Second

REPORT CARD

On

COMPUTER SECURITY

At

Federal Departments and Agencies

Overall Grade: F

November 9, 2001

Computer Security Report Card

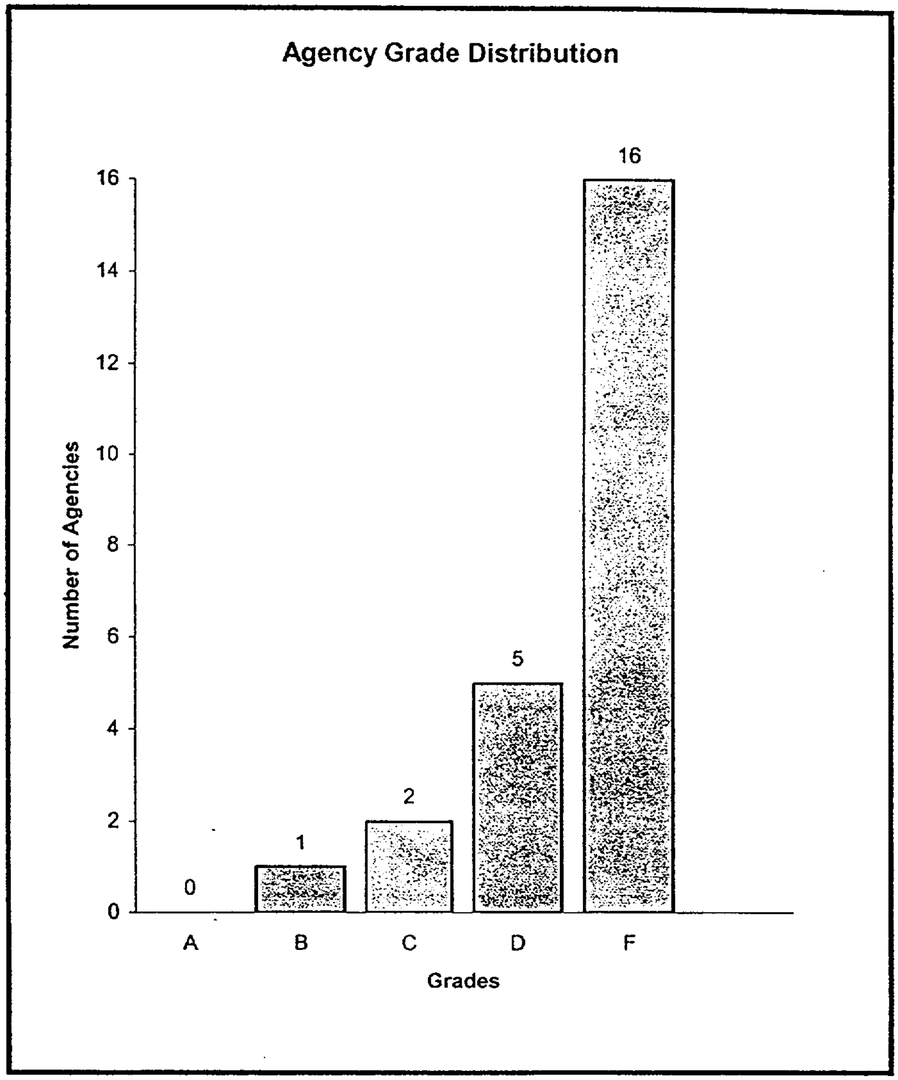
November 9, 2001

Departments and Agencies	Grade
NSF National Science Foundation	B+
SSA Social Security Administration	C+
NASA National Aeronautics & Space Administration	C-
EPA Environmental Protection Agency	D+
State Department of State	D+
FEMA Federal Emergency Management Agency	D
GSA General Services Administration	D
HUD Department of Housing and Urban Development	D
Agriculture Department of Agriculture	F
AID Agency for International Development	F
Commerce Department of Commerce	F
Defense Department of Defense	F

Departments and Agencies	Grade
Education Department of Education	F
Energy Department of Energy	F
HHS Department of Health & Human Services	F
Interior Department of the Interior	F
Justice Department of Justice	F
Labor Department of Labor	F
NRC Nuclear Regulatory Commission	F
OPM Office of Personnel Management	F
SBA Small Business Administration	F
Transportation Department of Transportation	F
Treasury Department of the Treasury	F
VA Department of Veterans Affairs	F
Governmentwide Grade	F

Prepared for Charman Stephen Horn, Subcomittee on Government Efficiency, Financial Management and Intergovernmental Relations. Based on agency reports required by the Security Act of 2000, and GAO and Inspectors General audit reports issued from July 2000 through September 2001.

Subcommittee Home Page: http://www.house.gov/reform/gefmir.htm


Agency Grade Distribution
Number of Agencies
16
14
12
10
8
6
4
2
0
0
1
2
5
16
A
B
C
D
F
Grades

How Grades Were Assigned

The subcommittee's computer security grades are based on information contained in agency reports to the Office of Management and Budget, and audit work conducted by agency Inspectors General and the General Accounting Office.

Last year, the Government Information Security Reform Act of 2000 (Security Act) was signed into law as part of the FY 2001 National Defense Authorization Act (P.L. 106-398). Among its provisions, the Act requires agency Chief Information Officers (CIOs) and Inspectors General (IGs) to evaluate their agency's computer security programs and report the results of those evaluations to the Office of Management and Budget (OMB) in September of each year.

In June 2001, the OMB issued reporting guidance to agencies on implementing the Security Act, directing them to transmit copies of the annual agency program reviews, the IG's independent evaluations, and an executive summary. To provide a consistent format for the agency reports, the OMB outlined 10 specific topic areas that needed to be included in both the CIO and IG executive summaries. These topic areas refer to the key elements of an effective computer-security program. In grading the agencies, the subcommittee assigned weighted point values to each of these topic areas, with a perfect score totaling 100 points.

As shown in the accompanying chart, "Analysis and Scoring Criteria," maximum point values were assigned to questions according to their importance to an agency's computer security program. Since most questions provide a range of possible responses, the number of points is proportional to the extent to which the element has been implemented. For example, agencies received zero (0) points for a response of "no," more points for "partially," and the full weighted value for "yes." Based on its analysis of the CIO's and IG's responses, the subcommittee tallied the scores for the 24 agencies.

Because the level of detail and/or responsiveness of reported data was uneven, the subcommittee also considered the results of computer security audits conducted by the General Accounting Office (GAO) and agency IGs from July 2000 through September 2001 examining security weaknesses in the following categories[1]:

- **Entity-wide security program planning and management** to provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls.

- **Access controls** to limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, or disclosure.

- **Application development and change controls** to prevent the unauthorized implementation of programs or modifications to existing programs.

- **Segregation of duties controls** to prevent one individual from controlling key aspects of computer-related operations that would allow him/her to conduct unauthorized actions or gain unauthorized access to assets or records.

[1] GAO routinely tracks the results of computer security audit work for the 24 major departments and agencies covered by the Chief Financial Officers Act. Results are shown in the accompanying chart entitled "Information Security Audit Results."

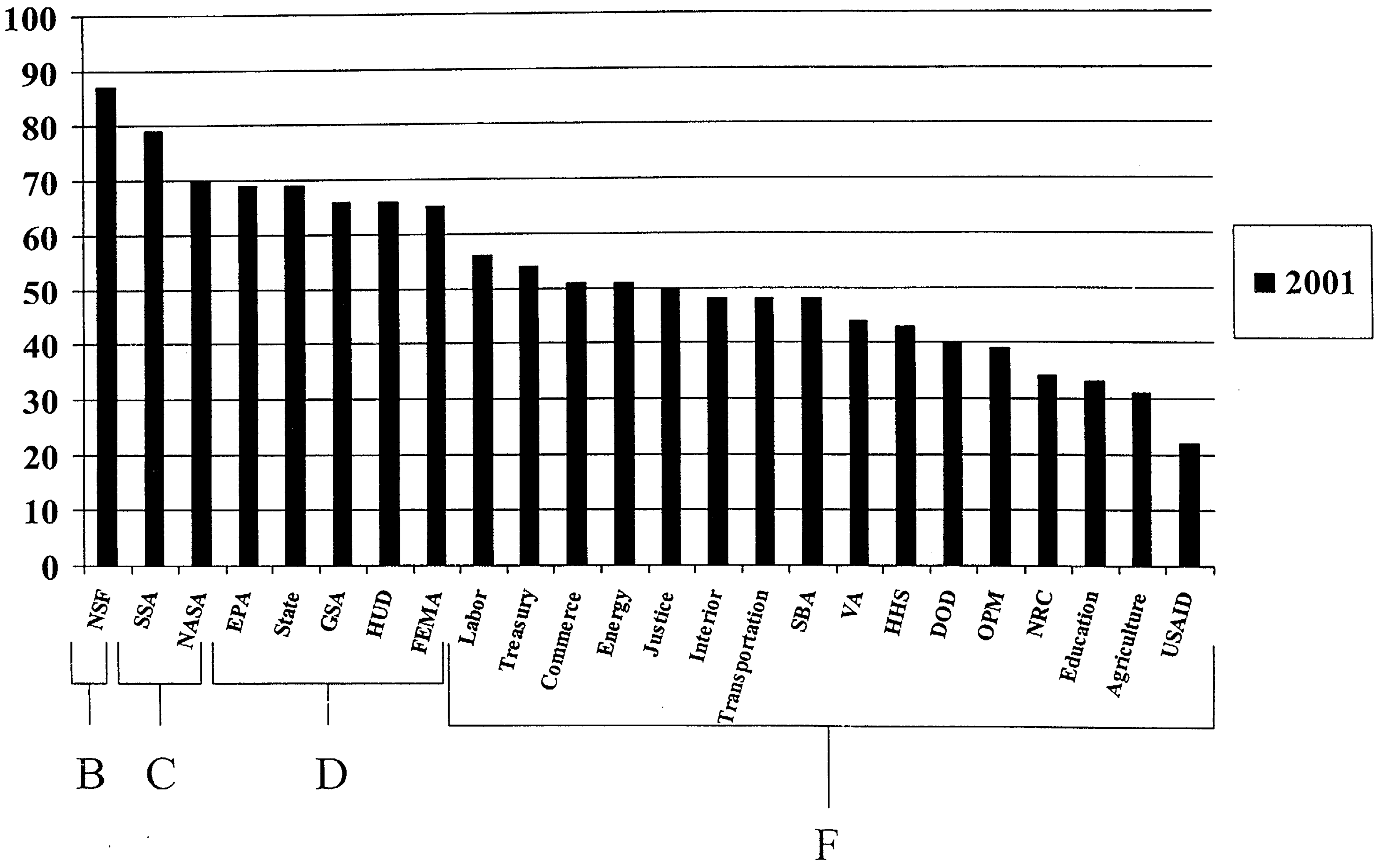
Analysis and Scoring Criteria

Part II – Report Grading Element	Weight (100 Points Max)
1. Does the report identify the agency's total FY02 security funding budget request broken down by operating unit and critical infrastructure protection costs? (OMB Memorandum 00-07, Memorandum 97-02, and Circular A-11)	**5 points max**
Agency provided total FY02 budget request broken down by operating unit and critical infrastructure protection costs.	(5)
Agency provided total, but not broken down by operating unit and critical infrastructure protection costs.	(3)
No specific security funding information was provided.	(0)
2. Has the agency implemented an up-to-date information security methodology for identifying and prioritizing its critical assets, including links with key external systems? (Sections 3535(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act)	**15 points max**
Methodology implemented, critical assets identified and ranked.	(15)
Methodology identified/developed but not fully implemented.	(10)
No.	(0)
3. Does the agency use measures of performance to ensure that program officials have: (1) assessed the risk to operations and assets under their control; (2) determined the level of security appropriate to protect such operations and assets; (3) maintained an up-to-date security plan that is practiced throughout the life cycle for each system supporting operations and assets under their control; and (4) tested and evaluated security controls? (Section 3534(a)(2) of the Security Act)	**10 points max**
Yes.	(10)
Performance measures have been established but not linked to any specific officials.	(8)
Performance measures are being developed, but were not implemented in 2001.	(8)
Performance measures not provided.	(0)
4. Does the agency use performance measures to ensure that the agency CIO adequately maintains an agency-wide security program, ensures the effective implementation of the program, and evaluates the performance of agency components? (Section 3534(a)(3)-(5) of the Security Act)	**10 points max**
Yes.	(10)
Performance measures have been established, but not specifically linked to the CIO.	(7)

Part I – Report Grading Element	Weight (100 Points Max)
Procedures for reporting incidents and for sharing information have been fully developed and implemented.	(15)
Development of procedures for reporting incidents and for sharing information is in process or complete, but implementation is not complete.	(10)
9. Has the agency integrated security into its capital planning and investment control process? (Section 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act)	**10 points max**
Yes, the agency has integrated security into its capital planning and investment control process and reported security costs on every FY02 capital asset plan submitted to OMB.	(10)
Partially. The agency has generally integrated security into its capital planning process but has not begun reporting security costs on every capital asset plan.	(8)
No, the agency has not integrated security into capital planning.	(0)
10. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities and other security programs? (Sections 3534 (a)(1)(B) and (b)(1) of the Security Act)	**5 points max**
The agency has no PDD-63 identified CIP systems.	(5)
Yes.	(5)
No.	(0)

Part II – Adjustment for Security Weaknesses Identified in IG & GAO Audit Reports Issued From July 2000 through September 2001	Weight (20 Points Max)
General Control Categories: Entitywide program planning and management	(±6)
Access Controls	(±5)
Application Development and Change Controls	(±2)
Segregation of Duties	(±1)
System Software	(±2)
Service Continuity	(±4)

Comparison of Computer Security Scores



Information Security Audit Results

DEPARTMENTS AND AGENCIES	QUESTION: DOES THE AGENCY HAVE SIGNIFICANT WEAKNESSES IN—					
	SECURITY PROGRAM: Plan, Implement, and Monitor Agency-wide Security Program to Manage Risk	**ACCESS CONTROL:** Limit or Detect Unauthorized Logical or Physical Access to Computer Resources	**CHANGE CONTROL:** Control Unauthorized Programs or Program Changes	**SEGREGATION OF DUTIES:** Limit Individual Responsibilities for Key Aspects of Computer-Related Operations	**SYSTEM SOFTWARE:** Limit & Monitor Access to Programs That Control Or Secure Computers and Applications	**SERVICE CONTINUITY:** Plan to Continue Critical Operations & Protect Data If Unexpected Events Occur
NSF National Science Foundation	Yes	Yes	Yes	No	No	No
SSA Social Security Administration	Yes	Yes	No	No	No	No
NASA National Aeronautics and Space Administration	Yes	Yes	?	?	Yes	No
EPA Environmental Protection Agency	Yes	Yes	?	Yes	Yes	No
State Department of State	Yes	Yes	No	No	No	Yes
FEMA Federal Emergency Management Agency	Yes	Yes	Yes	?	?	Yes
GSA General Services Administration	Yes	Yes	Yes	Yes	Yes	No
HUD Department of Housing and Urban Development	Yes	Yes	Yes	Yes	Yes	Yes
Agriculture Department of Agriculture	Yes	Yes	No	No	Yes	Yes
AID Agency for International Development	Yes	Yes	Yes	Yes	Yes	Yes
Commerce Department of Commerce	Yes	Yes	Yes	Yes	Yes	Yes
Defense Department of Defense	Yes	Yes	Yes	Yes	Yes	Yes
Education Department of Education	Yes	Yes	Yes	Yes	Yes	Yes
Energy Department of Energy	Yes	Yes	Yes	Yes	Yes	Yes
HHS Department of Health and Human Services	Yes	Yes	Yes	Yes	Yes	Yes
Interior Department of the Interior	Yes	Yes	Yes	Yes	Yes	Yes
Justice Department of Justice	Yes	Yes	Yes	Yes	Yes	Yes
Labor Department of Labor	Yes	Yes	Yes	Yes	Yes	Yes
NRC Nuclear Regulatory Commission	Yes	Yes	No	No	Yes	Yes
OPM Office of Personnel Management	Yes	Yes	Yes	No	No	Yes
SBA Small Business Administration	Yes	Yes	Yes	Yes	No	Yes
Transportation Department of Transportation	Yes	Yes	?	?	?	Yes
Treasury Department of the Treasury	Yes	Yes	Yes	Yes	Yes	Yes
VA Department of Veterans Affairs	Yes	Yes	Yes	Yes	Yes	Yes

Source: Information security audit reports issued by the General Accounting Office and agency Inspectors General from July 2000 through September 2001.

LEGEND:

Yes	=	Significant weaknesses have been identified.
No	=	No significant weaknesses have been identified.
?	=	Safeguards to protect computer operations and information from fraud, misuse, and disruption were either not reviewed or the scope of audit work was limited in such a way that significant agency operations were not covered.

Prepared for Subcommittee Chairman Stephen Horn
Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations