture Repository
- HEAR - HHS Enterprise Architecture Repository
- SPORT – HHS Security and Privacy Online Reporting Tool
- POAM – Plan of Action and Milestones
- PMT – Portfolio Management Tool (for Capital Planning [CPIC])
- ISSO – Information System Security Officer
- CISO - NIH Chief Information Security Officer
- CIO – Chief Information Officer
- ISAO – Information Security and Awareness Office
- NIH Master Glossary of IT Security Terms: http://ocio.nih.gov/security/ISSO%20Glossary.doc

New Changes Coming
(Things to watch for)

- All systems must be input into NEAR and NCAT in order to be listed in HEAR
  - Once systems are in HEAR, SPORT will be populated so PIAs can be started
  - Coordination done through the NCAT team
    - Coordinate with your ISSO and Privacy Coordinator
- New Privacy Controls will be part of SP 800-53
- POAM updates will be sent to HHS every two weeks
- Alignment of HEAR/NEAR/SPORT/PMT and new HHS Data Warehouse

Changes to Security Approach and Deliverables Per EPLC 1.4 (Phased in over time)

- Privacy Impact Assessment (PIA)
  - Preliminary done in Concept Phase per EPLC 1.4
  - Final PIA must be done in coordination with the Implementation Phase
  - Work with your IC Privacy Coordinator and ISSO
- Security Approach – Removed based on new SP 800-37 methodology
  - 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

Changes to Security Approach and Deliverables Per EPLC 1.4 (Phased in over time)

- Interconnection Security Agreement (ISA)
  - Could be part of a Computer Match Agreement (CMA)
  - Does not take the place of a CMA
  - NIH has ISA template
    - http://ocio.nih.gov/nihsecurity/NIH_ISA_Templates.html
    - More to come on CMAs and ISAs
- New Security templates in NCAT coming soon

Other Changes to the EPLC Rev 1.4 Related to Security

- Project Manager responsibilities regarding POAMs updated
  - Work with your ISSO and NCAT representative
  - Validation of mitigation is very important (audit issue)
  - Ongoing process
  - Various sources for weakness identification (vulnerability scans, Security Control Assessments, continuous monitoring, audits, etc.)
  - New HHS reporting process coming
    - POAM information will be sent to HHS every two weeks starting in 2012

Other Changes to the EPLC Rev 1.4 Related to Security

- An Authority to Operate may be granted for a period of time to be determined by the Authorizing Official (AO) in compliance with HHS policies (not just three year periods – more to come)
- Ensure that all high impact risks are documented and mitigated prior to entering the implementation phase
- Flexibility and tailoring regarding security control implementation is permitted
- Compensating controls can be utilized, but must be documented and accepted
- If waivers are required, submit them in a timely manner to the NIH CISO (via your ISSO)

Security Critical Partners –
What we look for

Comprehensive indication that security risks and compliance are being included and evaluated. Some examples include:

- Access control & segregation of duties implemented
- Configuration standards documented, followed and tested
- Privacy evaluated
- Security Authorization costs included in budget
- Accurate and thorough design documentation included
- ISSO involvement
- Vulnerability scans/penetration tests performed and issues mitigated
- Security Plan accurate and up-to-date
- Contingency Plans tested
- POAMs documented, tracked and mitigated in timely manner
- Residual Risk mitigated or accepted by appropriate authority
    - New program coming
    - CIO/CISO acceptance of risk may be needed for NIH HIGH RISKS

Remember….

- Security should be built-in during system concept and design phases, not added on at the end
- A good design document is worth its weight in gold
- Reach out to your IC ISSO, the NIH Privacy Office and ISAO if you have questions (we really are here to help)
- New programs and processes are being developed to assist you and your input is very important
- Security needs to be implemented and monitored on a continuous basis
- The “bad guys” don’t take vacations..............;-)

Reference Links

NIST Special Publications

http://csrc.nist.gov/publications/PubsSPs.html

NCAT Support Team

ncat@mail.nih.gov

Office of the Senior Official for Privacy

privacy @mail.nih.gov

OCIO Security Website

http://ocio.nih.gov/security/index.html

Contact Info

Kathleen (Kay) Coupe
NIH FISMA Program Coordinator
Information Security and Awareness Office
Office of the Chief Information Officer
coupek@mail.nih.gov
301-594-9848
Room 3G12
Fernwood Building