Use of Best Practice IT Security Products

Presenters

Patrick Howard, CISSP, CISM
Chief Information Security Officer, HUD

&

Brenda Abrams
OIG IT Audit Manager
at GSA
Agenda

• Background and Introduction
• Benefits
• Example: EAuthentication Risk Assessment
• Recommendation
• Final Thoughts and Questions
Background –

General IT Security Program Needs

- Strategic plan
- Organizational structure/staffing
- Policy & procedures
- Certification & accreditation methodology
- Categorization & inventory guidelines
- Contingency planning guidelines
Background –

The HUD IT Security Program

- Established in FY04
- Fully based on NIST guidance
- Industry and government best practices used in creation of program
- Achieved an “A+” on the FY06 FISMA Report Card
- Serves as a good test bed
Standard IT Security Documentation Requirements

- System Security Plan
- Risk Assessment
- Security Test & Evaluation
- Plan of Action & Milestones
- C&A Statement
- Privacy Impact Assessment
- Business Impact Analysis
- IT Contingency Plan
- E-Authentication Risk Assessment
Security Documentation Products

- Policies and Procedures
- Templates and instructions
- QA Checklists for Completed Documentation
- Instructions for QA Checklists
- Training presentations on the use of the products
Building on NIST Guidance

- NIST laid the foundation for these products with their IT security guidelines
- HUD and other agencies have added the next layer
- Have made them easier to use
- Have permitted consistency across the organization
- All agencies, large and small, could have the same quality starting point
What Does a Security Best Practice Product Look Like: An Example

The E-Authentication Risk Assessment Process
Benefits Of Using Best Practice IT Security Documentation Products

- Improved quality starting point
- Streamlines the process
- Reduced cost and time, enabling agencies to use resources more efficiently
- Can be used as quality check for contractors or incorporated as part of a statement of work
- Provides a consistent method for auditing these areas
So Why Not Just Post It On OMB Or NIST Websites as a Best Practice?

• Does not guarantee it will be used consistently across government
• Does not necessarily raise the quality level of the IT security information we are gathering on our systems to make better planning and budgeting decisions.
Recommendations

**OMB:**
- Endorse best practice products
- Mandate their use by agencies

**NIST:**
- Assume NIST ownership of the product set
- Maintain best practice documentation products
Benefits

– A reduction in the amount of time agencies use in “reinventing the wheel”
– Agencies can begin to use products immediately
– Results could be realized in 2008.
What Can The Board Do Now?

Support discussions with NIST and OMB on the recommendations to realize the benefit in 2008.
Final Thoughts and Questions
Contact Information

Patrick D. Howard, CISO
Department of Housing and Urban Development
patrick.d.howard@hud.gov
202-402-8094

Brenda Abrams, IT Audit Manager
GSA Office of Inspector General
brenda.abrams@gsa.gov
703-405-9366