Information Systems Security Requirements for Federal GIS Initiatives

Paper #1042

Presented at the ESRI 2006 Federal User Conference
Washington, DC

Session Title: Industry Perspectives on Enterprise GIS
Date: Wednesday, February 1, 2006
Time: 10:30 a.m. - 12:00 noon

Author
Alan R. Butler

Penobscot Bay Media, LLC
32 Washington Street, Suite 230
Camden, ME 04841

ABSTRACT

As Geospatial Information Systems take a more prominent position in the Federal Enterprise Architecture, GIS systems must come into compliance with Federal regulations and guidance mandates for Information Systems Security. A compliant, well-crafted capability establishes the minimum set of controls to be included in GIS-related information systems security programs; assigns agency responsibilities for security of GIS data and information; provides appropriate SDLC information systems security guidelines for government workers and contractors developing and maintaining GIS products and services; and, links agency GIS information security programs and management control systems to the Federal Enterprise Architecture. We will also specify, in a “methods to approach” manner, specific initiatives directed toward risk and data sensitivity analyses of GIS data and information, and how this particular effort is critical to Federal agency Systems Security Planning (SSP) efforts—an integral part of the Certification and Accreditation (C&A) process for all Federal GIS information systems.

PAPER

"We are 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.”

– National Research Council in *Computers at Risk*

“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

Laws and Regulations

The Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)), also known as the Information Technology Management Reform Act, was intended, among its many other purposes, to "reform acquisition laws and information technology management of the Federal Government." The Clinger-Cohen Act established a definition of information technology that has since been cited in numerous other Federal laws.

The term *information technology*, with respect to a Federal department or agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by any department/agency. As regards this preceding sentence, *equipment* is used by a department/agency if the equipment is used by the department/agency directly or is used by a contractor under a contract with the department/agency which requires the use of such equipment, or requires the use, to a significant extent, of such equipment in the performance of a service or the provisioning of a product. The term *information technology* includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Given these definitions, the term *information technology* does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

The Clinger-Cohen Act provided that government information technology (IT) be operated exactly as an efficient and profitable business would be operated. Acquisition, planning and management of technology must be treated as a *capital investment*. In concert with this provision, Clinger-Cohen implemented the Capital Planning Investment Control (CPIC) IT budget planning process, and 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. Furthermore, the Clinger-Cohen Act established Chief Information Officer (CIO) positions in every department and agency in the Federal government, established the CIO Council (CIOC) from twenty-eight major agencies and OMB, and defined the Information Technology Architecture (ITA) for evolving and acquiring information technology.

In 2001, as part of the President's Management Agenda (PMA), OMB's Office of E-Government and Information Technology (E-Gov & IT) was formed and extended guidance and support to the General Services Administration (GSA) and the CIOC. On February 6, 2002 the development of a Federal Enterprise Architecture (FEA) commenced. As stated on the E-Gov web site FEA home page, "Led by OMB, the purpose of this effort is to identify opportunities to simplify processes and unify work across the agencies and within the lines of business of the Federal government. The outcome of this effort will be a more citizen-centered, customer-focused [and market-based] government that maximizes technology investments to better achieve mission outcomes." This important step also established the Federal Enterprise Architecture Program, which replaced the ITA, leading the way to evolve a comprehensive business-driven blueprint of the entire Federal Government.

The 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 to facilitate the description and analysis of IT investments and enhance collaboration.

The FEA, aligned through a collection of interrelated *Reference Models*, is designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across Federal Agencies.

PRM *. . . Performance Reference Model*
BRM *. . . Business Reference Model*
SRM *. . . Service Reference Model*
DRM *. . . Data Reference Model*
TRM *. . . Technical Reference Model*

FEA Profiles are frameworks that cross-cut the inter-related FEA Reference Models based upon a particular subject matter. The profiles describe how each Reference Model addresses a specific area and how agencies can utilize existing resources, standards, best practices and use cases to implement or improve upon them.

- **Security & Privacy** (Phase I Final; 07/29/2004) provides guidance on designing and deploying measures that ensure the protection of information resources.

- **Records Management** (Version 1.0; 12/15/2005) provides an overview of the FEA and explains how the reference models provide a context for applying effective records management practices.

- **Geospatial** (Version 1.1; 01/27/2006) establishes a framework for more effective use and management of geospatial data and services as part of agencies' enterprise architectures. It describes how agencies can leverage geospatial data and technologies to enhance service delivery and mission accomplishment.

For any Federal Information Technology 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. Examples of initial and on-going reporting directives for FEA compliance include:

- 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

The E-Government Act (Public Law 107-347) passed by the one hundred and seventh Congress and signed into law by President George W. Bush in December 2002 recognized the importance of information security to the economic and national security interests of the United States. **Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA)**, emphasizes the need for Federal departments and agencies to develop, document, and implement organization-wide programs to provide information security for the information systems that support their operations and assets. FISMA superseded the Government Information Security Reform Act, or GISRA, which expired in 2002. While GISRA provided a management framework for security of Government IT and required agencies to assess the security of IT systems including *Risk Assessments* and security needs in budget requests, FISMA expands on these mandates and emphasizes a Risk-based Policy for cost-effective Information Systems Security.

With the passage of FISMA, there is no longer a statutory provision to allow for agencies to waive mandatory Federal Information Processing Standards (FIPS). The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, the references to the "waiver process" contained in prior regulatory guidance are no longer operative.

Furthermore, the requirements of FISMA and the Office of Management and Budget's (OMB) Circular A-130, Appendix III require annual reporting by all Federal agencies to both OMB and Congress on the effectiveness of their information systems security programs. OMB uses this 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 development of the E-Government Scorecard under the President's Management Agenda. This report data, in conjunction with mandated FEA compliance report data submitted as part of the annual CPIC process, assists OMB in developing its criteria for annual Federal Information Technology budget recommendations. Without favorable results, Federal agencies risk being denied legacy and new project funding within their yearly IT budgets.

As Geospatial Information Systems take a more prominent position in the FEA, they must come into compliance with Federal regulations and guidance mandates for Information Systems Security. The compelling reasons for GIS systems to fall in line with the stated regulations and guidance mandates are two-fold in nature: 1) Federal agencies may no longer waive Information Systems Security requirements, and 2) without favorable evaluative results in the yearly OMB reporting process funding may be severely reduced or even denied for both legacy and new GIS-related projects.

Federal agencies must plan for GIS Information Systems Security, ensure that the appropriate officials are assigned security responsibility, and authorize GIS systems processing prior to production operations and periodically thereafter. These management responsibilities presume that responsible agency officials understand the risks and other factors that could negatively impact their mission goals. Moreover, these officials must understand the current status of

security programs and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

Regulatory Guidance – National Institute of Standards and Technology

Information Systems Security standards and guidance are available for organizations that are part of or do business with the U.S. government. FISMA assigned the Computer Security Division of the National Institute of Standards and Technology (NIST) the important, multi-part task of developing and publishing these standards and guidance documents. The compliance timelines for NIST Information Systems Security standards and guidelines are as follows:

- For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines **within one year of the final publication date**.

- For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines **immediately upon deployment** of the information systems.

The NIST *FISMA Implementation Project* was established in January 2003 to produce the key Information Systems Security standards and guidelines required by the aforementioned legislation. These publications include FIPS 199, FIPS 200, and the series of NIST Special Publications (SP). All of these standards and guidance documents have reached their final publication date (with revision publications following periodic review and as warranted) with the exception of FIPS 200, which is due for final publication on or about April 2006, and SP 800-53A, which is due for final publication on or about October 2006.

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements) *draft*
- NIST SP 800-18, Rev 1 (Security Planning)
- NIST SP 800-26, Rev 1 (Reporting Formats)
- NIST SP 800-30 (Risk Management)
- NIST SP 800-37 (Certification & Accreditation)
- NIST SP 800-53 (Recommended Security Controls)
- NIST SP 800-53A (Security Control Assessment) *draft*
- NIST SP 800-59 (National Security Systems)
- NIST SP 800-60 (Security Category Mapping)

Security Commensurate with Risk

Federal Information Systems Security management responsibilities presume that responsible agency officials understand the risks and other factors that could adversely affect their missions. Moreover, Federal officials must understand the current status of their Information Systems 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 that appropriately mitigate risk to an acceptable level.

The ultimate objective of a comprehensive Federal GIS Information Systems Security program should be to enable day-to-day operations and to accomplish a given department or agencies' stated missions with *adequate security*, or **security commensurate with risk**, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of GIS systems data and information.

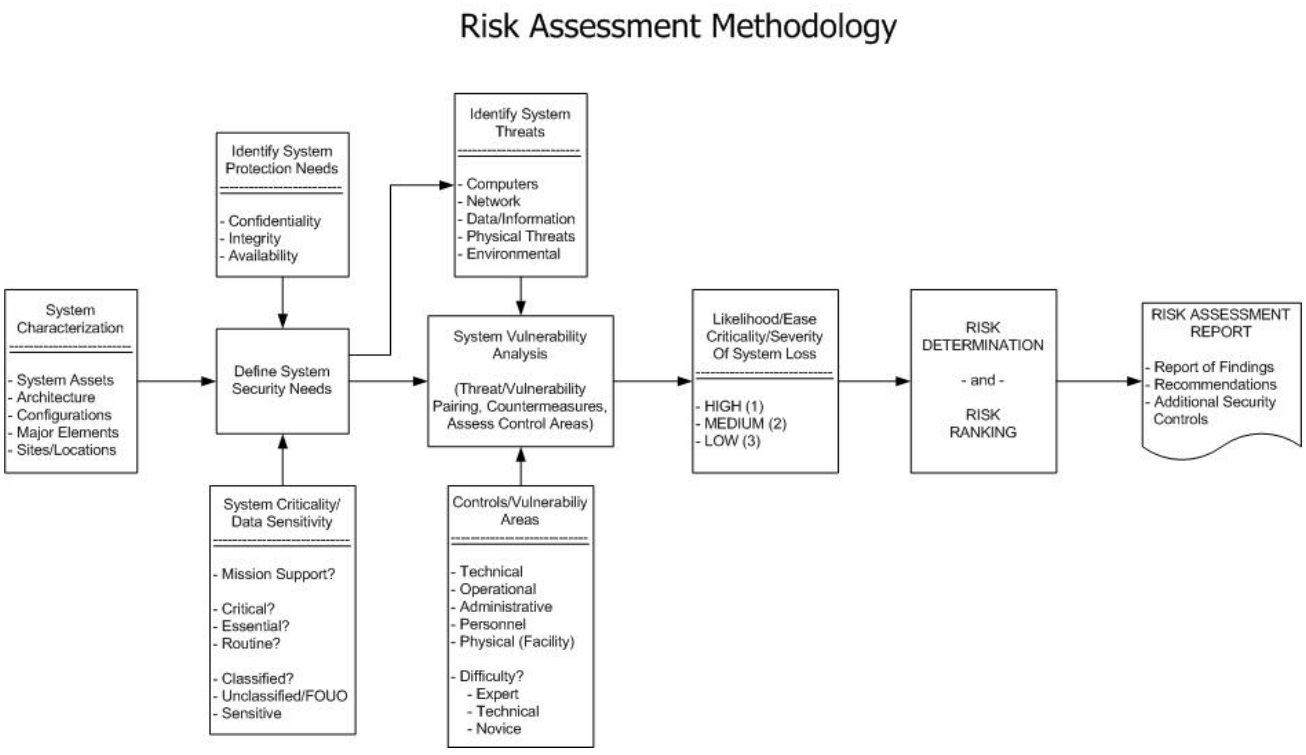
The *assessment of risk* and the development of *security plans* are two important activities in an agency's information security program that directly support the security accreditation process and are required under FISMA and OMB Circular A-130.

The classification of data sensitivity and its relative importance to the 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—as either a Major Application or as part of a General Support System.

Risk Assessments influence the development of the security requirements for GIS Information Systems, influence the security controls implemented, generate information needed for Information System Security Plans (ISSP), and influence the success of Certification and Accreditation (C&A). While there is varying localized, agency-developed controls—both civilian and defense—all must now follow security "Best Practices" and NIST guidance: Civilian . . . C&A, SCAP, etc., and DoD . . . DITSCAP (coming soon . . . DIACAP).

A well-defined Risk Assessment Methodology serves to 1) identify system assets (System Characterization), 2) define system security needs (Data Sensitivity Analysis, Rules of Behavior, etc.), 3) identify system threats, 4) analyze system vulnerabilities and evaluate possible compromises to a system and its mission, 5) determine and rank risk levels, and 6) develop the ***Risk Assessment Report***.

The following flow chart exemplifies this process in its logical form.



Defining GIS System Security Needs

Defining GIS system security (protection) needs is accomplished by first determining system sensitivity requirements and severity (impact of GIS system loss) related to GIS data and information *confidentiality*, *integrity*, and *availability* defined as follows:

- **Confidentiality** – is the requirement that private or confidential GIS information not be disclosed to unauthorized individuals;
- **Integrity** – is the requirement that GIS information and programs are changed only in a specified and authorized manner. System integrity is a requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system;
- **Availability** – is the accessibility to GIS information or a GIS system on a timely basis to support agency mission requirements and deadlines. An important measure of availability is the length of time that the system can be non-operational without affecting a given agency's mission.

Sensitivity is the degree to which a system requires protection to ensure confidentiality, integrity, and availability. GIS system sensitivity needs should be based on an evaluation of high-level system requirements (e.g., policies, directives, orders, standards, guidance documents, system specifications, and user requirements), the GIS system environment, and the criticality of the GIS system including information stored, processed, or transported by the system. The GIS system environment is defined by the system architecture and physical locations where the system is installed. The GIS system environment includes the physical and electronic access to system assets or data for each type of site installation.

Federal mandates require that each system be designated as classified (Level I), sensitive (Level II), or other (Level III) based on the sensitivity and criticality of information collected, processed, transmitted, stored, or disseminated therein. This criteria is specified per the following:

- **Classified (Level I)** – Classified information including Confidential, Secret and Top Secret.

- **Sensitive (Level II)** – Unclassified information requiring special protection; for example, Privacy Act, For Official Use Only (FOUO), and technical documents restricted to limited distribution. Level II is further divided into high, medium and low categories, in order to determine the level of protection required, for this sensitivity level. These categories are used to assist in determining minimum security specifications for the level of system protection needed to meet the requirements for confidentiality, integrity and availability.

- **Other (Level III)** – All other unclassified information. (Note: OMB Circular A-130 now defines all Government systems as **Sensitive**; hence Level III is no longer applicable).

The severity of impact is represented by the potential loss of confidentiality, integrity, and/or system availability, which affects GIS system assets or data. This impact is measured by loss of system functionality, impedance or inability to meet a given agency's mission, dollar losses, loss of life, loss of functional control, loss of safety, loss of public confidence, or unauthorized disclosure of data. The impact is determined by evaluating system assets, system requirements, and the information stored, processed or transported by the system. Severity of impact is determined by using a qualitative ranking of high, medium or low for system confidentiality, integrity, and availability, as indicated in the following table.

Severity of Impact Determination

Severity of Impact	Confidentiality	Availability	Integrity
High • Very serious; • Complete loss of mission capability for an extended period; or • Would result in the loss of major assets or resources and could pose a threat to human life.	High = 3	High = 3	High = 3
Medium • Moderately serious; • Severe impairment to agency missions, functions, image, and reputation. The impact would place the agency at a significant disadvantage; or • Would result in MAJOR damage, requiring extensive repairs to assets or resources.	Medium = 2	Medium = 2	Medium = 2
Low • Negligible. Not serious; • Noticeable impact on agency missions, functions, image, or reputation. A breach of this security level would result in a negative outcome. • Systems failure, damage or disruption which reduces functional capabilities or system performance and/or requires local restoration of system capabilities. • Would result in DAMAGE, requiring repairs, to an asset or resource. • Includes a recoverable loss of redundancy or backup capability in operations or support systems and/or self-repairing and limited damage or disruption to system functions.	Low = 1	Low = 1	Low = 1

Analyzing GIS System Threats

A threat is any event, process, activity or action with the potential to cause harm to a GIS system or that exploits a vulnerability to attack a GIS asset. It is any force or phenomenon that could degrade the confidentiality, integrity, or availability of said asset. The capabilities, intentions and attack methods of hostile entities that have a potential to cause harm to the system must be identified and evaluated.

Threat agents/actions used in the Risk Assessments are based on the threats identified in NIST and any subsequent agency-developed guidance. Four primary categories of threats are considered for Risk Assessments as follows:

- **Computer system threats** – are events, actions or agents that can destroy or disrupt assets, corrupt system resources, or compromise integrity of the asset.
- **Information threats** – are events, actions or agents that can cause disclosure, corruption, modification or deletion/loss of system data, documentation or information.
- **Communications threats** – are events, actions or agents that can cause disruption of communication assets and connectivity resources, which will impact the system availability.

- **Physical/Environmental threats** – are non-technical events, actions or agents that could compromise the availability or integrity of the system.

Initially a significant group of potential threats are considered for each of these threat categories. Then, based on the GIS system, its architecture, the security needs, and the system environment, threats are evaluated to determine their applicability to the GIS system. After the vulnerabilities to an asset are identified, threats deemed applicable to the GIS system are paired with that particular vulnerability. This process leads to a combination or pairing of vulnerabilities (V_1) and threats (T_1), which can be assessed for the specific system.

Analyzing GIS System Vulnerabilities

Vulnerabilities are weaknesses in the physical layout, organization, procedures, personnel, management, administration, hardware, or software that may be exploited to cause harm to a GIS system. They include technical weaknesses in the systems' software, hardware, and communications facilities, as well as mechanisms that may be exploited. The same vulnerability can exist in more than one asset and the vulnerability can be exploited by more than one threat. A vulnerability analysis, in most assessment exercises, encompasses the following five security control areas:

- **Technical** – are weak countermeasures in hardware, software, GIS system architecture, and modes of communication. Examples include insufficient security software controls and mechanisms, faulty operating system code, lack of virus controls and procedures, and lack of authentication and access controls.
- **Operational** – are weak countermeasures in the operational procedures that people perform with respect to a GIS information system. More often than not, these vulnerabilities stem from the lack of (or an insufficiency in) the various practices and procedures that are critical to the secure operation of a GIS system. Examples of operational vulnerabilities include the lack of adequate security awareness and training, security monitoring and detection provisions, and security auditing and the absence of some or all of the procedural documentation critical to an effectively applied and managed security program.
- **Administrative** – are weak countermeasures in the administrative procedures that affect information systems in an organization. Examples include lack of adequate security policies and implementing procedures, insufficient security life cycle procedures, administration and controls, and lack of addressing standards**.**
- **Physical** – are weak countermeasures in the physical layout of, and access to, the facilities and enclosures where the GIS information systems are housed. Such weaknesses include inadequate**/**ineffective physical access controls**/**intrusion detection, lack of appropriate structural or environmental protective measures or deficient security controls for the physical facility (e.g., perimeter monitors, fencing, door locks).
- **Personnel** – are weak countermeasures in the policy, process and procedures used for security screening of staff having access to the GIS information system. This includes aspects such as hiring practices, background clearance checks, and security training and awareness related to the job functions an individual performs.

GIS Data Protection

How do we defend against the myriad of possible attack vectors? The key is to focus on the GIS data. The first step should be a ***Data Sensitivity Analysis*** as part of an overall Risk Assessment and Management process. Data Sensitivity Analysis begins by identifying an organization's critical GIS data and ways in which that data is used. Once the sensitivity of data has been classified, the organization can reach decisions about the necessary level of protection for their GIS data. A tendency may be to apply the greatest level of protection available, but that level may

be neither necessary nor cost-effective. For example, we wouldn't recommend spending $100,000 on a firewall to protect an expected loss of only $5,000. We get a better idea of how to apply countermeasures if we include a ***Loss/Impact Analysis*** as part of the Risk Assessment process.

A Simple Approach to GIS Data Protection . . .

A simple approach to data protection looks at the various layers of security that can be applied. Consider the following starting checklist:

- *GIS Data Repository:*
  - Should the agency encrypt the GIS data repository?
  - Does the agency need a hash of GIS transactions for integrity purposes?
  - Should the agency digitally sign GIS transactions?
  - Is the agency's GIS database logging enabled and properly configured?
- *GIS resident server considerations:*
  - Harden the operating system.
  - Disable unnecessary services and close ports.
  - Change system defaults.
  - Group or shared account passwords should not be utilized.
  - Lock down file shares.
  - Restrict access to only necessary personnel.
  - Consider host-based firewalls and intrusion detection for critical servers.
  - Maintain proper patch procedures.
- *Network segment:*
  - Use switches rather than routers or hubs as much as possible.
  - Lock down unused router/switch ports.
  - Consider MAC filters for critical systems.
  - Establish logical subnets and VLANs.
  - Set up access control lists (ACLs) for access routes.
  - Use ingress/egress filters, anti-spoof rules.
  - Determine appropriate location and functionality for network-based firewalls and intrusion detection.
  - Use encrypted logins or SSL for web-based sessions.
- *Physical security for GIS data:*
  - Establish input/output handling procedures.
  - Use physical access logs for server rooms and network operations centers.
  - Document tape-handling procedures, tape rotation, offsite storage.
  - Consider an alternate data center or facility.
  - Archiving: Where does the agency's GIS data go to be archived?
  - Data destruction: Degauss, erase/overwrite, physical destruction?
  - How is GIS data handled when equipment is sent out for repair, replacement, or end of life?

This is just a quick list of points to consider and can easily be expanded upon as warranted.

Federal Certification and Accreditation (C&A) of GIS Systems

The C&A process is explained and documented in NIST publication SP 800-37 (Certification & Accreditation). The NIST guidelines provide the requisite framework for selecting, specifying, employing, and evaluating the security controls in information systems. These guidelines must be applied to any/all GIS information systems that reside in the Federal Enterprise Architecture.

The following basic outline for the C&A of any given GIS system adheres to the process guidance for Federal information systems:

- System Characterization
- Risk Assessment
- Plan of Action & Milestones (POAM)
- Security Test Plan & Results of Test(s) (ST&E)
- Information Systems Security Plan (ISSP)
    - Analysis (Boundaries and Categories)
    - Definition of System Information
    - Management Controls
    - Operational Controls
        - Major Application
        - General Support System
    - Technical Controls
        - Major Application
        - General Support System
    - Personnel Controls
        - Rules of Behavior
- Continuity of Operations Plan (CoOP) / Disaster Recovery
- Final Report
    - Certification Statement
    - Executive Summary
    - ISSP, ST&E, POAM, ISSP, CoOP, etc.

A Phased Approach to the C&A Process for GIS Systems

Phase I – Assessment

- Outline Tasks and Estimate Completion Costs
- System Inventory and Asset Identification
- Outline Tools to be used, Methods Employed and Schedule
- Perform Assessment
- Deliverables
    - ISS Initial Survey
    - System Protection Remediation Schedule
    - System Inventory and Asset Identification Report
    - Vulnerability Assessment Plan
    - Vulnerability Assessment Report

Phase II – Security

- Perform Risk Assessment
    - Includes Data Sensitivity Analysis
- Determine Remediation Efforts and Methods
- Consolidate documentation for ISSP
- Document Contingency and Disaster Recovery measures
- Deliverables

    - Risk Management Plan
    - Security Remediation Plan
    - ISSP
    - CoOP/Disaster Recovery Plan

Phase III – Remediation

- Implement Changes outlined in Phase II Plans
- Outline Security Test Procedures
- Document existing Security Tests
- Perform Security Tests and Evaluation (ST&E)
- Report Results of ST&E
- Deliverables
    - Security Remediation Report
    - Security Test Plan
    - Security Test Report

Phase IV – Certification

- Summarize Certification and Accreditation (C&A) activities
- Develop Deployment Plan including Remediation Intent
- Deliverables
    - Executive Summary
    - C&A Certification
    - Deployment Plan

Phase V – Deployment

- Necessary Changes are made to GIS and Supporting Infrastructure
- Deploy Certified and Authorized GIS Information System
- Deliverables
    - Deployment Report

CONCLUSION

Again, the requirements of the Federal Information Security Management Act (FISMA) and the Office of Management and Budget's (OMB) Circular A-130, Appendix III require annual reporting by all Federal agencies to both OMB and Congress on the effectiveness of their information systems 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 development of the E-Government Scorecard under the President's Management Agenda. This report data, in conjunction with mandated FEA compliance report data submitted as part of the annual CPIC process, assists OMB in developing its criteria for annual Federal Information Technology budget recommendations. Without favorable results, Federal agencies risk being denied legacy and new project funding within their yearly IT budgets.

A compliant, well-crafted capability will establish the minimum set of controls to be included in GIS-related information systems security programs; assign agency responsibilities for the security of GIS data and information; provide the appropriate systems development life cycle (SDLC) information systems security guidelines for government workers and contractors alike developing and maintaining GIS products and services; and, link agency GIS information security programs and management control systems to the Federal Enterprise Architecture. As stated in Appendix III to OMB Circular No. A-130, "This includes assuring that systems and applications used by [any] agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls."

CITATIONS

- Computer Security Act of 1987
- Information Technology Management Reform Act of 1996 - Clinger-Cohen Act (40 U.S.C. 1401(3))
- Presidential Decision Directive 63 (PDD 63)
- E-Government Act of 2002
- Federal Information Security Management Act of 2002 (FISMA); Title III of the E-Government Act of 2002
- Office of Management and Budget (OMB) Circular A-11; Part 7; Section 300 (Planning, Budgeting, Acquisition and management of Capital Assets)
- Office of Management and Budget (OMB) Circular A-11; Section 53 (Information Technology and E-Government)
- Office of Management and Budget (OMB) Circular A-16 (Coordination of Surveying, Mapping, and Related Spatial Data Activities)
- OMB Circular A-119 (Federal Participation in the Development and Use of Voluntary Consensus Standards and In Conformity Assessment Activities)
- Office of Management and Budget (OMB) Circular A-123 (Management Accountability and Control)
- Office of Management and Budget (OMB) Circular A-130 (Management of Federal Information Resources)
- Office of Management and Budget (OMB) Circular A-130; Appendix III (Security of Federal Automated Information Resources)
- Presidential Memorandum; M-05-15; June 13, 2005 (FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management)
- Department of Transportation (DOT) Handbook (DOT H 1350.2, Departmental Information Resources Management Manual (DIRMM))
- Department of the Interior (DOI) Departmental Manual Chapter 375 DM 19, "Information Technology Security Program"

REFERENCES

- http://www.whitehouse.gov/omb/egov/; Federal Enterprise Architecture Reference Models
- http://www.whitehouse.gov/omb/egov/; FEA Profiles and Case Studies
- *Overview of the Federal Enterprise Architecture*; Office of Management and Budget (OMB); February 2004
- 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*
- NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*
- NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
- NIST Special Publication 800-59, *Guide for Identifying an Information System as a National Security System*
- FIPS Publication 200, *Security Controls for Federal Information Systems*
- NIST Special Publication 800-26 Rev. 1, *Assessment Guide for Information Systems and Security Programs*
- NIST Special Publication 800-18 Rev. 1, *Guide for Developing Security Plans for Information Systems*
- Implementing the President's Management Agenda for E-Government; E-Government Strategy; February 27, 2002; Appendix D. Initiative Summaries (Geospatial Information One-Stop)
- *Geospatial One-Stop Portal Is Key to President's E-Government Strategy*; Federal GIS Connections, ESRI, Fall 2003
- Executive Order 12906 (April 13, 1994); amended by Executive Order 13286 (March 5, 2003); Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure
- *Mapping the Risks, Assessing the Homeland Security Implications of Publicly Available Geospatial Information*; RAND National Defense Research Institute, RAND Corporation, 2004
- *Why Your Data is at Risk*, Randall Nash, 3 January 2005
- *Identifying Sensitive Critical Infrastructure Data*, Brent A. Jones, PE, PLS, 2005

AUTHOR INFORMATION

Alan R. Butler, CDP
Senior Project Manager
GeoInfoSec™ Practice Manager

Penobscot Bay Media, LLC
32 Washington Street, Suite 230
Camden, ME 04843
Voice: (207) 230-0182 x29
Fax: (207) 236-4977
E-mail: abutler@penbaymedia.com
On the web: http://www.penbaymedia.com