



Department of Commerce IT Review Board



Enterprise IT Security FY 2012 Budget Submission

Larry Reed
June 23, 2010



Agenda



- Description
- IT Investment Proposal
 - Overview
 - Requirements
 - Information Technology and Risk Based Approach
 - Cost Estimates
 - Integrated Project Schedule / Baseline Changes
- Impact on OMB FY 2011 Passback Initiatives
- Summary/Recap
- Recommendation
- Backup



IT Investment Proposal

Overview



- Expand Enterprise IT Security Services
 - Focused on building common controls
 - Improve C&A compliance and cost avoidance across NOAA
 - Enterprise security posture awareness and visibility
 - Integrated with Enterprise Architecture
 - Address common security weakness across NOAA
 - Leverage existing capabilities
 - Create IT Security services that will be used across NOAA
- NOAA Cyber Security Center (NCSC)
 - Nationwide 24x7 security monitoring and Incident Response (IR)
 - Enterprise proactive services
- Implement OMB Trusted Internet Connection (TIC) Services
 - Complete current TIC services and expand to 3 additional access points
- Strategically aligned with DOC FY12 Enterprise Security Operations Initiative.
 - Leverage NOAA's capability and expand to DOC Enterprise SOC
 - DOC ESOC depends on NOAA's investment



Description

Background



- IT Security Current Capabilities and Functions
 - NOAA satisfies incident response common controls through the N-CIRT
 - Currently only 2/3rds implemented
 - 12x5 onsite coverage
 - No overnight or weekend coverage
 - Only Highest Priority Incidents receive adequate attention, medium priority incidents receive no attention
 - 12x5 security monitoring
 - Intrusion Detection System (IDS) Data Analysis limited to highest priority incidents
 - Many cyber-attacks go undetected for days
 - Limited automated tools for intrusion detection and response, none for prevention
 - Limited to 2 IT Security Consulting Projects per year (e.g., OPeNDAP; Secure Elements)
 - Reactive Services Only
 - 72% of OMB Trusted Internet Connections (TIC) Services Implemented for 1 of 4 NOAA TIC Access Points (TICAP)



IT Investment Proposal Requirements



- NOAA Cyber Security Center (NCSC)
 - Repeatable process based approach
 - Re-Use
 - Expand and Build on existing capabilities
 - NOAA Security Operations Center and Incident Response Team
 - New Tools, processes and people to support
 - 24x7 Incident Response Team
 - 24x7 Security Monitoring
 - Security event/log data correlation and reduction
 - Turn millions of log entries into tens of actionable events
 - Security consulting projects, new technology review
 - Coordination with external entities
 - DOC CIRT, US-CERT, OIG, Law Enforcement, OMB TIC



IT Investment Proposal Requirements



- Alternative: Current State
 - 5x12 support for incident response
 - 24x7 ad hoc on call, only critical high priority incidents get full response
 - 5x12 Security Monitoring Incomplete
 - Minimal Intrusion Detection System coverage
 - Partial Enterprise View of Security Posture
 - Individual security software solutions
 - Not cost effective, consistent, or sustainable
 - 72% TIC compliance at one of four locations



IT Investment Proposal

Information Technology and Risk Based Approach

- Cybersecurity
 - NOAA/OCIO/Enterprise IT Security
 - Affects 1 existing FISMA IT Systems: NOAA0100
 - NIST FIPS 199 Risk Impact level: Moderate
 - N-CIRT (NOAA0100) POA&M Status
 - 17 POA&Ms from FY07 C&A activity
 - ✓ 13 Completed
 - ✓ 4 behind schedule due to insufficient resources
 - Currently Undergoing C&A Testing

NOAA System ID:	NOAA0100
C&A Date (planned or current)	6/29/07
Expiration Date:	6/29/10



IT Investment Proposal

Information Technology and Risk Based Approach



- Enterprise Architecture
 - This investment is part of the NOAA Enterprise Architecture Plan.
 - Leverages NOAA's Technical Reference Model (TRM) by supporting:
 - Identification of IT security standards for inclusion in the TRM
 - Vetting of proposed (non-security specific) TRM standards to identify and mitigate potential security issues



IT Investment Proposal

Information Technology and Risk Based Approach

Risk Management and Assessment

Risk Area	Description	Probability	Impact	Mitigation Strategy
Project Resources - Personnel	NCSC relies on highly-skilled IT security engineers. Cost and availability of the appropriate cyber security resources is critical to the project.	Moderate	High	Recruit, evaluate, hire, and retain qualified staff. Close coordination with contractor, utilize all available recruiting techniques Career ladder defined with training program
Technology	Lack of software and hardware maturity for NOAA's cutting edge IT environment could delay implementation.	High	Moderate	Use Pilot programs, extensive pre-purchase testing and peer review of requirements.
Changing requirements and OMB directives. (e.g. TIC, FDCC)	Changing mandates may impact project schedule, cost, and performance	Moderate	Moderate	Project coordination and support with NOAA and DOC senior management



IT Investment Proposal

Cost Estimates FY 2012 Budget



(\$K):	FY 11 PB	FY 12	FY 13	FY 14	FY 15	FY 16
CAPABILITY:						
Current IT Resources	\$6,829	\$6,829	\$6,829	\$6,829	\$6,829	\$6,829
Proposed IT Adjustment	\$0	\$7,400	\$7,483	\$7,568	\$7,655	\$7,753
IT Total	\$6,829	\$14,229	\$14,312	\$14,397	\$14,484	\$14,582
IT COMPONENT INCREASE:	FY 11 PB	FY 12	FY 13	FY 14	FY 15	FY 16
Hardw are: (Supercomputing Hardw are/Cycles Only)	\$0	\$0	\$0	\$0	\$0	\$0
Hardw are: (All other IT Hardw are – excluding IT Security HW)	\$0	\$0	\$0	\$0	\$0	\$0
COTS Softw are (Example: UNIX)	\$0	\$0	\$0	\$0	\$0	\$0
Support Services: (Example: Contractors for Softw are Development – excluding IT Security support)	\$0	\$0	\$0	\$0	\$0	\$0
Telecommunications: (Circuits Only)	\$0	\$30	\$33	\$36	\$39	\$43
IT Security : (All IT Security Costs: HW, SW, Contractors, Training, Security Plan Development, Incident Response, etc.)	\$0	\$7,127	\$7,197	\$7,269	\$7,340	\$7,420
IT Training: (Example: Router Training – excluding IT Security Training)	\$0	\$0	\$0	\$0	\$0	\$0
Common Services (Example: Help Desk)	\$0	\$0	\$0	\$0	\$0	\$0
Government FTE Costs: (This <u>includes</u> any IT Security FTE costs)	\$0	\$243	\$253	\$263	\$276	\$290
IT Component Total	\$0	\$7,400	\$7,483	\$7,568	\$7,655	\$7,753



IT Investment Proposal

Cost Estimates FY 2012 Budget



Funding Breakout by IT Security Sub-Category

IT Investment Category	Sub-Category	Adjustment Amount
IT Security	IT Security Hardware	\$3008K
	IT Security Commercial-Off-The-Shelf (COTS) Software	\$1805K
	IT Security Support Services (i.e., Contractors)	\$2314K
Government FTE Costs	IT Security Professionals	\$243K
	Telecommunications	\$30K
TOTAL		\$7400K



IT Investment Proposal

Integrated Project Schedule / Baseline Changes



Milestones	Planned Completion
NCSC: Complete Design	2/2010 - Complete
NCSC: Complete draft AU common controls requirements	3/2010 - Complete
NCSC: Initial Operating Capability	7/2010
NCSC: Complete on-boarding of NMFS	9/2010
NCSC: On-board second customer	2/2011
NCSC: On-board third customer	6/2011
NCSC: Increase staff to support 24x7 operations	6/2012
NCSC: Enhance security services at second TIC Access Provider (TICAP)	7/2012
NCSC: Enhance security services at third TIC Access Provider (TICAP)	10/2012
NCSC: Enhance security services at fourth TIC Access Provider (TICAP)	2/2013



Impact on OMB FY 2011 Passback Initiatives



- HSPD-12
 - The NCSC will be deployed using HSPD-12 Compliant systems
- Trusted Internet Connection (TIC)
 - DHS Approved NOAA's four TICAPs.
 - The NCSC implements the TIC Security services for NOAA
- Green IT
- Privacy
- Migration to Networx
 - Communications will be procured using Networx



Summary/Recap



- Fortify critical IT support of NOAA's mission
- Increase the coverage and capabilities of the NOAA Cyber Security Center
- Enhance nationwide 12x5 security monitoring and incident response to 7x24
- Meet OMB requirements for TIC at all four NOAA TICAPs.



Recommendation



- Provide funding at requested levels
 - Improves security posture
 - Improve NCSC to 24x7
- Risks if not funded
 - Reduced security posture
 - NOAA unable to adequately manage IT risks
 - DOC Enterprise Security Operations Initiative will be at risk



Backup Slides

