How Grades Were Assigned

The Committee's computer security grades are 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 2005.

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. FISMA requires that agency heads and IGs evaluate their agencies' computer security programs and report the results of those evaluations to 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 Government Accountability Office.

OMB's 2005 reporting guidance instructed the agencies and IGs 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 other work performed during the reporting period. Agencies and IGs were required to use OMB's performance measures in assessing and reporting the status of their agencies' security programs. In addition, agencies were permitted to include additional performance measures they had developed.

Assignment of Grades

In assigning grades, the Committee followed the methodology developed for the fiscal year 2004 FISMA grades, with the exception of adjustments required by changes in OMB's FISMA reporting instructions (see below). This approach 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. OMB provided a range of responses for most questions. 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 (for example: 50% or less of known IT security weaknesses being incorporated in the Plan of Action and Milestones). Proportionally, more points were given for answers that ranged between 51 and 70%, 81 and 95%, etc. The full weighted value was awarded for answers that ranged between 96 and 100%.

For more specific weighting of questions see the scoring methodology.

The Committee tallied the scores for the 24 agencies on the basis of its analysis of agency and IG responses. 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 93 = A-	94 to 96 = A	97 to 100 = A+
80 to 83 = B-	84 to 86 = B	87 to 89 = B+
70 to 73 = C-	74 to 76 = C	77 to 79 = C+
60 to 63 = D-	64 to 66 = D	67 to 69 = D+
59 and lower = F		

Major Changes to the Weighting of Grades

Changes in OMB's FISMA reporting instructions from FY04 to FY05 required the Committee to make several adjustments to the scoring methodology that was used to determine the FISMA grades. The major changes are listed below.

To facilitate future consistency, the Committee continued using the following major categories: Annual Testing, Plan of Action and Milestones, Certification and Accreditation, Configuration Management, Incident Detection and Response, Training and Systems Inventory. Changes for each area are listed below.

Annual Testing – Removed questions regarding the CIO and NIST self-assessment that are not included in OMB's FY05 FISMA reporting guidance. Expanded questions regarding the review of agency and contractor systems, to include impact levels. Added question regarding IGs' evaluation of the agency's oversight. If an IG indicates a range of 96 to 100%, no points are taken; if between 51 and 95 % the agency loses half of its annual testing points; if 50% or less, the agency loses all annual testing points.

Plan of Action and Milestones – Removed agency-related POA&M question since it is not in FY05 FISMA reporting guidance. All POA&M questions for FY05 FISMA reporting were directed to the IG.

Certification and Accreditation – Removed question relating to security controls being integrated into the life cycle, as this issue is no longer a reporting requirement. Expanded questions to include impact levels—high, moderate, low.

Configuration Management – Removed the question regarding the patching of security vulnerabilities and added a question regarding emerging technologies.

Incident Response and Detection – Removed the question regarding systems undergoing vulnerability scans and penetration tests.

Training – No changes made.

Inventory – Removed agency-related inventory question and added two new IG questions for a total of three questions. The IG must rate the agency at 96% to 100% for all three questions or a full letter grade will be deducted from the final score.

Improvements still Needed

Although many agencies reported improvements in their implementation of FISMA, such as certifying and accrediting a higher percentage of their systems and maintaining an inventory, much work is still needed to ensure federal information systems are secure. Areas of continued weaknesses include:

- Annual Testing
    a. Some agencies reported large numbers of their systems as uncategorized. These agencies coincidentally all scored in the F range.
    b. While many agencies show improvements over last year in testing their contingency plans, several report testing under 60% of contingency plans for high-impact systems.
- Configuration Management
  Many agencies have begun to develop or have these policies; however, several agencies continue to have a low level of implementation.
- Incident Reporting
  Agencies continued to show inconsistencies in reporting incidents. Some agencies reported few or no incidents. Several reported less than half of all incidents to USCERT.
- Training
  Most agencies have ensured that their employees have received security training and awareness; however, agencies are less successful in ensuring that those with significant security responsibilities receive specialized training.
- Inventory
  Many agencies have not developed an inventory of major IT systems.
- Overall
  Four of the largest agencies have failing scores: Treasury, DOD, DHS, USDA.