FEDERAL STUDENT AID

We Help Put America Through School

The Government Information Security Reform Act (GISRA)

Replaced by

The Federal Information Security Management Act (FISMA)

April 1, 2003

Key Questions

1. What was GISRA?
2. What did FSA do in the past?
3. What is FISMA?
4. How is FSA going to approach FISMA?

© 2003 BearingPoint, Inc.

For FSA SSO's GISRA Was …

- The Government Information Security Reform Act
- Filling out the 261 question Self-Assessment Questionnaire for the 5 performance levels (Policies, Procedures, Implementation, Testing, and Integration)
  - 17 Control Areas
  - 36 Critical Elements

Expired November 2002

© 2003 BearingPoint, Inc.

Remember This?

Department of Education
NIST SELF-ASSESSMENT SUBMISSION FORM

PLEASE NOTE: Use one template per system or resource. Answers for each question are only required in columns F through M. Enter a 'Y' in columns F through K for all that apply, comments can entered in column L for each question, and initials in column M. All questions are grouped by category and in some cases further grouped by subcategory1 & subcategory2. Click the plus signs in the far left column to expand the categories. When a minus sign is displayed, there are no further subcategories beneath.

QUESTION	CRITICAL ELEMENT		POLICY	PROCEDURE	IMPLEMENTED	TESTED	INTEGRATED	RISK DECISION	COMMENTS	INITIALS
			Check 'Y' for Yes where controls are in place. If not applicable, place an "N/A" in the field. Leave blank if control is not in place.						NOTE: Text will wrap within field	
MGT CONTROLS										
Risk Mgt										
1	Yes	Is risk periodically assessed?	Y	Y	Y					
2		1.1.1 Is the current system configuration documented, including links to other systems? NIST SP 800-18	Y	Y	Y				FSA Policy Sect 2.3	
3		1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? FISCAM SP-1	Y	Y	Y				FSA Policy Sect 2.1	
4		1.1.3 Has data sensitivity and integrity of the data been considered? FISCAM SP-1	Y	Y	Y				FSA Policy Sect 2.1	
5		1.1.4 Have threat sources, both natural and manmade, been identified? FISCAM SP-1	Y	Y	Y				FSA Policy Sect 2.1	
6		1.1.5 Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current? NIST SP 800-30[1]	Y	Y	Y				FSA Policy Sect 2.1	
7		1.1.6 Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities?	Y	Y	Y				FSA Policy Sect 2.1	
8	Yes	Do program officials understand the risk to systems under their control and determine the acceptable level of risk?	Y							
9		1.2.1 Are final risk determinations and related management approvals documented and maintained on file? FISCAM SP-1	Y						FSA Policy Sect 2.1	
10		1.2.2 Has a mission/business impact analysis been conducted? NIST SP 800-30	Y						FSA Policy Sect 2.1	
11		1.2.3 Have additional controls been identified to sufficiently mitigate identified risks? NIST SP 800-30	Y						FSA Policy Sect 2.1	

© 2003 BearingPoint, Inc.

FISMA Is …

- The Federal Information Security Management Act (passed as part of E-Government Act of 2002)
- Similar to GISRA, but some changes include:
  - Requirement to report to Congress and others more explicit (not just through OMB)
  - The IG's independent review must now include actual "testing" of the effectiveness of IT security policies, procedures and practices of "a representative subset of the agency's information systems" (i.e. testing of the requirements in the self-assessment questionnaire)
  - Risk based decisions now limited because of the requirement that NIST and OMB must promulgate minimum mandatory management controls for securing IT systems (which will be "compulsory and binding")

© 2003 BearingPoint, Inc.

How is FSA going to approach FISMA?

- Guidance from OMB expected in April 2003. Once FSA receives the guidance the Security and Privacy team will provide training.
- We expect FSA's SSO's roles to be similar to GISRA
  - SSO's or contractors filling out the 261 question Self-Assessment Questionnaire for the 5 performance levels
    - 17 Control Areas
    - 36 Critical Elements
- Some possible changes however to POA&M's submitted by systems
  - POA&M's this year may also be based off the self-assessment questionnaire.
  - The Critical Elements that have not reached Level 3 (Implemented) will be considered a weakness. The underlying questions to the critical elements will then be considered the milestones to remediation of the weaknesses found.

© 2003 BearingPoint, Inc.