Improving the FISMA Security Report Card Grades
Recommendations and Lessons Learned

Marc Noble, FCC CSO
CISSP, ISSAP, CISM

Small Agencies Perspective

- CISO's with budgets of less than $500,000 spend 45% on FISMA compliance
- CISO's with budgets greater than $10,000,000 spend 27% on FISMA compliance
- Small/Micro Agencies CISO's often lack time and funds

Results from Intelligent Decisions Survey of CISO's conducted in 2004.

Thanks to Loren Schwartz, CPA, CISA, IT Partner Cotton & Company LLP

Small Agencies Compliance
What to do *Inexpensively*

- Develop a IT Security Program
  - Information Security Policies, Procedures, and Guidelines
    - ✓ Comprehensive Policies and Procedures for less than $1000
    - ✓ Policies, Procedures and Guidelines are on line from other Federal agencies
    - ✓ Policies should be high level, detailed policy can cause failure
    - ✓ Guidelines/Baselines (Free for self-assessment)
      - **http://www.cisecurity.org/**

Small Agencies Compliance
What to do *Inexpensively*

- Risk based – document decisions
  - ✓ Standards allow for judgment by the agency
    - Agencies are allowed to accept risk
    - Document the judgment calls and be able to defend them
    - Undocumented judgment won't fly to an auditor
  - ✓ Annual Review systems – risk based (FIPS-199)
  - ✓ Program Review for Information Security Management Assistance (PRISMA) http://prisma.nist.gov/index.html
  - ✓ Develop Plan of Action and Milestones (POAMS)

Small Agencies Compliance
What to do *Inexpensively*

- Best practices in developing Federal Agency Security Practices **http://csrc.nist.gov/fasp/index.html**
- Certification and Accreditation major system and general support system
  - ✓ Start with a template – once the first one is done, it gets easier
  - ✓ Use automated tools

Small Agencies Compliance
What to do *Inexpensively*

- Configuration Management
- Incident Detection and Response
- Awareness Training (Inexpensive for general population, expensive for technical employees)(FCC developed quarterly specialized training bulletins that have been accepted by IG)
  - ✓ Part of HR new employee training and once annually
  - ✓ Document who attended

Dealing with Auditors

- Auditors are human beings - work with them
- Support what you do – basic audit premise is professional skepticism
- Guidance for auditors related to FISMA is unclear – gain an understanding of the OIG expectations during planning
- OMB submissions from CIO and OIG should match
- Don't be afraid of auditors - they will talk to you

Good links on the Internet

- **http://csrc.nist.gov/sec-cert/index.html**
  - ✓ NIST FISMA resource center
- **http://www.cisecurity.org**
  - ✓ Benchmarks and free tools to analyze systems
- **http://www.sans.org/**
  - ✓ Policies and articles
- **http://csrc.nist.gov/fasp/index.html**
  - ✓ C&A's, federal best practices, statement of work, policies and procedures