

How Grades Were Assigned

The Subcommittee's computer security grades were based on information contained in agencies' and Inspectors General's (IGs) Federal Information Security Management Act (FISMA) reports to the Office of Management and Budget (OMB) for fiscal year 2003.

On December 17, 2002, the President signed into law the Electronic Government Act. Title III of that Act is the FISMA. FISMA lays out the framework for annual IT security reviews, reporting and remediation planning at federal agencies. It seeks to strengthen federal government information security by reauthorizing and expanding the information security, evaluation, and reporting requirements enacted into law as the Government Information Security Reform provisions (commonly referred to as "GISRA") in the National Defense Authorization Act for fiscal year 2001. FISMA requires that agency heads and IGs evaluate their agencies' computer security programs and report the results of those evaluations to the OMB in September of each year along with their budget submissions. FISMA also requires that agency heads report the results of those evaluations annually to the Congress and the General Accounting Office.

On August 6, 2003, OMB provided this year's final reporting guidance to agencies and IGs on implementing the provisions of FISMA. OMB instructed the agencies to submit reports summarizing the results of annual IT security reviews of systems and programs, agency progress on correcting identified weaknesses, and the results of IG independent evaluations. As with last year's guidance, specific performance metrics were required for agency heads, program officials, chief information officers and IGs to use in assessing and reporting their agencies' actual level of performance.

Effect of Changes in Legislation on Reporting and Grading

FISMA incorporated several significant changes from GISRA, including:

- Requiring annual reports to contain information regarding: (1) agency risk assessments; (2) security policies and procedures; (3) subordinate plans; (4) training of employees; (5) annual testing and evaluation; (6) process for corrective actions; (7) security incident reporting; and, (8) continuity of operations planning.
- Requiring each agency to develop specific system configuration requirements that meet their needs and ensure compliance with those requirements.
- Requiring that at least annually, agencies perform testing and evaluation of the effectiveness of information security policies, procedures, and practices. Furthermore, the testing must include management, operational and technical controls.
- Requiring that each agency's security program ~~must~~ include provision for the continuity of operations for information systems that support agency activities.

- Requiring the Department of Commerce, through the National Institute of Standards and Technology, to develop compulsory and binding standards that will be used to categorize all information and information systems collected or maintained by or on behalf of each agency.
- Requiring each agency to appoint a Senior Agency Information Security Officer
- Providing additional details on the reporting of significant deficiencies, tying the reporting to both the Federal Managers Financial Integrity Act and the Federal Financial Management Improvement Act.
- Requiring the head of each agency to develop and maintain an inventory of major information systems (including national security systems) operated by, or under the control of, the agency. The identification of systems must include an identification of interfaces between each system and all other systems or networks, including those not owned, or operated, by the agency. This inventory must be updated annually.

Assignment of Grades

In assigning grades, the Subcommittee followed the weighted point values that were used to develop the fiscal year 2002 GISRA grades with the exception of those where changes in FISMA required that adjustments be made (see below). This ensures consistency in the methodology used to assign grades and serves to highlight progress made by an agency if this year's grade indicates improvement.

The weighted scores are based on OMB's performance metrics, with a perfect score totaling 100 points. Since most questions provide for a range of responses, the number of points assigned to each response is proportional to the extent the element has been implemented. For example, agencies received zero (0) points for a response indicating a percentage that falls below an acceptable threshold (such as 29% or less of employees who received security training). Proportionally, more points were given for answers that ranged between 30 and 44%, 45 and 59%, etc. The full weighted value was awarded for answers that ranged between 90 and 100%. Similarly, partial points were awarded for on-going implementation of actions, full points for completed implementation, etc.

Based on its analysis of the agency and the IG's responses, the Subcommittee tallied the scores for the 24 agencies. The final numerical score is the basis for the agency's letter grade. Letter grades for the 24 major departments and agencies were assigned as follows:

90 to 100 = A
 80 to 89 = B
 70 to 79 = C
 60 to 69 = D
 59 and lower = F

Major Changes to the Weighting of Grades

Changes in legislation required the Subcommittee to make several changes to the scoring methodology that was used to determine the GISRA grades in 2002. The major changes are listed below

The Department of Homeland Security (DHS) was established on January 24, 2003. The Department combined 22 separate agencies involved in a wide variety of activities. One of the agencies entirely subsumed by DHS was the Federal Emergency Management Agency (FEMA), which was separately graded last year. The grade for DHS reflects the status of the Department from January to September of 2003. FEMA has not been graded separately.

Several questions were consolidated to reflect changes in FISMA. For example, FISMA consolidates under the agency head many responsibilities that under GISRA were assigned to program officials and CIOs. Questions have been consolidated to reflect this. Nevertheless, to maintain consistency with last year, the weighting of these questions remains largely the same.

New questions were added to reflect FISMA's requirement that agencies follow NIST guidance and develop plans for mitigating identified weaknesses. In addition, questions related to Project Matrix were reworded or eliminated to reflect the changing status of that program.

Finally, FISMA requires that agencies develop and maintain inventories of their critical systems. To accommodate this change while maintaining consistency with previous years' scoring, this requirement has been incorporated by adjusting the final score. If an agency has developed and maintained an inventory, zero (0) points were deducted from the final score. If the agency is in the process of developing an inventory, five (5) points were deducted (i.e., if the agency has a score of 70, but has not fully developed an inventory, the final score would be adjusted to 65). If the agency has not even begun developing an inventory, ten (10) points were deducted.

Lack of IG Reports

The IGs for the Departments of Veterans Affairs, the Treasury, and Defense did not submit their reports as required by FISMA. Therefore, the Subcommittee did not have access to an independent evaluation of the information security programs at these agencies. As a result, scores for these agencies are based solely on the information self-reported by the agencies and may not reflect the same accuracy as the scores of the other 21 agencies, whose scores are based on more objective reporting. However, for the Department of Treasury, we did have access to the report of the Inspector General for Tax Administration, which reported on the Internal Revenue Service, which constitutes approximately 80% of the Department's systems.