Global Information Assurance Certification Paper

GIAC LevelOne Security Essentials Practical Assignment

New Information Security Requirements for Federal Agencies

Robert Host
January 2001

Introduction

Federal government agencies are sure to take a close look at their information security programs this year as a result of the recently enacted Government Information Security Reform Act, part of the FY 2001 Defense Authorization Act (P.L. 106-398). This Act requires each agency to develop and implement an agency-wide information security plan for its assets and operations. It also requires this plan to be reviewed annually by agency program officials and Inspector General audits of information security programs and practices. There is a wide range of resources available to Federal IT employees and contractors alike who chose to take this opportunity to review and strengthen their agency's plan.

GAO Review of Federal Information Security Operations

A GAO report titled "Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk" was issued in September of 1998. The report found widespread and serious weaknesses in the Federal Government's ability to adequately protect federal assets from fraud and misuse. The report also found weaknesses in the ability of agencies to protect sensitive information from inappropriate disclosure and their critical operations from disruption.

Information Security Planning Requirements

The Government Information Security Reform Act (GISRA) builds on some previous requirements established by Office of Management and Budget (OMB). These requirements were

established in an effort to improve the information security posture of federal agencies. OMB policy requires agencies to implement and maintain a program to adequately secure their information and system assets. Agency programs must: 1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and 2) protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

New Requirements Imposed by GISRA

The new legislation reaffirms the need for each agency to develop and implement an agency-wide information security plan for its assets and operations. GISRA subjects each program to approval by the Director of the Office of Management and Budget (OMB)- or the Secretary of Defense and the Director of Central Intelligence for mission critical national security systems or intelligence information. The Act also requires agencies to follow OMB guidance to:

1) Ensure policies are founded on a continuous risk management cycle.

2) Implement controls that adequately assess information security risks.

3) Promote continuing awareness of information security risks.

4) Continually monitor and evaluate information security policy.

5) Control effectiveness of information security practices.

The Director of OMB oversees compliance with these requirements and is provided the authority to recommend reductions or increases in funds for information resources based on the amount proposed by the heads of agencies in their budget submissions. The Director also is provided

the authority to adjust or restrict existing information resource apportionments.

The Act also directs specific requirements directly to the head of each agency. They are responsible for:

1) Adequately ensuring the integrity, confidentiality, authenticity, availability, and nonrepudiation of information and information systems supporting agency operations and assets.

2) Developing and implementing information security policies, procedures, and control techniques sufficient to afford the security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the agency.

3) Ensuring that the agency's information security plan is practiced throughout the life cycle of each agency system and that risks associated with operations and assets for programs and systems are assessed, that appropriate levels of information security to protect such operations and assets are determined, and that there is periodic testing and evaluation of information security controls and techniques.

The CIO must be provided with the authority to develop and maintain an agency-wide information security program and ensure the agency effectively implements and maintains information security policies, procedures, and control techniques. Agency heads must ensure the availability of sufficient personnel to meet the requirements of the Act, and CIOs must are to ensure adequate training and oversight is provided for personnel with significant information security responsibilities. Agency heads are to ensure the CIO periodically evaluates the effectiveness of the information security program, including testing control techniques and implementation of remedial actions based on that evaluation.

OMB Guidance on Implementing GISRA

On January 16, 2001 the Office of Management and Budget issued a Memorandum M-01-08 to the heads of executive departments and agencies to assist them on carrying out the Act. This guidance notes that the Act covers both agency systems as well as those used by a contractor on behalf of an agency. Reports from the Inspector General evaluations and audits of systems and security programs are to be submitted to OMB. Agencies are to submit this information beginning in 2001 as part of the budget process. OMB will summarize the material received from agencies and send an annual report to Congress.

Improving Information Security in Government Agencies

While Federal IT workers should review GISRA to ensure their plans include the specific requirements cited in the Act, there are a variety of tools available which will assist in designing or improving an agency information security plan. The Federal CIO Council in November 2000 published "Federal Information Technology Security Assessment Framework", one of the most comprehensive frameworks for the foundation of an agency information security plan. The Framework provides for a consistent and effective measurement of the security status for agency IT assets.

Five levels of security are used to categorize agency assessments of their security programs and assist in prioritizing efforts for improvement. Ultimately, agencies should seek to bring all assets to level five.

Level 1 - Documented Policy
Level 2 - Documented Procedures
Level 3 - Implemented Procedures and Controls
Level 4 - Tested and Reviewed Procedures and Controls
Level 5 - Fully Integrated Procedures and Controls

The Framework recommends a self-assessment questionnaire be used by program officials to rate assets on a wide variety of security issues based on their sensitivity level.

Conclusion

OMB and Inspector Generals will almost certainly look to see not only that agencies comply with the requirement to have an information security plan, but also to see if that plan is comprehensive, consistent with best practices, updated, and followed. They may also review agency risk mitigation efforts. It is important for federal IT workers to take this opportunity to review materials which will aid them in developing strong information security plans that address these concerns. The speed and adequacy to which each agency addresses the requirements of GISRA may have a direct impact on the level of information resource funding that agency is provided by Congress in future appropriations.

Sources

Federal CIO Council. "Federal Information Technology Security Assessment Framework" 28 November 2000. URL: http://www.cio.gov/docs/federal_it_security_assessment_framework.htm

GAO. "Information Security: Opportunities for Improved OMB Oversight of Agency Practices" September 1996. URL: http://www.gao.gov/AIndexFY96/abstracts/ai96110.htm

GAO. "Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk" GAO/AIMD-98-92 September 1998. URL: http://www.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:ai98092.txt

OMB. "Management of Federal Information Resources" Circular No. A-130. 30 November 2000. URL: http://www.whitehouse.gov/OMB/circulars/a130/a130trans4.html

U.S. Congress. "Government Information Security Reform Act" as part of the appropriations for the fiscal year ending September 30, 2001. URL: http://www.gpo.gov