**DEPARTMENT OF HEALTH & HUMAN SERVICES**
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850


***CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)***
***Office of Information Services (OIS)***
***Security and Standards Group (SSG)***
7500 Security Blvd
Baltimore, MD 21244-1850

# *CMS Information Security and Privacy Legislation Resource*

***Version # 2***
**February 25, 2003**

# Table of Contents

# 1. Explanation of Changes:

The status of the following has changed from the previous reviews:

- GISRA has been removed from Active Legislation to Expired Legislation
- The Homeland Security Act has been moved from Pending Legislation to Active Legislation.
- Cyber Security Research Act has been moved from Pending Legislation to Active Legislation.
- Development Act has been moved from Pending Legislation to Active Legislation.
- E-Government Act of 2002 has been moved from Pending Legislation to Active Legislation.
- The Paperwork Reduction Act was added to Active Legislation.

As of November 2002, the Government Information Security Reform Act (GISRA) expired. Congressman Tom Davis (R-VA) introduced H.R. 3844, The Federal Information Security Management Act (FISMA), to the House of Representatives as a replacement for GISRA. FISMA of 2002, which was passed as TITLE X of The Homeland Security Act (signed into law on November 27, 2002) and TITLE III of the E-Government Act of 2002 (signed into law on December 17, 2002) are now in effect. JANUS completed an analysis of the two versions of FISMA enacted by Congress. This analysis reveals that the text of TITLE III of the E-Government Act incorporates the text of TITLE X of the Homeland Security Act in its entirety with the following additions:

<u>New paragraphs</u>
Subsection 3542 (b) (2) (A) (ii)
Subsection 3543 (a) (7)
Subsection 3543 (8) (B)
Subsection 3543 (c)
Subsection 11331 (b)
Subsection 11331 (c)
Subsection 11331 (g)
Section 303 (d) (6)
Section 303 (f)

<u>New Subsection:</u>
Section 3546

TITLE III of the E-Government Act supersedes TITLE X of the Homeland Security Act "in those occurrences where both Acts prescribe different amendments to the same provisions of the United States Code"[1].

Furthermore, The Computer Security Act Section 11332 of Title 40, United States Code was repealed under FISMA. Section 11332 of Title 40, was added to the United States Code by

[1] George W. Bush ,The White House, For Immediate Release, Office of the Press Secretary, December 17, 2002 "President Signs E-Government Act" Statement by the President

Public Law 107-217 August 21, 2002. Section 11332 addressed the federal computer system security plan and training. The subject areas of Section 11332 of Title 40, United States Code are incorporated in the E-Government Act of 2002. The Computer Security Act allows agencies to obtain waivers from following National Institute of Standards and Technology (NIST) recommendations. FISMA grants more responsibility to NIST to develop and maintain standards for minimum information security controls. Compliance with the standards will be compulsory.

# 2. Introduction

This document identifies the current and potential legal requirements facing the Centers for Medicare & Medicaid Services (CMS) in information security. Implications of enacted and pending Bills for CMS have been included with each of the entries.

**Section 1:** Summaries of laws, regulations and standards to which CMS must currently adhere.

**Section 2:** A self-assessment tool including a checklist of legal directives for determining compliance with specific objectives. Cross-references to enacted legislation are included.

**Section 3:** Pending laws that are not yet legally binding, and their potential impact on CMS.

**Section 4:** Expired public laws that do not have a potential impact on CMS.

Each section has an introduction that describes both the section's contents, and the format of the information included.

# 3. Legislation Presenting Implications for CMS

The following section contains summaries of the laws currently in place that affect information security and privacy policies, practices, and procedures in place at CMS. Following each summary is a list of the specific requirements for CMS that are stipulated by the law.

The laws in this section are presented in the order in which they were enacted.

## 3.1 The Privacy Act of 1974

**Description:**

The Privacy Act of 1974 (5 U.S.C. Section 552a) is designed to protect an individual's right to determine the extent of the dissemination of personally identifiable information regarding herself/himself.

Under this law, each agency maintaining information systems that contain or access sensitive information shall only store personally identifiable information about an individual if that information is necessary to accomplish the goals of the agency established by executive order of the President. When collecting this information, the agency must inform an individual of his/her rights regarding the collection and dissemination of that information, as well as the purpose for which the information is being collected in the first place. In addition, the Privacy Act affords individuals the right to gain access to records for any purpose including the making of corrections to stored data.

**Implications for CMS:**

- CMS is directed to maintain in its records only such information about an individual as is relevant and necessary to meet the agency mission.
- CMS must establish procedures to notify an individual that the agency maintains records about her/him, and the reason for maintaining the information.
- CMS must establish procedures to allow individuals access to their records.
- CMS must define reasonable requirements to identify an individual who requests his/her record or information pertaining to her/him before making the record or information available.
- Procedures must be established for reviewing requests from individuals concerning the modification of any record or information pertaining to the individual.
- CMS must establish procedures and guidelines for releasing or disclosing data only after appropriate review or with prior written consent of the individual to whom the information pertains.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/bdquery/z?d093:SN03418:|TOM:/bss/d093query.html|
Cornell University
http://www4.law.cornell.edu/uscode/5/552a.html

## 3.2 Computer Security Act of 1987

**Description:**

The Computer Security Act of 1987, Public Law 100-235, establishes the first mechanism for minimum security standards for Federal information systems.

The law requires all agencies with computer systems that contain or use sensitive information to follow guidelines and standards defined by the National Institute of Standards and Technology (NIST). These standards are to be submitted to the Secretary of Commerce by NIST and promulgated under section 111(d) of the Federal Property and Administrative Services Act of 1949.

The most significant requirements of the Computer Security Act of 1987 are that CMS follow NIST standards for System Security Plans (plans must be written for all systems that contain, modify, or use sensitive information) and that the agency must provide mandatory training for all operators and maintainers of sensitive information systems. The mandatory training must be directed at achieving greater security and shall be guided by NIST.

**Implications for CMS:**

- The Bill "creates a means for establishing minimum acceptable security standards" to be developed by NIST, promulgated by the Secretary of Commerce. These standards apply to all federal computer systems.
- The CMS Administrator may employ standards of security that are more stringent than those distributed by the Secretary of Commerce only if the standards fully encompass and exceed the provisions defined by the Secretary.
- All computer systems that contain sensitive information must be identified.
- CMS must develop and maintain system security plans for the security and privacy of each federal computer system that contains sensitive information.
- A summary of these plans should be included in the agency's five-year plan. This plan is subject to disapproval by the Director of the Office of Management and Budget and must be revised annually as needed.
- Requires periodic training for all "persons involved in management, use, or operation of federal computing systems that contain sensitive information."
  i. Guidelines for the training are set by NIST.
  ii. Training should be designed to encourage the use of improved computer security practices, and to enhance awareness of threats and vulnerabilities to federal computer systems.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/bdquery/z?d100:HR00145:|TOM:/bss/d100query.html|
Epic
http://www.epic.org/crypto/csa/csa.html

## 3.3 The Paperwork Reduction Act of 1995

**Description:**

The Paperwork Reduction Act of 1995, Public Law 104-13 [44 USC Section 35], amends the Paperwork Reduction Act of 1980.

The Act of 1995 directs agencies to implement a management system for all information dissemination products, and states that, at a minimum, such a system would:

- Assure that information dissemination products are available for proper performance of agency functions.
- Ensure that members of the public with disabilities have reasonable access.
- Facilitate availability of government publications to depository libraries through the Government Printing Office.
- Communication with the public must include adequate notice when initiating, substantially modifying, or terminating significant information products.

The Act also establishes the authority and functions of the Office of Information and Regulatory Affairs (OIRA) in the Office of Management and Budget (OMB). The OIRA is directed to establish a consistent and uniform government information resources management plan. OIRA is also required to oversee the establishment of a Government Information Locator Service, and facilitate identification and sharing of information among federal agencies. In addition, OMB is required to conduct pilot projects to test alternative policies and procedures.

**Implications for CMS:**

- CMS is required to comply with OIRA information resource management policies. Refer to section 3.10 OMB, Circular A-130 (November 2000)

**Source:**

GPO
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ13.104.pdf

## 3.4 Electronic Freedom of Information Act (1996)

**Description:**

The Electronic Freedom of Information Act of 1996 (E-FOIA), Public Law 104-231 [5 USC Section 552], mandates agencies to make all reasonable efforts to provide government records to requestors in the medium of their choice. It amends the Freedom of Information Act's (FOIA) definition of "record" to mean that all information collected and maintained by an agency, regardless of format, is subject to E-FOIA.

The law encourages agencies to use technology to ensure greater public access to simplify the process; decrease response time; increase consistency and quality of information provided; and enhance usefulness of information collected, maintained, and disseminated. It requires agencies to expand the types of records made available online, and to make reasonable efforts to search for information in electronic form.

**Implications for CMS:**

- The director of CMS must establish:
  i. Electronic reading rooms to organize and make accessible specific categories of agency information (e.g., opinions, policy statements, staff manuals) and records already released through FOIA.
  ii. Reference guides to educate the public on how to request and obtain records.
  iii. An index of all of CMS major information systems with a description of records locator systems maintained by CMS. OMB has recommended that these be available through the agency's web-site or a Government Information Locator Service.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/bdquery/z?d104:HR03802:|TOM:/bss/d104query.html|

## 3.5 Health Insurance Portability and Accountability Act of 1996

**Description:**

The Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, requires parties that maintain or transmit protected health information to implement reasonable and appropriate administrative, technical, and physical security controls. These security mechanisms should ensure the integrity and confidentiality of protected health insurance information, protect against any reasonably anticipated threat or hazard to the security or integrity of protected health insurance information, and protect against unauthorized use or disclosure of protected health insurance information. In addition, organizations must ensure employee compliance with security controls to protect the confidentiality and integrity of protected information.

HIPAA imposes severe accountability consequences on both organizations and individuals that fail to protect sensitive health insurance information adequately.

**Implications for CMS:**

- CMS will need to develop and implement a HIPAA security/privacy program (as a component of the existing security program) for CMS to ensure compliance with this legislation.
- CMS must perform a thorough risk assessment to identify the health information resources within the CMS environment, identify risks to the confidentiality and integrity of such information, and define risk-reduction security controls that protect health insurance information from unauthorized access or misuse.
- To comply with the HIPAA mandate, CMS may be required to implement additional security controls from both a technical and non-technical standpoint (administrative processes) if existing security controls cannot provide sufficient levels of protection.
- HIPAA security training and awareness programs for employees must be implemented for all CMS personnel to ensure organizational and employee compliance with the HIPAA legislation.
- CMS must ensure that employees are trained in proper security procedures and practices.
- CMS will be held responsible for ensuring employee compliance with HIPAA standards.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c104:H.R.3103.ENR:

## 3.6 Executive Order 13011 (July 16, 1996)

**Description:**

Executive Order Number 13011 is a legally binding expression of the government's policy regarding the management of federal information systems. In the order, fundamental responsibilities are identified for agency Chief Executive Officers and Chief Information Officers with respect to investments in new information systems, and cooperation with other agencies in efforts to improve government-wide practices in information system management, etc.

This Executive Order encourages agency executives to collaborate with one another with the intention of improving agency methods and best practices. Collaboration is also intended to reduce costs by identifying opportunities for information sharing between agencies.

**Implications for CMS:**

- CMS must have a Chief Information Officer (CIO) to be responsible for designing and implementing a management structure at the agency with the goal of providing accountability and enhanced quality of information technology.
- The CMS Administrator is responsible for ensuring that the information security policies, procedures, and practices of the executive agency are adequate.
- CMS's CIO may be selected to take part in one or more of several executive branch committees assigned the task of designing minimum standards with NIST, assisting in the design, acquisition, or management of any government information system, etc.

**Source:**

GPO
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1996_register&docid=fr19jy96-133.pdf

## 3.7 The Clinger-Cohen Act (1996)

**Description:**

The Clinger-Cohen Act assigns to the head of each executive agency the responsibility to assess Information Technology (IT) resources and makes him/her responsible for effectively managing the risks of IT investments. The law includes the establishment of the following:

1. Best practices for capital planning for IT acquisitions and investments.
2. CIO positions within federal departments and agencies
3. Performance evaluation measurements for IT.

The Act requires that agencies establish a process to ensure that the public has timely and equitable access to the agency's information. Agencies also must regularly solicit and consider public input on information dissemination activities. In addition, the Clinger-Cohen Act assigns overall responsibility for promoting improvements in the efficiency and management of IT acquisitions to the Director of OMB.

**Implications for CMS:**

- The CMS Administrator is responsible for maximizing the value and managing the risks of information technology resources and investments.
- CMS should use commercial-off-the-shelf (COTS) technology when possible to reduce costs.
- Establish best practices for capital planning for IT acquisitions investments.
- CMS must establish performance evaluation measurements for IT:
  i. IT management processes for assessing and managing the risks of information technology. This would assist CMS in carrying out its missions and achieving the performance they require from information systems.
  ii. Encourage the use of pilot tests before production.
- Establish goals for improving the efficiency and effectiveness of CMS operations and the delivery of services to the public through the effective use of IT.
  i. Prepare an annual report on the progress in achieving the goals, to be included in the CMS administrator's budget submission to Congress.
- Appoint a Chief Information Officer (CIO)
  i. Develop strategies for training and professional development of CMS personnel in information technology management
  ii. Maintain an inventory of all computer equipment including equipment that is excess or surplus property.

**Source:**

GPO

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ106.104

## 3.8 Government Paperwork Elimination Act (1998)

**Description:**

The Government Paperwork Elimination Act, Public Law 105-277 (GPEA, Title XVII of 44 U.S.C. 3504), was enacted to make government service delivery more efficient while ensuring baseline standards for electronic signatures across federal agencies. This Act allows citizens to use electronic technologies when filing information with, or retrieving it from the federal government. It directs federal agencies to provide public access to government services and documents by 2003 and gives the public the option of submitting government forms electronically.

Under GPEA, agencies will develop information systems that enable online submissions of forms, reports and other data. Agencies will be required to guard privacy and protect documents from alteration. Electronic signatures and other measures will be used to authenticate citizens as they transact business with the government.

The Office of Management and Budget (OMB) has issued guidelines to assist agencies in complying with the provisions of GPEA. OMB calls upon agencies to perform business case analyses, cost/benefit analyses, technology assessments, and risk assessments to determine which technologies, systems, and procedures best support compliance with GPEA. OMB also requires agencies to ensure maximum security related to authentication and privacy. Agencies must submit a copy of their GPEA implementation plan to OMB by October 2000.

**Implications for CMS:**

- CMS must provide public access to government services and documents by 2003.
- CMS must develop information systems that enable online submissions of forms, reports and other data.
- CMS will be required to guard privacy and protect documents from being altered. Electronic signatures and other measures will be used to authenticate citizens as they transact business with the government.

**Source:**

GPO
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ277.105

## 3.9 PDD 63: Critical Infrastructure Protection (May 22, 1998)

**Description:**

Presidential Decision Directive (PDD) 63 is a statement of the Clinton Administration's policy concerning the protection of the United States' critical infrastructures. In it the Administration describes roles and procedures that are designed to "swiftly eliminate any significant vulnerability to both physical and cyber attacks" on U.S. critical infrastructures.

**Implications for CMS:**

- CMS shall have a plan to protect its critical infrastructure that includes, but is not limited to, its networked information systems.
- CMS's CIO is responsible for information security.
- CMS must appoint a Chief Infrastructure Assurance Officer who is responsible for protecting the department's critical infrastructure.
- CMS may be required to assign one of its Assistant Secretaries (or a more senior employee) to the role of Sector Liaison Official for a sector of the US Critical Infrastructure. This official would work with private sector representatives to recommend components of the National Infrastructure Assurance Plan and to facilitate the implementation of all parts of this PDD that correspond to the industry.

**Source:**

Federation of American Scientist
http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

## 3.10 Office of Management and Budget M-99-18 Privacy Policies on Federal Web-sites (June 1999)

**Description:**

The OMB Memorandum 99-18, requires agencies to post clear privacy policies on their principle websites and other major points of Internet entry that "clearly and concisely inform visitors to the site, what information the agency collects about individuals, why the agency collects it, and how the agency will use it."

**Implications for CMS:**

- CMS must post clear privacy policies on their web site and other major points of entry
  - i. By September 1, 1999.
  - ii. By December 1, 1999, privacy policies must be added to any other known major entry points to the CMS website.

**Source:**

Office of Management and Budget, Memoranda
http://www.whitehouse.gov/omb/memoranda/m99-18.html

## 3.11 OMB, Circular A-130 (November 2000)

**Description:**

OMB Circular A-130 is a statement of policy for the management of federal computer systems and information resources. As required by the Paperwork Reduction Act, the OMB defines the information resource management policies that must be applied in all executive branch agencies to all information systems.

In addition to defining management policies, the OMB is charged with overseeing the implementation of information management principles, standards, and guidelines, evaluating the security practices of executive agencies, and determining the compliance of the security programs with the policies distributed by the Director of OMB and the standards defined by NIST.

*Note: OMB Circular A-130 provides implementation guidance for the Paperwork Reduction Act of 1995.*

**Implications for CMS:**

- An individual's right to privacy must be protected by CMS.
- At all points throughout the life-cycle of an information system at CMS, the agency must consider the effects of decisions and actions on other stages of the lifecycle.
- CMS must ensure consultation with the public when appropriate.
- CMS must ensure consultation with state and local governments when those groups might be affected by CMS policy.
- CMS must use interagency and intergovernmental information sharing to satisfy new information needs.
- CMS must provide access to agency records under provisions of the Freedom of Information Act and the Privacy Act.
- CMS should use electronic media for the dissemination of materials when appropriate and within budget.
- CMS "must ensure that all information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of information."
- CMS must limit the collection of information that is personally identifiable to that which is permitted legally.
- CMS must limit the sharing of information that is personally identifiable.
- The agency shall provide individuals access to records about themselves that are kept in Privacy Act systems of records and allow those individuals to make corrections wherever it may be necessary.
- CMS must prepare a benefit/cost analysis for each information system throughout its life cycle.

- CMS must establish an oversight mechanism to monitor the effectiveness of information security practices and policies.
- CMS needs to "make security's role explicit in information technology investments and capital programming." This can be accomplished by consistently employing the minimum standards developed by NIST.
- CMS must demonstrate specific methods to show that risks and potential for loss are understood and periodically reassessed.
- The head of CMS must appoint a CIO to implement the requirements of the Paperwork Reduction Act and the Clinger-Cohen Act, as well as Executive Order 13011.
- Responsibility for individual systems must be delegated to an individual knowledgeable about the system.
- Each Major Application or General Support System containing or using sensitive data must have a System Security Plan that follows the NIST guidelines.
- System Security Plans should be reviewed whenever significant modifications are made, but at least every three years.
- Agencies must correct deficiencies identified during the review process for each system.
- Summaries of Security Plans should be included with the strategic plan required by the Paperwork Reduction Act.
- At least every three years an independent review of each major application must be performed. The review should be independent of the manager of the system being reviewed.

**Source:**

OMB, Circulars

http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

## 3.12 FIPS PUB 140-2: Security Requirements for Cryptographic Modules

**Description:**

NIST develops and distributes the Federal Information Processing Standards (FIPS) pursuant to the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987. FIPS publications serve as mandates for federal agencies in improving the utilization, management, and security of information technology systems.

FIPS publication 140-2 (FIPS PUB 140-2) supercedes FIPS publication 140-1, which was issued on January 11, 1994. FIPS PUB 140-2 specifies the security requirements to be satisfied through the use of cryptographic modules in the protection of sensitive but unclassified information. The security requirements specified through FIPS PUB 140-2 relate to the secure design and implementation of cryptographic modules. This includes basic design and documentation, module interfaces, authorized roles and services, physical security, application security, operation system security, key management, cryptographic algorithms, electromagnetic interference, and self-testing.

**Implications for CMS:**

- FIPS 140-2 certification is required for the sale of cryptographic software applications to federal agencies.

**Source:**

NIST Computer Security Resource Center, Federal Information Processing Standards
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

## 3.13 The PATRIOT Act of 2001

**Description:**

The PATRIOT (Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act of 2001, Public Law 107-56, is intended to enhance the monitoring and surveillance capabilities of law enforcement and national intelligence agencies. The PATRIOT Act provides increased power to law enforcement in utilizing wiretaps and pen registers in the prevention, detection, and obstruction of terrorism. The PATRIOT Act also includes modified provisions relating money laundering, bank secrecy laws, and immigration procedures.

Section 1016 of the PATRIOT Act focuses upon the protection of the nation's critical infrastructure. This section declares it to be United States policy that any physical or "virtual" disruption of the operation of the critical infrastructure of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and United States' national security. It must also be United States policy to have in place a comprehensive and effective program to ensure the continuity of essential federal government functions under all circumstances. The PATRIOT Act states that actions necessary to achieve this policy are carried out in a public-private sector partnership.

The PATRIOT Act establishes the National Infrastructure Simulation and Analysis Center, which is intended to serve as a source of national competency to address critical infrastructure protection and continuity through support for activity related to counter-terrorism, threat assessment, and risk mitigation.

Finally, the PATRIOT Act defines critical infrastructure as systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would result in a debilitating impact on security, national economic security, or national public health or safety.

**Implications for CMS:**

- The PATRIOT Act requires CMS to develop and implement policies that protect the security of the national critical infrastructure, which includes the Health and Human Services Administration, in the manner prescribed through the legislation.
- CMS must ensure that any disruption to the business operations of the agency be rare, brief, geographically limited in effect, manageable, and minimally detrimental to government services.

This may require CMS to implement technical security and contingency controls, such as redundant fail-over systems in dispersed locations, or to develop administrative policy, such as incident response and management policies to ensure disruptions have minimal impact upon operations and can be quickly resolved.

**Source:**

GPO
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107

## 3.14 FIPS PUB 197 Advanced Encryption Standard (November 2001)

**Description:**

FIPS publication 197 (FIPS PUB 197, November 2001) specifies a FIPS-approved cryptographic algorithm, known as the Advanced Encryption Standard (AES), which can be utilized in the protection of federal information resources. The AES standard is an implementation of the Rijndael encryption algorithm.

AES is a symmetric block cipher capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. This standard may be used by federal agencies for the cryptographic protection of sensitive but unclassified information. In addition, this standard may be used by non-federal government organizations.

The AES standard may be used in conjunction with, or as an alternative to other FIPS-approved cryptographic algorithms. The AES algorithm may be implemented in software, firmware, hardware, or any combination of the three, however the specific implementation will largely depend upon the target environment.

**Implications for CMS:**

- The acceptance of AES as a FIPS-compliant standard enables CMS to implement encryption technologies supporting this standard. This provides CMS with additional flexibility in the software, firmware, or hardware selection process for cryptographic technologies.
- AES may serve as an alternative to other FIPS-approved algorithms (DES) for CMS environments where symmetric key encryption is suitable.

**Source:**

NIST Computer Security Resource Center, FIPS
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

## 3.15 Homeland Security Act of 2002

**Description:**

The Homeland Security Act of 2002, Public Law 107-296, replaced H.R. 1158 National Homeland Security Agency Act, H.R. 1292 Homeland Security Strategy Act, H.R. 3026 Office of Homeland Security Act of 2001, and H.R. 3378 Commission on Homeland Security Act.

Congressman Tom Davis (R-VA) presented H.R. 3844, The Federal Information Security Management Act (FISMA), to the House of Representatives as a replacement for the Government Information Security Reform Act (GISRA), FISMA provides for mandatory compliance that is missing from GISRA. TITLE X of the Homeland Security Act of 2002 includes some of the language from H.R. 3844. This portion of the proposed law requires the NIST to develop and promulgate new policies and minimum standards for security practices and features on federal computer systems. The law also supplies a framework for providing accountability for the quality and vigilance of agencies' security programs.

Title X is the only portion of the Homeland Security Act of 2002 that affects CMS. TITLE III of the E-Government Act supersedes TITLE X of the Homeland Security Act. Refer to section 3.18 The Federal Information Security Management Act (FISMA), TITLE III of the E-Government Act of 2002 for the implications

**Implications for CMS:**

- This Bill is an extension of GISRA (October 2000).
- TITLE III of the E-Government Act supersedes TITLE X of the Homeland Security Act. Refer to section 3.18 The Federal Information Security Management Act (FISMA), TITLE III of the E-Government Act of 2002 for the implications.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.5005.ENR:

## 3.16 Cyber Security Research and Development Act of 2002

**Description:**

The Cyber Security Research and Development Act, Public Law 107-305, increases federal investment in computer and network security research and development to:

- Improve vulnerability assessment and technological security solutions,
- Expand and improve the pool of information security professionals (including researchers) in the United States workforce,
- Better coordinate information sharing and collaboration among industry, government, and academic research projects.

This Act establishes a research program providing assistance to academic institutions that enter into partnerships with private organizations in support of research to improve the security of computer systems. The research program combines the abilities of higher learning institutions, the NIST, the National Science Foundation, and private industry.

**Implications for CMS:**

- The research conducted under the Cyber Security Research and Development Act will provide federal agencies with increased knowledge and awareness of security threats, vulnerabilities, and security technologies.
- The information provided through the research capabilities addressed within the Act can assist CMS in implementing leading-edge security technologies that protect CMS information resources from current and emerging threats.
- Resources and information are available to implement and maintain increased levels of protection even as the security and technology fields evolve.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3394.ENR:

## 3.17 The E-Government Act of 2002

**Description:**

The E-Government Act of 2002, Public Law107-347, includes the promotion of "the use of the Internet and emerging technologies within and across government agencies to provide citizen-centric government information and services," transforming agency operations by "utilizing, where appropriate, best practices from public and private sector organizations," and providing "enhanced access to government information and services in a manner consistent with laws regarding the protection of personal privacy."

The E-Government Act of 2002 requires government agencies to develop electronic means of providing information to the public. The Act specifically calls for the "adoption of innovative information technology, including the appropriate use of commercial best practices." The availability of this information to those without access to the Internet shall not be diminished through the application of new technologies or methods of Internet access.

Congressman Tom Davis (R-VA) introduced H.R. 3844, The Federal Information Security Management Act, to the House of Representatives as a replacement for the Government Information Security Reform Act (GISRA), which expired in October of 2002. The Federal Information Security Management Act provides for mandatory compliance that lacking in GISRA. TITLE III of the E-Government Act of 2002 includes language from H.R. 3844.This portion of the proposed law requires the NIST to develop and promulgate new policies and minimum standards for security practices and features on federal computer systems. This law also defines a framework for providing accountability for the quality and vigilance of agencies' security programs. TITLE III of the E-Government Act supersedes TITLE X of the Homeland Security Act.

For Title III, The Federal Information Security Management Act (FISMA), refer to Section 3.18.

**Implications for CMS:**

- The E-Government Act requires CMS to comply with standards as defined by the federal CIO, as well as adopt new standards, procedures, methods, or strategies for the dissemination of government information.
- An infrastructure for Internet-based information dissemination is required, and such infrastructure requires critical security measures. The costs associated with such an implementation may be substantial. However, funding from the E-Government Fund may decrease the financial impact upon CMS. Additionally, the allocation of funds will enable CMS to enforce better compliance with the requirements as defined in the legislation.
- Upon the enactment of this Bill, CMS would also be required to adopt, use, and accept digital signatures to ensure the authenticity of electronic transactions.
- CMS would need to ensure that all required government information is accessible on the agency website, and that an online agency directory is accessible online. The

accessibility of agency contact information may present additional security vulnerabilities, as the potential for social engineering would increase.

- To ensure protection from social engineering methods, CMS may need to develop and implement sufficient employee training and awareness programs.
- The privacy assessment requirement may affect CMS's ability to procure, develop, and implement new technologies efficiently.
- Changes to personal identification data must undergo a privacy assessment, which may require additional time and resources. This may also require modification of policies and procedures for the collection and use of personally identifiable information.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.2458.ENR::

## 3.18 The Federal Information Security Management Act (FISMA) of 2002

**Description:**

The Federal Information Security Management Act (FISMA), TITLE III of the E-Government Act of 2002 supersedes TITLE X of the Homeland Security Act. This Bill revises the government information security requirements.

FISMA requires agencies to assess risks to IT systems and to provide "information security protections commensurate with the risk." It also requires development of security programs, annual evaluations of the programs and annual reports to OMB. The Director of OMB is required to develop and verify that IT security is incorporated adequately in each agency's programs and budgets. The Director of OMB must make a status report to Congress each year on agency compliance with this Act.

In addition, this Bill requires the NIST to develop and promulgate new policies and minimum standards for security practices and features on federal computer systems. The law also supplies a framework for providing accountability for the quality and vigilance of agencies' security programs.

**Implications for CMS:**

- CMS is responsible for providing information security protection commensurate with the risk and magnitude of the harm resulting from unauthorized access and complying with information security standards and guidelines.
- The senior agency officials are required to provide information security for the information and information systems that support operations and assets.
- The head of each agency shall delegate to the agency CIO the authority to ensure compliance with the regulations imposed under this Bill.
- CMS is required to maintain sufficient trained personnel to assist the agency in complying with the Act's requirements.
- The CIO is required to report annually to the head of the agency on the effectiveness of the agency's information security program.
- CMS is required to develop, document, and implement agency-wide information security programs to provide information security for the systems that support the operation's assets. The Director of OMB must approve the information security program. The program shall include the following:
    i. Periodic risk assessments.
    ii. Policies and procedures that ensure that information security is addressed throughout the life cycle of CMS information system.
    iii. Subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems.
    iv. Security awareness training.
    v. Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices.
    vi. A process for planning, implementing, evaluating, reporting, and responding to security incidents.

vii. Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

- CMS is required to report annually to the Director of OMB, specified congressional committees, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures and practices and on compliance with this Bill:
    i. Address adequacy and effectiveness relating to annual agency budgets, information resources management, IT management, program performance, financial management, financial management systems, and internal accounting and administrative controls.
    ii. Report any significant deficiency.
- CMS is required to implement the standards provided by NIST for securing computer systems.
- The Director of OMB will advise agencies of new standards as they are developed.
- CMS must develop and maintain an inventory of major information systems operated or under the control of CMS including identification of the interfaces between each system and all other systems or networks.
    i. Update the inventory at minimum annually
    ii. The list shall be made available to the Comptroller General
    iii. The list shall be used to support information resources management
- This Bill is an extension of GISRA (October 2000).

**Source:**

GPO
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf

# 4. CMS Legal Compliance Assessment Tool

## 4.1 Self-Assessment

The following subsections identify specific requirements for CMS as mandated in the laws summarized in Section 2. The subsections group similar requirements together, but directives from a given law may be found in several subsections. Section 3.2 is a correlation guide to the laws and requirements.

### 4.1.1 Information Availability

☐ N/A ☐ Pass ☐ Fail a. Non-sensitive information is available from CMS electronically. [E-FOIA]

☐ N/A ☐ Pass ☐ Fail b. CMS provides a means of educating the public about how to request and obtain records. [E-FOIA]

☐ N/A ☐ Pass ☐ Fail c. CMS makes an index of all major information systems, with a description of records locator services, available to the public. [E-FOIA]

☐ N/A ☐ Pass ☐ Fail d. CMS provides public access to government documents. If CMS does not currently do so, there are plans to provide such access by 2003. [Gov. Paperwork Elimination Act, E-Gov. Act]

☐ N/A ☐ Pass ☐ Fail e. There are procedures in place that allow individuals access to their records. [Privacy Act, OMB A-130]

### 4.1.2 CMS System Security Plans and Other Plans

☐ N/A ☐ Pass ☐ Fail a. Each Major Application or General Support System containing or using sensitive data has a System Security Plan that follows NIST guidelines. [OMB A-130]

☐ N/A ☐ Pass ☐ Fail b. CMS verifies that there is an SSP for every information system that contains sensitive information. [Computer Security Act]

☐ N/A ☐ Pass ☐ Fail c. CMS SSPs apply to all stages of the life-cycle, and are in place for all systems that support the agency's operations and assets. [FISMA]

☐ N/A ☐ Pass ☐ Fail d. CMS includes a summary of the SSPs in the five-year plan it submitted to the Office of Management and Budget. [OMB A-

130, Computer Security Act, Gov. Paperwork Elimination Act]

☐ N/A ☐ Pass ☐ Fail e. CMS delegates responsibility for individual systems to an individual knowledgeable about the system. [OMB A-130]

☐ N/A ☐ Pass ☐ Fail f. CMS has enacted a plan to ensure that any disruption to CMS business is rare, brief, manageable, and recoverable. [PATRIOT Act]

☐ N/A ☐ Pass ☐ Fail g. CMS has a plan to protect its critical infrastructure from network-based and other attacks. [PDD-63, PATRIOT Act, E-Gov. Act]

### 4.1.3 Review/Analysis/Monitoring

☐ N/A ☐ Pass ☐ Fail a. CMS has a method of ensuring that all computer systems that contain sensitive information are properly identified. [Computer Security Act]

☐ N/A ☐ Pass ☐ Fail b. Agency officials review all agency-wide security programs (and programs covered by the security programs) each year. [FISMA]

☐ N/A ☐ Pass ☐ Fail c. An annual internal assessment— guided by NIST documentation and including an independent report from the agency's Inspector General— is submitted to the Office of Management and Budget. [FISMA, OMB A-130]

☐ N/A ☐ Pass ☐ Fail d. An independent review of each Major Application is performed at least every three years. (The review should be independent of the Manager of the system under review.) [OMB A-130]

☐ N/A ☐ Pass ☐ Fail e. CMS prepares a cost-benefit analysis of each information system, at all stages of the system's life cycle. [OMB A-130]

☐ N/A ☐ Pass ☐ Fail f. CMS evaluates the effects of security related decisions on all stages of an information system's life-cycle. [OMB A-130]

☐ N/A ☐ Pass ☐ Fail g. There is a mechanism, internal to CMS that monitors the effectiveness of information security practices and policies. [OMB A-130]

☐ N/A ☐ Pass ☐ Fail h. All agency deficiencies are reported to the Office of Management and Budget. [FISMA]

☐ N/A ☐ Pass ☐ Fail i. CMS has documented procedures for detecting, reporting, and responding to information security incidents. The policies and

procedures clearly document how information is to be shared with appropriate authorities. [FISMA]

### 4.1.4 Role-Specific

☐ N/A ☐ Pass ☐ Fail a. The CMS Administrator approves the adequacy of the policies, procedures and practices of the agency with respect to information technology. [FISMA]

☐ N/A ☐ Pass ☐ Fail b. CMS has appointed a Chief Infrastructure Assurance Officer who is responsible for protecting the department's critical infrastructure. [PDD-63]

☐ N/A ☐ Pass ☐ Fail c. CMS has a CIO with responsibility for implementing the requirements of the Paperwork Reduction Act, the Clinger-Cohen Act, and Executive Order 13011. [Executive Order 13011, OMB A-130]

☐ N/A ☐ Pass ☐ Fail d. The CMS CIO is charged with the responsibility for the overall quality of IT systems. [Executive Order 13011]

### 4.1.5 Standards

☐ N/A ☐ Pass ☐ Fail a. There is a mechanism in place at CMS that ensures all sensitive information systems comply with NIST minimum security standards and guidelines. [Computer Security Act]

☐ N/A ☐ Pass ☐ Fail b. Where CMS minimum security standards differ from those defined by NIST, they fully encompass and exceed the applicable NIST standards. The CMS security standards are compared to NIST minimum standards periodically. [Computer Security Act]

☐ N/A ☐ Pass ☐ Fail c. CMS has developed a HIPAA security program component. [HIPAA]

☐ N/A ☐ Pass ☐ Fail d. CMS has assessed the risk of all of its information systems to identify weaknesses in HIPAA compliance in the area of the confidentiality and integrity of information. [HIPAA]

☐ N/A ☐ Pass ☐ Fail e. CMS incorporates the concept "security's role [is] explicit in information technology investments and capital programming." [OMB A-130]

### 4.1.6 Training

☐ N/A ☐ Pass ☐ Fail a. Training is provided for operators of sensitive information systems and follows NIST guidelines. [Computer Security Act, FISMA]

☐ N/A ☐ Pass ☐ Fail b. CMS provides HIPAA compliance training to all of its employees. [HIPAA]

### 4.1.7 Privacy

☐ N/A ☐ Pass ☐ Fail a. CMS protects all information "commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of [such information]." [OMB A-130, E-Gov. Act]

☐ N/A ☐ Pass ☐ Fail b. CMS maintains only the information about individuals that is necessary and relevant to the agency's mission. [Privacy Act, OMB A-130]

☐ N/A ☐ Pass ☐ Fail c. There are documented procedures in place at CMS for notifying an individual if the agency possesses personally identifiable information about that individual. [Privacy Act]

☐ N/A ☐ Pass ☐ Fail d. There are documented procedures in place for reviewing requests from individuals concerning the modification of records or information pertaining to him/her. [Privacy Act, OMB A-130]

☐ N/A ☐ Pass ☐ Fail e. CMS employs systems that permit the electronic submission of forms, reports, and other data. [Gov. Paperwork Elimination Act]

☐ N/A ☐ Pass ☐ Fail f. Procedures and guidelines are in place to ensure that data is released or disclosed only after appropriate review, or with prior written consent of the individual to whom the information pertains. [Privacy Act, OMB A-130]

☐ N/A ☐ Pass ☐ Fail g. There is a documented policy addressing the type of information required to identify an individual who requests his/her record or information pertaining to her/him. [Privacy Act]

☐ N/A ☐ Pass ☐ Fail h. CMS uses encryption signatures in electronic communications between users and the agency when transacting business over the Internet. [Gov. Paperwork Elimination Act, FIPS 140-2, FIPS

197, E-Gov. Act]

☐ N/A ☐ Pass ☐ Fail i. CMS posts its privacy policies on its web page. [OMB M-99-18]

☐ N/A ☐ Pass ☐ Fail j. The agency identifies, uses, and shares best security practices. [FISMA, E-Government Act]

☐ N/A ☐ Pass ☐ Fail k. It is CMS policy to take every precaution to protect an individual's rights to privacy [confidentiality] of personally identifiable information. [OMB A-130]

☐ N/A ☐ Pass ☐ Fail l. CMS seeks the opinion of the public as well as local and state governments regarding decisions that must be made for protecting information systems whenever possible and appropriate. [OMB A-130, Cyber Security Research and Development Act]

## 4.2 Self-Assessment – Legislation Correlation

Included in this section are two guides to identifying the legislation related to the self-assessment categories.

### 4.2.1 Self Assessment Correlation by Subject

The following correlation by subject identifies the source of legislation for each of the self-assessment entries.

| Subject | Question | Legislation |
|---|---|---|
| Info. Availability | 4.1.1 a | E-FOIA |
| | b | E-FOIA |
| | c | E-FOIA |
| | d | Gov. Paperwork Elimination Act, E-Gov. Act |
| | e | Privacy Act, OMB A-130 |
| Security Plans, etc. | 4.1.2 a | OMB A-130 |
| | b | Computer Security Act |
| | c | FISMA, |
| | d | OMB A-130, Computer Security Act, Gov. Paperwork Elim. Act |
| | e | OMB A-130 |
| | f | PATRIOT Act |
| | g | PDD-63, PATRIOT Act, E-Gov. Act |
| Review, Analysis, etc. | 4.1.3 a | Computer Security Act |
| | b | FISMA |
| | c | FISMA, OMB A-130 |
| | d | OMB A-130 |
| | e | OMB A-130 |
| | f | OMB A-130 |
| | g | OMB A-130 |
| | h | FISMA |
| | i | FISMA |
| Role Specific | 4.1.4 a | FISMA |
| | b | PDD-63 |
| | c | Executive Order 13011, OMB A-130, Clinger-Cohen Act |
| | d | Executive Order 13011 |
| Standards | 4.1.5 a | Computer Security Act |
| | b | Computer Security Act |
| | c | HIPAA |
| | d | HIPAA |
| | e | OMB A-130 |
| Training | 4.1.6 a | Computer Security Act, FISMA |

| Subject | Question | Legislation |
|---|---|---|
| | b | HIPAA |
| Privacy | 4.1.7 a | OMB A-130, E-Gov. Act |
| | b | Privacy Act, OMB A-130 |
| | c | Privacy Act |
| | d | Privacy Act, OMB A-130 |
| | e | Gov. Paperwork Elimination Act |
| | f | Privacy Act, OMB A-130 |
| | g | Privacy Act |
| | h | Gov. Paperwork Elimination Act, FIPS 140-2, FIPS 197, E-Gov. Act |
| | i | OMB M-99-18 |
| | j | FISMA, E-Gov. Act |
| | k | OMB A-130 |
| | l | OMB A-130, Cyber Sec. Research and Dev. Act |

### 4.2.2 Self Assessment Correlation by Legislation

The following correlation identifies the specific requirements for CMS that are associated with each law.

| Legislation | Questions |
|---|---|
| Privacy Act | 4.1.1 (e), 4.1.7 (b,c,d,f,g) |
| Computer Security Act | 4.1.2 (b,d), 4.1.3 (a), 4.1.5 (a,b), 4.1.6 (a), |
| E-FOIA | 4.1.1 (a,b,c) |
| HIPAA | 4.1.5 (c,d), 4.1.6 (b) |
| Clinger-Cohen Act | 4.1.3 (b) |
| Exec. Order 13011 | 4.1.4 (c,d) |
| Gov. Paperwork Elimination Act | 4.1.1 (d), 4.1.2 (d), 4.1.7 (e,h) |
| PDD-63 | 4.1.2 (g), 4.1.4 (b), |
| OMB M-99-18 | 4.1.7 (i), |
| FISMA | 4.1.2 (c), 4.1.3 (c,h,i), 4.1.4 (a), 4.1.7 (j) |
| OMB A-130 | 4.1.1 (e), 4.1.2 (a,d,e), 4.1.3 (c,d,e,f,g), 4.1.4 (c), 4.1.5 (e), 4.1.7 (a,b,d,f,l,k,l) |
| FIPS 140-2 | 4.1.7 (h) |
| PATRIOT Act | 4.1.2 (f,g) |
| FIPS 197 | 4.1.7 (h) |
| E-Gov. Act | 4.1.1 (d), 4.1.2 (g), 4.1.7 (a, h, j) |
| Cyber Sec. Research & Dev. Act | 4.1.7 (i) |

# 5. Pending Legislation

This section includes legislation currently under Congressional review. The status of these Bills should be monitored as they progress through the legislative process to enable CMS to respond quickly when a Bill is enacted into law.

The Bills are divided into two subsections (Security Legislation and Privacy Legislation).

In addition, the matrix below includes the pending Bills that have not yet been incorporated in this document but are currently under review for potential implications for CMS. The Bills are presented in order of when first introduced to Congress. The current status of each Bill is included to indicate how far Bills have progressed in the legislative process.

| Pending Legislation | First Introduced | Legislative Status |
|---|---|---|
| **S.6** - A Bill to enhance homeland security and for other purposes | Introduced 1/7/2003 by Senator Daschle, Thomas A. [SD] | 1/7/2003: Read twice and referred to the Committee on the Judiciary. |
| **S. 22 -** Justice Enhancement and Domestic Security Act of 2003 | Introduced 1/7/2003 by Senator Daschle, Thomas A. [SD] | 1/7/2003: Read twice and referred to the Committee on the Judiciary. |
| **S. 41 -** A Bill to strike certain provisions of the Homeland Security Act of 2002 (Public Law 107-296), and for other purposes. | Introduced 1/7/2003 by Senator Lieberman, Joseph I. [CT] | 1/7/2003: Read twice and referred to the Committee on Governmental Affairs. |
| **H.R. 48 -** To develop and deploy technologies to defeat Internet jamming and censorship | Introduced 1/7/2003 by Representative Cox, Christopher [CA-48] | 1/7/2003: Referred to the House Committee on International Relations |
| **H.R. 70** - To regulate the use by interactive computer services of Social Security account numbers and related personally identifiable information | Introduced 1/7/2003 by Representative Frelinghuysen, Rodney P. [NJ-11] | 1/7/2003: Referred to the House Committee on Energy and Commerce. |
| **S. 187** - National Cyber Security Leadership Act of 2003 | Introduced 1/16/2003 by Senator Edwards, John [NC] | 1/16/2003: Read twice and referred to the Committee on Governmental Affairs |

## 5.1 Security Legislation

This section of the report includes documentation of those computer security Bills that may bear on the Information Security Program at CMS.

The Bills are presented in order of when first introduced to Congress. The current status of each Bill is included to indicate how far Bills have progressed in the legislative process.

### 5.1.1 House Representative (H.R.) 749 – Paperwork Elimination Act of 2001

**Description:**

The Paperwork Elimination Act of 2001 (an update to the Public Law 105-277) requires all federal agencies to take steps toward the acquisition and use of electronic technology that would enable electronic submission, maintenance, and disclosure of information as an alternative to completing the same tasks using paper. In addition, the Act requires the use and acceptance of digital signatures.

This legislation is designed to reduce paper utilization, improve data quality, and increase agency efficiency and responsiveness to the public.

**Potential Implications for CMS:**

- The enactment of this Bill would require CMS to increase the level of electronic processing, and, accordingly, store and transfer increased amounts of data electronically that are now dependent on paper processes.
- CMS may need to perform a review of current security controls to ensure such controls maintain the scalability and flexibility to support increased data communications. Based upon this review, CMS may need to modify requirements for existing security controls, or implement additional security controls to sufficiently secure agency paperless efforts.
- CMS would be required to adopt, use, and accept digital signatures to ensure the authenticity of electronic transactions. The implementation of digital signature support may require additional work effort for CMS, including the installation of software, hardware, and infrastructure, as well as policy development and implementation. CMS would need to provide guidance and policy for this technology.

**Legislative Status:**

***House status:*** This Bill was first introduced to the House on February 27, 2001. March 5, 2001 the Bill was referred to the Subcommittee on Energy Policy, Natural Resources and Regulatory Affairs.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.749:

### 5.1.2 H.R. 1259 – Computer Security Enhancement Act of 2001

**Description:**

The Computer Security Enhancement Act of 2001 amends the Computer Security Act of 1987. This legislation requires the NIST to provide assistance to federal agencies in the protection of computer networks, promotes federal compliance with computer information security and privacy guidelines, and assists federal agencies in responding to unauthorized access to federal systems. NIST is also required to develop uniform standards for the cost-effective security and privacy of sensitive information in certain federal systems, to provide a list of commercial federal computer security products, and to report annually on federal computer security evaluations.

The Act requires the National Research Council of the National Academy of Sciences to study electronic authentication technologies, and the Director of NIST to develop technology-neutral electronic authentication infrastructure standards for federal agencies. The Director of NIST must also provide a list of commercially available authentication products, establish core specifications for federal electronic certification and management technologies, provide a list of conforming systems, and report annually on infrastructure implementation.

**Potential Implications for CMS:**

- NIST would be required to assist CMS in the protection of computer networks, and the response to unauthorized access.
- NIST would publish a list of commercially available security products that could be implemented to enhance the security of CMS operations. Each commercial product would undergo testing to ensure compliance with NIST standards.
- NIST would annually present an unclassified report to Congress detailing the results of security testing during the previous twelve months and the planned evaluations and tests for the following twelve months. This report would include any recommendations made by NIST to federal agencies resulting from the test results. This would require CMS compliance with federal security standards, and publicly expose any weaknesses in the security program.
- The studies conducted by the National Academy of Sciences and the Director of NIST would enable CMS to gain further knowledge of current and developing authentication technologies. The list of commercial products, and the development of authentication infrastructure standards would provide guidance on implementing secure authentication technologies and methodologies to strengthen the CMS security posture.

**Legislative Status:**

***House Status:*** This Bill was first introduced to the House on March 28, 2001.
***Senate Status:*** The Bill was referred to the Senate on November 28, 2001, read twice, and then referred to the Committee on Commerce, Science, and Transportation.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.1259:

### 5.1.3 H.R. 4561 & Senate (S.) 2492, Federal Agency Protection of Privacy Act of 2002

**Description:**

The Federal Agency Protection of Privacy Act is very similar to the Federal Privacy and Data Protection Policy Act of 2002 (section 3.1.3). Both Bills require all federal agencies to publish updates to all policies and practices regarding the protection of personally identifiable information. However, the Federal Agency Protection of Privacy Act also requires each agency to perform and make available for public comment an initial privacy impact analysis for the proposed changes to policy before they are enacted. The impact analysis should contain discussions of the following:

- Notice of collection of personally identifiable information (including what the information is).
- Any access to the information by the person to whom it pertains (for the purpose of making corrections, etc.).
- Mechanisms that prevent information from being used for any purpose other than that for which it was initially collected.
- Security of the information.

In addition, a summary and discussion of public comments must be made public with a final privacy impact analysis when a rule change takes effect as well as relevant steps taken by the agency to prevent unauthorized access to an individual's information.

**Potential Implications for CMS:**

- Under this Bill, if CMS were to consider making adjustments to privacy rules, the agency would first need to publish the proposed changes and an analysis of how the changes would affect the public.
- The proposed changes and the associated analysis should be made available to the public for feedback.

**Legislative Status:**

***House Status:*** This Bill, introduced to the House on April 24, 2002 and referred to the House Committee on the Judiciary
***Senate status:*** May 9, 2002, the Senate has referred the Bill to the Committee on Governmental Affairs.

**Source:**

THOMAS
*H.R. 4561*
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.4561:
*S.2492*
http://thomas.loc.gov/cgi-bin/query/z?c107:S.2492:

### 5.1.4 Senate (S.) 2629, Federal Privacy and Data Protection Policy Act of 2002

**Description:**

The Federal Privacy and Data Protection Act of 2002 will require all federal agencies to disclose their policies and practices regarding personal information. According to the Bill, "in order to ensure that people in the United States understand and have confidence in the proper use and safety of personal information, it is essential for agencies to implement effective privacy policies and procedures and to state those privacy policies, both online and offline."

**Potential Implications for CMS:**

- CMS would need to publish records indicating "the policies and practices of the agency for the security of personally identifiable information."
- CMS would be required to conduct annual internal "benchmark assessments" of their policies and practices, specifically those that concern the "collection, use, sharing, disclosure, transfer, and security of personally identifiable information."
- The Inspector General of each agency must contract with an outside privacy consultant to "evaluate the privacy and data protection practices of the agency."
- The annual benchmark assessment and outside review materials must be made available to the public on the website of the agency.

**Legislative Status:**

***Senate Status:*** This Bill was first introduced to the Senate on June 17, 2002. The Federal Privacy and Data Protection Policy Act of 2002 was referred to the Senate Committee on Governmental Affairs on June 17, 2002.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:S.2629:

### 5.1.5 H.R. 2435 – Cyber Security Information Act

**Description:**

The Cyber Security Information Act encourages the secure disclosure and protected exchange of information related to computer security problems, solutions, test practices and results, and other matters in connection with the protection of critical infrastructure resources. This Bill is focused primarily on providing businesses with incentives to share information related to network threats and vulnerabilities with the federal government.

**Potential Implications for CMS:**

- The enactment of this Bill would provide for the secure exchange of cyber-threat and vulnerability information, and better provide information to assist public and private sector organizations to protect critical resources.
- More timely data would be available to guide CMS in:
  i. Adopting more secure information security policies and procedures in coordination with private sector efforts,
  ii. Implementing additional technical security controls, and
  iii. Modifying existing security controls to provide increased levels of protection.

**Legislative Status:**

***House Status:*** This Bill was first introduced to the House of Representative on July 10, 2001. This Bill was referred to the House Committee on Government Reform and the House Committee on the Judiciary on July 10, 2001.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.2435:

### 5.1.6 H.R. 2915 Public Safety and Cyber Security Enhancement Act

**Description:**

This Act amends federal criminal law to provide an exception to current wiretap prohibitions for law enforcement personnel to intercept electronic communications of a "computer trespasser" to "protected" computer systems. Law enforcement personnel are also provided the ability to implement emergency pen registers and trap-and-trace devices during an ongoing attack on a protected computer system that constitutes a crime punishable by a term of imprisonment greater than one year, or for those instances where the attack represents an immediate threat to national security.

The term "protected computer system" refers to a computer system used exclusively by the United States government, or one that is utilized in interstate or foreign commerce or communications. The term "computer trespasser" refers to any person who gains access to a protected computer without authorization. Computer trespassers are considered unlawful, and therefore maintain no reasonable expectation of privacy in any communications transmitted to, through, or from the protected computer.

**Potential Implications for CMS:**

- The capabilities provided to law enforcement through this Act provide for increased measures in the detection, investigation, and immediate prevention of attacks against information resources.
- Federal law enforcement is granted the authority to monitor and perform surveillance upon individuals gaining unauthorized access to CMS computer systems, which will allow for the prosecution of computer trespassers.
- CMS would maintain increased control over the protection of information systems.

**Legislative Status:**

***House Status:*** This legislation was introduced to the House on September 20, 2001 and referred to the Committee on the Judiciary. On September 28, 2001 this Bill was referred to the Subcommittee on Crime.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.2915:

### 5.1.7 S. 1456 – Critical Infrastructure Information Security Act of 2001

**Description:**

This legislation prohibits critical infrastructure information voluntarily submitted to specified federal agencies from being made publicly available under the Freedom of Information Act. In addition, such information is prohibited from being used directly by the specified federal agency, any other federal, state, or local authority, or third party in a civil action, without the written consent of the person or organization submitting the critical infrastructure information, unless such information is submitted in bad faith.

The Critical Infrastructure Information Security Act of 2001 defines provisions for the notification, the dissemination and analysis of significant and credible information about the security of protected systems or critical infrastructure received by specified federal agencies from private persons and organizations.

The Act also directs the President to designate an element in the executive branch to conduct and report to information sharing and analysis organizations on strategic analyses of potential threats to the critical infrastructure.

**Potential Implications for CMS:**

- This Act would enable CMS to submit information to federal authorities without the risk of dissemination, public availability, or civil actions against the agency or its employees.
- Information regarding potential threats to information resources may be made available to CMS providing a better opportunity to protect against such threats.
- This Bill would enable CMS to share information relating to critical infrastructure threats.

**Legislative Status:**

***Senate status:*** This legislation was introduced to the Senate on September 24, 2001. On October 9, 2001 referred to the Committee on Energy and Natural Resources. Hearings held.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:S.1456:

### 5.1.8 S. 1568 – Cyberterrorism Prevention Act of 2001

**Description:**

This Bill is intended to deter and prevent cyber-terrorism in connection with computers by imposing more severe penalties for those convicted of computer crimes. In addition, this Bill requires the FBI to take appropriate actions to develop at least ten regional computer forensic laboratories, and provide support, education, and assistance for existing computer forensic laboratories. This will ensure that existing laboratories have the capability to:

1. Provide forensic examinations with respect to seized or intercepted computer evidence relating to criminal activity;
2. Provide training and education for federal, state, and local law enforcement personnel and prosecutors relating to the investigation, forensic analysis, and prosecution of computer related crime;
3. Assist federal, state, and local law enforcement in enforcing federal, state, and local criminal laws relating to computer crime;
4. Facilitate and promote the sharing of federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer related crime with state and local law enforcement personnel and prosecutors, including the use of multi-jurisdictional task forces; and
5. Carry out such other activities, as the Attorney General considers appropriate.

The Bill authorizes an annual appropriation of $50,000,000 for the purposes of carrying out these activities, and these funds will remain available until expended.

**Potential Implications for CMS:**

- Legal ramifications of computer crime may require the implementation of new policies and procedures for breach response methodology and the preservation of evidence.

**Legislative Status:**

***Senate Status:*** This legislation was introduced to the Senate on October 18, 2001 and referred to the Committee on the Judiciary.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:S.1568:

### 5.1.9 H.R. 3316 Computer Security Enhancement and Research Act

**Description:**

This Bill amends the NIST Act to establish research programs intended to improve the security of networked information systems, and to enhance the ability of NIST to improve computer security within the federal government. The research programs promote the development of an academic research community engaged in leading edge research on computer and communications security.

This legislation reinforces the role of NIST in providing guidance on security of unclassified information stored and processed in federal computer systems, and promotes technology solutions based on private sector offerings to protect the security of federal computer systems.

Appropriations are provided to NIST to support the funding of activities defined in the Act.

**Potential Implications for CMS:**

- CMS would be required to comply with enhanced NIST regulations to support increased levels of information security.
- NIST would develop the resources to publish standards and best practices to provide guidance to CMS on implementing and maintaining increased levels of information security, even as the security and technology fields evolve.

**Legislative Status:**

***House Status:*** This legislation was introduced to the House on November 16, 2001 and referred the House Committee on Science. On November 27, 2001 the Bill was referred to the Subcommittee on Environment, Technology, and Standards.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3316:

### 5.1.10 S. 1800 – Homeland Security Federal Workforce Act

**Description:**

The Homeland Security Federal Workforce Act would provide federal agencies and military establishments with human capital resources that may effectively support the homeland security requirements of the federal government, including technical security knowledge and skills. This Act enables federal agencies to obtain skilled personnel resources through incentive programs, including a student loan repayment program for federal employees in areas of critical importance.

This legislation provides necessary resources, accountability, and flexibility to meet the national security educational needs of the United States.

**Potential Implications for CMS:**

- The enactment of this legislation would provide CMS with increased capacity for attracting and acquiring skilled security personnel who may effectively support the CMS information security mission.

**Legislative Status:**

***Senate Status:*** This legislation was introduced to the Senate on December 11, 2001 and referred to the Committee on Governmental Affairs. On March 12, 2002, the Bill was referred to the Governmental Affairs Subcommittee on International Security, Proliferation and Federal Services, which has held hearings on the Bill.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:S.1800:

## 5.2 Privacy Legislation

This section includes descriptions of privacy-oriented legislation that may bear on the work of CMS.

The laws are presented in order of most recent Congressional activity; those that have been considered more recently are presented first, although that does not indicate the likelihood that a given Bill will become law. The current status of each law is included to indicate how far along laws are in the legislative process.

### 5.2.1 H.R. 89 – Online Privacy Protection Act of 2001

**Description:**

The Online Privacy Protection Act of 2001 makes it unlawful for an operator of a web-site or online service to collect, use, or disclose personal information concerning an individual in a manner that violates regulations to be prescribed by the Federal Trade Commission (FTC). The FTC regulations are intended to require online service operators to protect the confidentiality, security, and integrity of personal information collected from individuals. This Act also requires Web-site operators to provide a process for individuals to consent to or limit the disclosure of information.

This Act provides for enforcement through the Federal Trade Commission Act.

**Possible Implications:**

- CMS would be required to apply adequate security controls for the protection of personal information collected through online means, and to ensure the confidentiality, integrity, and security of such information during processing and storage.
- CMS may be required to develop and implement additional security policies and procedures, implement additional technical security controls, or modify existing security policies and technical controls.

**Legislative Status:**

***House Status:*** This legislation was introduced to the House on January 3, 2001 and referred to the House Committee on Energy and Commerce. On February 7, 2001 it was referred to the Subcommittee on Commerce, Trade and Consumer Protection.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.89:

### 5.2.2 H.R. 220 – Identity Theft Protection Act of 2001

**Description:**

The Identity Theft Protection Act of 2001 amends the Privacy Act of 1974 and the Social Security Act (42 U.S.C. 405(c)(2)) to prohibit any federal, state, or local government agency from requiring or requesting individuals to disclose Social Security Numbers. This Act also prohibits federal agencies from establishing any uniform national identifying numbers as well as imposing standards for identification of individuals on other agencies or persons.

**Possible Implications:**

- CMS would be prohibited from requiring or requesting individuals to disclose Social Security Numbers.
- CMS administrative policies may require modification to support the identification regulations addressed through this legislation.
  i. Prohibits federal agencies from establishing or mandating a uniform standard for individual identification that is required to be used within the agency, or by any other federal or state agency, or by a private person for regulating a transaction to which the federal government is not a party, or for administrative simplification.
  ii. Prohibits federal agencies from establishing or mandating a uniform standard for individual identification that is required to be used by any other federal or state agency, or by a private person except for conducting the activities of the federal agency establishing or mandating the standard.

**Legislative Status:**

***House Status***: This legislation was introduced to the House on January 3, 2001 and referred to the Committee on Ways and Means. It is currently being reviewed by the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.220:

### 5.2.3 S. 197 – Spyware Control and Privacy Protection Act

**Description:**

This Act prohibits computer software vendors from including capabilities to collect and disclose information about the user of such software, the hardware on which such software is used, or the manner in which such software is used. Only under specified exceptions may software incorporate these capabilities, including:

1. A clear notice that software contains such capabilities is provided to the user.
2. A description of the information subject to collection is provided to the user.
3. Clear electronic instructions on how to disable such capabilities without affecting software performance or operation are provided to the user.

The Act treats each violation of these prohibitions as unfair or deceptive acts or practices under the Federal Trade Commission Act.

**Possible Implications:**

- CMS would have to provide increased levels of protection over critical personal and organizational information.
- CMS would be notified by software vendors of spyware functionality and how to disable these capabilities in their products.

**Legislative Status:**

***Senate Status:*** On January 29, 2001, this legislation was introduced to the Senate and referred to the Committee on Commerce, Science, and Transportation.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:S.197:

### 5.2.4 H.R. 1215– Medical Info. Protection and Research Enhancement Act

**Description:**

This Act mandates administrative, technical, and physical safeguards for the protection of health information by specified health entities in possession of protected health information. These entities must also maintain a record of any protected health information disclosures.

The Bill prescribes guidelines for the disclosure of protected health information with respect to:

- Authorizations for treatment, payment, and health care operations.
- The individual's next of kin.
- Emergency circumstances.
- Certain oversight agencies.
- Public health authorities.
- Health researchers.
- Civil, judicial, and administrative procedures.
- Certain law enforcement procedures.
- Payment for health care through card or electronic means.
- Certain duly authorized representatives acting on behalf of a subject individual.
- Certain business sales, transfers, or mergers.

**Possible Implications:**

- CMS may be required to develop and implement administrative, technical, and physical security controls to ensure the protection of health information. This may involve the implementation of additional security controls and policies, or the modification of existing security controls to provide increased levels of protection.
- CMS may also be required to maintain detailed records of protected health information disclosures.

**Legislative Status:**

***House Status:*** This legislation was introduced to the House on March 27, 2001 and referred to the Committee on Energy and Commerce and the Committee on the Judiciary. On May 9, 2001 it was referred to the Subcommittee on Crime.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.1215:

### 5.2.5 S. 848 Social Security Number Misuse Prevention Act

**Description:**

This legislation prohibits the display, sale, or purchase of Social Security Numbers, and authorizes civil penalties for persons or organizations that the Attorney General determines have violated this Act. This Act sets forth enforcement procedures and criminal sanctions as well.

This Bill also amends the Social Security Act to prohibit governmental agencies from using Social Security Numbers on checks issued for payment. Civil monetary penalties for misuse of a Social Security Number are also extended through this legislation.

**Possible Implications:**

- CMS would be required to review and modify existing polices and procedures for the protection of Social Security Numbers as needed. This includes the logical protection of Social Security Numbers stored on computer systems, and the physical protection of Social Security Numbers printed on checks issued for payment.

- CMS may need to implement additional security controls to protect Social Security Numbers from display or disclosure, or modify existing security controls to provide increased levels of protection.

**Legislative Status:**

***Senate Status:*** This legislation was introduced to the Senate on May 9, 2001 and referred to the Committee on the Judiciary. On July 11, 2002 it was referred to the Committee on Finance Subcommittee on Social Security and Family Policy.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:S.848:

### 5.2.6 S. 851 – Citizen's Privacy Commission Act of 2001

**Description:**

This legislation establishes the Citizen's Privacy Commission, which is directed to study and report to Congress and the President on issues relating to the protection of individual privacy, and the appropriate balance to be achieved between protecting such privacy and allowing appropriate uses of information. This study will focus on the collection, use, and distribution of personal information by government, the privacy protection efforts and proposals of government, and individual redress for privacy violations by government.

**Possible Implications:**

- Policies and procedures for the collection, use, and distribution of personal information by CMS may also be reviewed during the process.
- The report to Congress and to the President may ultimately require CMS to change current privacy policies, and methods in which personal information is collected, used, and distributed. This may include the implementation of additional security controls to adequately protect personal information, or the modification of existing security controls to provide greater security.

**Legislative Status:**

***Senate Status:*** On May 9, 2001 this legislation was introduced to the Senate and referred to the Committee on Governmental Affairs.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:S.851:

### 5.2.7 House Resolution 159

*(Full title: Expressing the Sense of the House of Representatives that Machine-Readable Privacy Policies and the Platform for Privacy Preferences Project Specification are Important Tools in Protecting the Privacy of Internet Users, and for Other Purposes)*

**Description:**

A technology referred to as the Platform for Privacy Preferences Project (P3P) has been developed to enable web-site operators to implement a compact privacy policy that can be read and interpreted by client web browser software. This legislation calls for executive departments and agencies to deploy P3P-compliant privacy policies on their web-sites. The Bill also calls for current and future legislation relating to online privacy to investigate the use of the P3P specification, and for the education of Internet users concerning P3P.

This Bill also calls for commercial software vendors to support and implement fully the P3P specification.

**Possible Implications:**

- CMS would be required to implement P3P-compliant privacy policies on the CMS organizational website
- CMS web-site users would need to be made aware of the organizational privacy policy.

**Legislative Status:**

***House Status***: This legislation was introduced to the House on June 7, 2001 and referred to the Committee on Energy and Commerce and to the Committees on House Administration, and Government Reform. On July 9, 2001, the Bill was referred to the Subcommittee on Technology and Procurement.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:H.RES.159:

### 5.2.8 H.R. 2135 – Consumer Privacy Protection Act

**Description:**

The Consumer Privacy Protection Act defines limitations upon the disclosure by an information recipient of consumer personal information. This Act authorizes civil suits brought in Federal district courts by consumers for violations of this Act, or a State for any person or entity engaging in a pattern or practice of such violations.

**Possible Implications:**

- CMS would be required to take measures to protect information received from consumers (general public requesting services), and prevent disclosure of such information.
- Technical security controls and organizational policy may need to be developed and implemented.

**Legislative Status:**

***House Status***: On June 12, 2001 this Bill was introduced to the House and referred to the House Committee on Energy and Commerce. On June 18, 2001, it was referred to the Subcommittee on Commerce, Trade and Consumer Protection.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.2135:

### 5.2.9 S. 1014– Social Sec. Number Privacy and Identity Theft Protection

**Description:**

This Act amends title II of the Social Security Act to specify restrictions on the sale or public display of Social Security Numbers, or any derivatives of these numbers by federal, state, and local governments. The Act also prohibits the display of Social Security Account Numbers on checks issued for payments by federal agencies, the display of Social Security Numbers (or any derivatives) on employee identification cards, and the display, sale, or purchase of Social Security Numbers.

**Possible Implications:**

- CMS would be required to protect employee Social Security Numbers adequately, by both technical and non-technical means.
- CMS must ensure that Social Security Numbers stored on data systems are not accessible in any means that could lead to disclosure or display.
- Payment and employee identification procedures may require modification if they currently utilize Social Security Numbers or any derivative of such numbers. This includes employee identification numbers present on badges, labels, and paychecks, and includes the format of system user ID's that may be based upon Social Security Numbers.

**Legislative Status:**

***Senate Status:*** This legislation was introduced to the Senate on June 12, 2001 and referred to the Committee on Finance.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:S.1014:

### 5.2.10 S. 1055 – Privacy Act of 2001

**Description:**

The Privacy Act of 2001 amends federal criminal law to prohibit the display, sale, or purchase of Social Security Numbers without the expressed consent of the individual. This Bill also amends the Social Security Act to prohibit the use of Social Security Account Numbers on checks issued for payment by governmental agencies. In addition, the Privacy Act of 2001 closely regulates the activities of commercial entities in the collection, sale, and disclosure of personally identifiable information and Social Security Numbers.

**Possible Implications:**

- CMS would be required to implement proactive security controls to protect sensitive personal information, including Social Security Numbers. CMS and CMS staff could face legal action for the display of Social Security Numbers without expressed consent.
- CMS must accordingly implement policy for the protection of the confidentiality of stored and processed Social Security Numbers.

**Legislative Status:**

***Senate Status***: This legislation was introduced to the Senate on June 14, 2001 and referred to the Committee on the Judiciary. On February 14, 2002 it was referred to The Committee on the Judiciary Subcommittee on Technology, Terrorism, and Government Information.

**Source:**

THOMAS
http://thomas.loc.gov/cgi-bin/query/z?c107:S.1055:

# 6. Expired Legislation

This section of the report includes those computer security Bills that have expired and are no longer law. Following each summary is a list of the specific requirements for CMS that were stipulated by the law.

The laws in this section are presented in the order in which they became inactive.

## 6.1 The Government Information Security Reform Act (October 2000)

**Description:**

The Government Information Security Reform Act (GISRA) requires the Director of the OMB to establish government-wide policies for the management of programs that support the implementation of cost-effective security mechanisms for federal information systems, which promote security as an integral component of each federal agency's business operations, and which include information technology architectures as defined under the Clinger-Cohen Act of 1996.

The GISRA legislation outlines the information security responsibilities of each agency, including the development and implementation of agency-wide security plans for agency operations and assets. In addition, each agency's security program is subject to approval by the Director of OMB, and to annual review by agency security officials. In addition to the internal security review, GISRA requires each agency to undergo annually an independent evaluation of its information security program and practices. Related reports should be produced detailing such activity.

The mission critical information security policies developed by the Department of Defense and the Central Intelligence Agency may be adopted by the Director of OMB and heads of other federal agencies with respect to mission critical systems under GISRA. In addition, GISRA enables agencies to develop and implement more stringent information security policies than those required under the Act.

**Implications for CMS:**

- Agencies must implement risk-based security plans that apply to all stages of the life cycle for any agency system that supports the agency's operations and assets.
- The CMS Administrator is charged with implementing the NIST guidelines for information security on federal computer systems.
- All agencies must have procedures in place for detecting, reporting, and responding to security incidents.
- Policies and procedures must be clearly documented for sharing any information with appropriate authorities.
- Responsibilities of specific agency officials are described in the Bill.
- CMS must provide security awareness training for operators of information systems.
- Agency-wide security programs, and all operations addressed by the security programs, should be reviewed each year by agency officials (an internal assessment). Each agency shall include this report to the OMB with budget requests. The annual agency self-assessment should include an independent report by the agency's Inspector General.
- Agencies must report all deficiencies in their information security programs to the OMB.

- Agencies must identify, use, and share best security practices.
- This law has expired, but it was replaced with the Federal Information Security Management Act, which is currently included as Title III of the E-Government Act (H.R. 2458).

## Source:

NARA
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ398.106