FISMA Update

PRESENTED BY
THE FEDERAL RETIREMENT THRIFT INVESTMENT BOARD

February 26, 2018

Thrift Savings Plan

tsp4gov @

FISMA Program

- Continue with security enhancements
- Define an organization-wide risk-based information security program
  - Target FISMA level
  - Prioritization of domains
  - Key activities
- Reevaluate and strengthen governance structures

Thrift Savings Plan

FISMA Targets

	Domain	Ad-hoc	Defined	Consistently Implemented	Managed and Measureable	Optimized
Identify	Risk Management		In place in FY18, reflected in FY19 audit	In place in FY19, reflected in FY20 audit	To be determined	
Protect	Configuration Management					
	Identity and Access Management					
	Security Training					
Detect	Continuous Monitoring					
Respond	Incident Response					
Recover	Contingency Planning					

Thrift Savings Plan

Prioritization of FISMA Domains

Factors

- FRTIB Top Enterprise Risks

- Audit Findings

- Ease of Implementation

Prioritization

- Configuration Management
- Identity and Access Management
- Incident Response
- Contingency Planning
- Information Security Continuous Monitoring
- Risk Management
- Security Training

Thrift Savings Plan

Key Program Activities

- Undertake a risk based assessment of priorities
- Treat each FISMA domain as a stand alone project and manage it aggressively
- Customize standard NIST controls for FRTIB
- Review FISMA audit issues for insights to Agency gaps
- Update documents to aligned with policy
- Ensure Agency and contractor personnel are trained and following new processes

Thrift Savings Plan

Governance Structure and Activities

- Enhance our contracts with our IT partners

- Put needed tools and processes in place

- Institute joint forum (e.g. configuration management) for oversight, monitoring, and decision making

Thrift Savings Plan