1. FISMA, TITLE X OF THE HOMELAND SECURITY ACT AND TITLE III OF E-GOVERNMENT ACT OF 2002

As of November 2002, the Government Information Security Reform Act (GISRA) expired. The Federal Information Security Management Act (FISMA) of 2002, which was passed as TITLE X of The Homeland Security (signed into law on November 27, 2002) Act and TITLE III of the E-Government Act of 2002 (signed into law on December 17, 2002) are now in effect. These laws have been analyzed and the attached matrices are a comparison of FISMA as enacted (Sec. 3 Analysis Matrix-FISMA), and the subject areas in which Section 11332 of Title 40, United States Code correlates with E-Government Act of 2002 (Sec. 4 Analysis Matrix-Computer Security Act of 1987- Repeal of Section 11332). 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:

New paragraphs
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)

New Subsection:
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].

FISMA grants more responsibility to the National Institute of Standards and Technology (NIST) to develop and maintain standards for minimum information security controls. Compliance with the standards will be compulsory.

In addition, The Computer Security Act Section 11332 of Title 40, United States Code was repealed under FISMA.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 Public Law 107-217 August 21, 2002. Section 11332 addressed the federal computer system security training and plan. The attached matrix under section 4 of this document, Analysis Matrix-Computer Security Act of 1987- Repeal of Section 11332, demonstrates the subject areas in which Section 11332 of Title 40, United States Code correlates with E-Government Act of 2002.

[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

2. ANALYSIS MATRIX - FISMA

The following matrix is a comparison of FISMA as enacted in TITLE X Homeland Security Act of 2002 and TITLE III E-Government Act of 2002.

Sec No./ Para No.	FISMA, TITLE X Homeland Security Act of 2002	Sec No./ Para No.	FISMA, TITLE III E-Government Act of 2002
Sec 3532 (b) (2)	**`Sec. 3532. Definitions** `(b) ADDITIONAL DEFINITIONS- As used in this subchapter-- … `(2) the term `national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency …	**Sec 3542 (b) (2) (A) (ii)**	**§ 3542. Definitions** ‘‘(b) ADDITIONAL DEFINITIONS. —As used in this subchapter: … ‘‘(2)(A) The term ‘national security system’ means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency … ‘‘(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Sec. 3533 (a)	**`Sec. 3533. Authority and functions of the Director** `(a) The Director shall oversee agency information security policies and practices …	**Sec 3543 (a) (7)**	**§ 3543. Authority and functions of the Director** a) IN GENERAL. —The Director shall oversee agency information security policies and practices … . ‘‘(7) overseeing the operation of the Federal information security incident center required under section 3546;
Sec. 3533 (a) (8)	`(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including …	**Sec 3543 (a) (8) (B)**	‘‘(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including … ‘‘(B) an assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) and promulgated under section 11331 of title 40;

Sec No./ Para No.	FISMA, TITLE X Homeland Security Act of 2002	Sec No./ Para No.	FISMA, TITLE III E-Government Act of 2002
		Sec 3543 (c)	‘‘(c) DEPARTMENT OF DEFENSE AND CENTRAL INTELLIGENCE AGENCY SYSTEMS. —(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of Central Intelligence in the case of systems described in paragraph (3)…
Sec 3535 (e)	`Sec. 3535. Annual independent evaluation `(e) Each year, not later than such date established by the Director, the head of each agency shall …	**Sec 3545 (e) (2)**	**§ 3545. Annual independent evaluation** “(e) AGENCY REPORTING.—(1) Each year, not later than such date established by the Director, the head of each agency shall … ‘‘(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director …
		Sec 3546 (a) (1)	**‘‘§ 3546. Federal information security incident center** ‘‘(a) IN GENERAL. —The Director shall ensure the operation of a central Federal information security incident center — ‘‘(1) provide timely technical assistance to operators of agency information systems regarding security incidents …
Sec. 11331 (b)	**Sec. 11331. Responsibilities for Federal information systems standards** `(b) REQUIREMENT TO PRESCRIBE STANDARDS- `(1) IN GENERAL- `(A) REQUIREMENT- Except as provided under paragraph (2), the Director of the Office of Management and Budget shall…	**Sec 11331 (a) (1)**	**§ 11331. Responsibilities for Federal information systems standards** ‘‘(a) STANDARDS AND GUIDELINES. — ‘‘(1) AUTHORITY TO PRESCRIBE. —Except as provided under paragraph (2), the Secretary of Commerce shall, …
Sec 11331 (b) (1) (B)	`(B) REQUIRED STANDARDS- Standards promulgated under subparagraph (A) shall include-- `(i) standards that provide minimum information security requirements …	**Sec 11331 (b)**	‘‘(b) MANDATORY REQUIREMENTS. — ‘‘(1) AUTHORITY TO MAKE MANDATORY. —Except as provided under paragraph (2), the Secretary shall make standards prescribed under subsection …

Sec No./ Para No.	FISMA, TITLE X Homeland Security Act of 2002	Sec No./ Para No.	FISMA, TITLE III E-Government Act of 2002
		Sec 11331 (c)	‘‘(c) AUTHORITY TO DISAPPROVE OR MODIFY. —The President may disapprove or modify the standards and guidelines referred to in subsection (a)(1) if the President determines such action to be in the public interest. …
		Sec 11331 (g)	‘‘(g) DEFINITIONS. —In this section:
SEC. 1003 (d) (1)	**SEC. 1003. National Institute of Standards and Technology.** `(d) The Institute shall-- `(1) submit standards developed pursuant to subsection (a) …	**SEC. 303 (d) (6)**	**SEC. 303. National Institute of Standards and Technology.** ‘‘(1) submit standards developed pursuant to subsection (a) … ‘‘(d) INFORMATION SECURITY FUNCTIONS. —The Institute shall … ‘‘(6) assist the private sector, upon request, in using and applying the results of activities under this section;
		SEC. 303 (f)	‘‘(f) AUTHORIZATION OF APPROPRIATIONS. —There are authorized to be appropriated to the Secretary of Commerce $20,000,000 for each of fiscal years 2003, 2004, 2005, 2006, and 2007 to enable the National Institute of Standards and Technology to carry out the provisions of this section.’’

3. ANALYSIS MATRIX- COMPUTER SECURITY ACT OF 1987- REPEAL OF SECTION 11332

The following matrix is a correlation between section 11332 of Title 40, United States Code and E-Government Act. Section 11332 of Title 40, United States Code was repealed under FISMA.

Sec No./ Para No.	Computer Security Act - Section 11332 of Title 40, United States Code	Sec No./ Para No.	E-Government Act of 2002
Sec. 11332 (b)	b) TRAINING— (1) IN GENERAL. —Each federal agency shall provide for mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each federal computer system within or under the supervision of the agency.	**Sec 209 (b) (2)** **Sec. 3707 (f)**	**(2) INFORMATION TECHNOLOGY TRAINING PROGRAMS. —**The head of each Executive agency, after consultation with the Director of the Office of Personnel Management, the Chief Information Officers Council, and the Administrator of General Services, shall establish and operate information technology training programs consistent with the requirements of this subsection. (f) REPORT ON THE ESTABLISHMENT OF A GOVERNMENTWIDE INFORMATION TECHNOLOGY TRAINING PROGRAM. — (1) IN GENERAL. —Not later January 1, 2003, the Office of Personnel Management, in consultation with the Chief Information Officers Council and the Administrator of General Services, shall review and submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate a written report on the following: (A)The adequacy of any existing information technology training programs available to Federal employees on a Government-wide basis. (B)(i) If one or more such programs already exist, recommendations as to how they might be improved. (ii) If no such program yet exists, recommendations as to how such a program might be designed and established. (C) With respect to any recommendations under subparagraph (B), how the program under chapter 37 of title 5, United States Code, might be used to help carry them out.

Sec No./ Para No.	Computer Security Act - Section 11332 of Title 40, United States Code	Sec No./ Para No.	E-Government Act of 2002
	The training shall be– (A) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the Act (15 U.S.C. 278g-3(a)(5)) and the regulations prescribed under paragraph (3) for federal civilian employees; or	**Sec. 3543 (a) (3)** **Sec. 209 (b) (2)**	‘‘(a) IN GENERAL. —The Director shall oversee agency information security policies and practices, including— ‘‘(3) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems; (2) INFORMATION TECHNOLOGY TRAINING PROGRAMS… shall establish and operate information technology training programs consistent with the requirements of this subsection.
	(B) provided by an alternative training program that the head of the agency approves after determining that the alternative training program is at least as effective in accomplishing the objectives of the guidelines and regulations.	**Sec. 209 (b) (2)**	(2) INFORMATION TECHNOLOGY TRAINING PROGRAMS. — The head of each Executive agency, after consultation with the Director of the Office of Personnel Management, the Chief Information Officers Council, and the Administrator of General Services, shall establish and operate information technology training programs consistent with the requirements of this subsection.

Sec No./ Para No.	Computer Security Act - Section 11332 of Title 40, United States Code	Sec No./ Para No.	E-Government Act of 2002
	2) TRAINING OBJECTIVES. — Training under this subsection shall be designed— (A) to enhance employees' awareness of the threats to, and vulnerability of, computer systems; and (B) to encourage the use of improved computer security practices.	**Sec. 209 (b) (2)**	(2) INFORMATION TECHNOLOGY TRAINING PROGRAMS… Such programs shall— (A) have curricula covering a broad range of information technology disciplines corresponding to the specific information technology and information resource management needs of the agency involved; (B) be developed and applied according to rigorous standards; and (C) be designed to maximize efficiency, through the use of self-paced courses, online courses, on-the-job training, and the use of remote instructors, wherever such features can be applied without reducing the effectiveness of the training or negatively impacting academic standards.
		Sec. 3544 (b) (4)	Sec. 3544 (b) (4) ''(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of— ''(A) information security risks associated with their activities; and ''(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

Sec No./ Para No.	Computer Security Act - Section 11332 of Title 40, United States Code	Sec No./ Para No.	E-Government Act of 2002
	(3) REGULATIONS. —The Director of the Office of Personnel Management shall maintain regulations that establish the procedures and scope of the training to be provided federal civilian employees under this subsection and the manner in which the training is to be carried out.	**Sec. 209 (b) (3)**	(3) GOVERNMENTWIDE POLICIES AND EVALUATION.— The Director of the Office of Personnel Management, in coordination with the Director of the Office of Management and Budget, shall issue policies to promote the development of performance standards for training and uniform implementation of this subsection by Executive agencies, with due regard for differences in program requirements among agencies that may be appropriate and warranted in view of the agency mission. The Director of the Office of Personnel Management shall evaluate the implementation of the provisions of this subsection by Executive agencies.
Sec. 11332 (c) (1)	(c) PLAN. — (1) IN GENERAL. —Consistent with standards, guidelines, policies, and regulations prescribed pursuant to section 11331 of this title, each federal agency shall maintain a plan for the security and privacy of each federal computer system the agency identifies as being within or under its supervision and as containing sensitive information. The plan must be commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information contained in the system.	**Sec. 3544 (a) (1)**	‘‘(1) be responsible for— ‘‘(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of— ‘‘(i) information collected or maintained by or on behalf of the agency; and ‘‘(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
	2) REVISION AND REVIEW. —The plan shall be revised annually as necessary and is subject to disapproval by the Director of the Office of Management and Budget.	**Sec. 3544 (b)**	‘‘(b) AGENCY PROGRAM. —Each agency shall develop, document, and implement an agency-wide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—
Sec. 11332 (d)	(d) HANDLING OF INFORMATION NOT AFFECTED. —This section does not— (1) constitute authority to withhold information sought pursuant to section 552 of title 5; or requiring or authorizing the public	**Sec 206 (b)**	b) INFORMATION PROVIDED BY AGENCIES ONLINE. — To the extent practicable as determined by the agency in consultation with the Director, each agency (as defined under section 551 of Title 5, United States Code) shall ensure that a

Sec No./ Para No.	Computer Security Act - Section 11332 of Title 40, United States Code	Sec No./ Para No.	E-Government Act of 2002
	disclosure of information; or 2) authorize a federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is— (A) privately owned information; disclosable under section 552 of title 5 or another law (C) public domain information		publicly accessible Federal Government website includes all information about that agency required to be published in the Federal Register under paragraphs (1) and (2) of section 552(a) of title 5, United States Code.