Information Systems Security Requirements for Federal GIS Initiatives

Alan R. Butler, CDP
Senior Project Manager

Penobscot Bay Media, LLC
32 Washington Street, Suite 230
Camden, ME 04841
"We are at risk," advises the National Research Council in *Computers at Risk*.

"Although we trust them, computers are vulnerable to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun...

“To date, we have been remarkably lucky.”

“The risk of fraud, waste, abuse, embarrassment to the government, and loss of public confidence increases as computer systems are more widely used and software becomes more complex.”

– President’s Management Council
Information Systems Security
Take Away from our Time Together . . .


- GIS compliance with Federal Regulations and Guidance Mandates for Information Systems Security / Information Assurance

- Awareness of and Diligence toward INFO SEC Requirements, GIS-related Security Programs and Management Controls

- GIS INFO SEC -- Not just an Integral Part of Federal Workers and Contractors day-to-day Responsibilities . . . It’s the Law!
Clinger-Cohen Act (40 U.S.C. 1401(3))
Information Technology Management Reform Act of 1996

- Implemented the Capital Planning Investment Control (CPIC) IT budget planning process
- Granted to the Director of the Office of Management and Budget (OMB) authority to oversee the acquisition, use, and disposal of information technology by the Federal government
- Established Chief Information Officer (CIO) positions in every department and agency in the federal government
- Established CIO Council from 28 major agencies (CIOC) and OMB
- Defined Information Technology Architecture (ITA) for evolving and acquiring Information Technology

OMB grades IT projects and funds accordingly - with an “at-risk” category. The risk involved is not receiving initial or on-going funding for the IT project.
As part of the President’s Management Agenda (PMA) . . .
- OMB’s Office of E-Government and Information Technology (E-Gov & IT)
- Support of the General Services Administration (GSA)
- Support of the Federal CIOC
- Established the Federal Enterprise Architecture (FEA) Program
  (replacing ITA) -- Comprehensive business-driven blueprint of the entire Federal Government.

FEA Program Management Office (FEA PMO) . . .
- Located in OMB’s Office of E-Gov and IT
- Equips OMB and Government with a common language and framework
  - Describe and analyze IT investments
  - Enhance collaboration
  - Transform Government . . . citizen-centered, results-oriented and market-based
FEA “Reference Models” designed to facilitate cross-agency . . .

- Analysis and Identification of Duplicative Investments
- Uncover Gaps and Opportunities for Collaboration within and across Agencies
  - PRM (Performance Reference Model)
  - BRM (Business Reference Model)
  - SRM (Service Reference Model)
  - DRM (Data Reference Model)
  - TRM (Technical Reference Model)

FEA “Profiles” framework . . .

- Cross-cut the inter-related FEA reference models
- Based upon a particular subject matter (Expertise Area)
  - Security & Privacy (Phase I Final; 07/29/2004)
  - Records Management (Version 1.0; 12/15/2005)
  - Geospatial (Version 1.1; 01/27/2006)

- Describe how each Reference Model addresses Expertise Areas and how agencies can utilize resources, standards, best practices and use cases
TODAY: Department/Agency Reports required by OMB

For any IT project to be included for OMB review (i.e., Will the agency get its initial and continuing IT funding?) it must be “mapped” into the FEA.

Initial and on-going reports for FEA compliance:

- OMB Circular A-11; Exhibit 53 (IT Investment Portfolio)
- OMB Circular A-11; Exhibit 300 (Business Case)
- OMB Circular A-130; Appendix III (Information Systems Security)
  - Deficiencies & Material Weaknesses
  - Summary of Department/Agency Security Plans
From Clinger-Cohen CPlC – to- GISRA – to- FISMA . . .

Clinger-Cohen requires agencies to manage IT budgets by adhering to the CPlC process.

- Provided Management Framework for Security of Government IT
- Required Agencies to Assess the Security of IT systems
- Included Risk Assessments and Security Needs in Budget Requests

Federal Information Security Management Act (FISMA - December 2002)
- Title III of the E-Government Act
- Replaced GISRA
- FISMA Emphasizes a Risk-based Policy for Cost-Effective IT Security
FISMA requires executive agencies within the federal government to:

- Plan for Information Systems Security
- Ensure that Appropriate Officials are Assigned Security Responsibility
- Periodically Review the Security Controls in their Information Systems
- Authorize System Processing Prior to Operations, and
- Authorize System Processing Periodically thereafter

“Federal IT Managers and officials must understand the current status of their Security Programs and the security controls planned or in place to protect their information and information systems in order to make informed judgments and investments.” - E-Gov Act; Title III; FISMA (2002)

FISMA also authorizes and empowers the National Institute of Standards and Technology (NIST) to develop and implement a suite of security standards and guidelines required by the legislation.
FISMA Implementation focuses on the development of a suite of security standards and guidelines (NIST) necessary to create a robust information security program and effectively manage risk to agency operations and agency assets.

- **FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems**
- **NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories**
- **NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems**
Information Systems Security Standards & Guidance

Security Standards and Guidelines Development continued . . .


- NIST Special Publication 800-59, *Guide for Identifying an Information System as a National Security System*


- NIST Special Publication 800-26 Rev. 1, *Assessment Guide for Information Systems and Security Programs*

NIST publishes two types of security documents:
1) Federal Information Processing Standards (FIPS); and
2) Special Publications (800-series guidance).

IT’S THE LAW!
FISMA requires Federal Departments/Agencies to comply with FIPS. FIPS are mandatory and non-waiverable. Office of Management and Budget policy requires Federal Government to comply with NIST Special Publications (800-series guidance). The compliance dates for NIST Security Standards and Guidelines are as follows:

⇒ For legacy information systems, compliance with NIST security standards and guidelines within one year of the final publication date.

⇒ For information systems under development, compliance with NIST security standards and guidelines immediately upon deployment of the information systems.
GIS and the Federal Government . . .

Electronic Geospatial Information Systems (GIS) data resides in two basic areas:

- Bulk in some form of repository, such as a database or collection of individual files (called *Data at Rest*)
- Small quantities being transmitted over networks or the Internet (called *Data on the Wire*)

GIS data is vulnerable no matter where it resides. While most agencies take precautions, many of those precautions turn out to be woefully lacking mandated management, personnel, operational and technical controls. The key lies in knowing the regulations and guidance that implements an approved Information Systems Security capability, knowing where vulnerabilities exist and making appropriate risk-based decisions.
GIS and the Federal Government . . .

The **assessment of risk** and the development of **security plans** are two important activities in an agency's information security program that directly support the security accreditation process and are required under FISMA and OMB Circular A-130.

The classification of data sensitivity and its relative importance to overall success of “agency mission” is integral to the **assessment of risk**. And, all federal information systems must undergo the process of **Certification & Accreditation** – no matter if they are legacy systems, new software systems ready for production, or planned systems only in development.
Risk Assessments . . .

- Influence the Development of the Security Requirements for Information Systems
- Influence the Security Controls implemented for Information Systems
- Generate information needed for System Security Plans (SSP)
- Influence the success of Certification and Accreditation (C&A)

✓ Varying guidance for civilian and defense
✓ All now must follow Security “Best Practices” and NIST Guidance:
  ⇒ Civilian: C&A, SCAP, etc.
  ⇒ DoD: DI TSCAP (coming soon . . . DI ACAP)
Risk Assessment Methodology . . .

- Identify System Assets (System Characterization)

- Define System Security Needs (Data Sensitivity Analysis, Rules of Behavior, etc.)

- Identify System Threats

- Analyze System Vulnerabilities

- Evaluate possible compromise to system and its mission

- Determine Risk Levels

- Develop the Risk Assessment Report
Information Systems Security

Risk Assessment Methodology

- Identify System Protection Needs
  - Confidentiality
  - Integrity
  - Availability

- Define System Security Needs

- System Characterization
  - System Assets
  - Architecture
  - Configurations
  - Major Elements
  - Sites/Locations

- System Criticality/Data Sensitivity
  - Mission Support?
  - Critical?
  - Essential?
  - Routine?
  - Secret?
  - Unclassified/FOUO
  - Sensitive

- Identify System Threats
  - Computers
  - Network
  - Data/Information
  - Physical Threats
  - Environmental

- System Vulnerability Analysis
  - Threat/Vulnerability Pairing
  - Countermeasures
  - Assess Control Areas

- Controls/Vulnerability Areas
  - Technical
  - Operational
  - Administrative
  - Personnel
  - Physical (Facility)
  - Difficulty?
    - Expert
    - Technical
    - Novice

- Likelihood/Ease Criticality/Severity Of System Loss
  - HIGH (1)
  - MEDIUM (2)
  - LOW (3)

- Risk Determination
  - AND
  - Risk Ranking

- Risk Assessment Report
  - Report of Findings
  - Recommendations
  - Additional Security Controls
All agencies must implement the requirements of FISMA and report annually to OMB on the effectiveness of their security programs. OMB uses the information to help evaluate agency-specific and government-wide security performance, develop its annual security report to Congress, assist in improving and maintaining adequate agency security performance, and inform on the development of the E-Government Scorecard under the President’s Management Agenda. OMB uses a simple color-code to visually rank each agency’s “at-risk” status (Green = Fully Compliant, Yellow = With Issues, and Red = Non-compliant).

If an agency is not “in the Green” (i.e., at-risk) then they stand a good chance of not receiving and/or maintaining funding for their IT budgets. **As GIS begins to take a more prominent position in the Federal Enterprise Architecture, GIS systems MUST come into compliance with FISMA and its related mandates.** We should provide the expertise and tools to assist those agencies in meeting their Information Systems Security goals.
President’s Geospatial One-Stop Initiative . . . provide Federal, State, local and tribal agencies with a single point of access to map-related data enabling consolidation of redundant data. The goal is to improve the ability of the public and government to use geospatial information to support the business of government and improve decision making. Geospatial One-Stop awards contract to ESRI for Version 2 portal February 2, 2005.

OMB has issued guidance (i.e., OMB Circulars A-11 and A-16) providing direction for Federal agencies producing, maintaining or using spatial data either directly or indirectly in the fulfillment of their mission. This direction includes general responsibilities for preparing, maintaining, publishing and implementing a strategy for advancing spatial data activities in support of the National Spatial Data Infrastructure (NSDI) strategy. It instructs agencies to use Federal Geographic Data Committee (FGDC) data standards. Annual reporting through A-11 Exhibit 300 submissions is also required.
Thank You for your Time and Attention!

Penobscot Bay Media, LLC
32 Washington Street, Suite 230
Camden, ME 04841
207-230-0182 www.penbaymedia.com

Alan Butler abutler@penbaymedia.com