AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

COMPUTER SECURITY REPORT CARD

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

SEPTEMBER 11, 2000

Serial No. 106–260

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

74–495 DTP WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512–1800 Fax: (202) 512–2250
Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. MCINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
BOB BARR, Georgia
DAN MILLER, Florida
ASA HUTCHINSON, Arkansas
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin
HELEN CHENOWETH-HAGE, Idaho
DAVID VITTER, Louisiana

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee
JANICE D. SCHAKOWSKY, Illinois

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JAMES C. WILSON, *Chief Counsel*
ROBERT A. BRIGGS, *Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois
THOMAS M. DAVIS, Virginia
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin

JIM TURNER, Texas
PAUL E. KANJORSKI, Pennsylvania
MAJOR R. OWENS, New York
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
BEN RITT, *Professional Staff Member*
BRYAN SISK, *Clerk*
TREY HENDERSON, *Minority Counsel*

CONTENTS

	Page
Hearing held on September 11, 2000	1
Statement of:	
Dyer, John R., Chief Information Officer, Social Security Administration	142
Gilligan, John, Chief Information Officer, Department of Energy, cochair, security, privacy and critical infrastructure committee, Chief Information Officers Council	116
Hobbs, Ira L., Deputy Chief Information Officer, Department of Agriculture	184
Hugler, Edward, Deputy Assistant Secretary for Administration and Management, Department of Labor	179
Singleton, Solveig, director of information studies for the CATO Institute	201
Spotila, John T., Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget	27
Tanner, Mark A., Information Resources Manager, Federal Bureau of Investigation, Department of Justice	193
White, Daryl W., Chief Information Officer, Department of the Interior	155
Willemssen, Joel, Director, Accounting and Information Management Division, U.S. General Accounting Office, accompanied by Robert Dayce, Director for Computer Security Issues, General Accounting Office	95
Letters, statements, etc., submitted for the record by:	
Dyer, John R., Chief Information Officer, Social Security Administration, prepared statement of	145
Gilligan, John, Chief Information Officer, Department of Energy, cochair, security, privacy and critical infrastructure committee, Chief Information Officers Council, prepared statement of	120
Hobbs, Ira L., Deputy Chief Information Officer, Department of Agriculture, prepared statement of	186
Horn, Hon. Stephen, a Representative in Congress from the State of California:	
Letter dated July 27, 2000	46
Prepared statement of	4
Hugler, Edward, Deputy Assistant Secretary for Administration and Management, Department of Labor, prepared statement of	181
Singleton, Solveig, director of information studies for the CATO Institute, prepared statement of	204
Spotila, John T., Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget, prepared statement of	31
Tanner, Mark A., Information Resources Manager, Federal Bureau of Investigation, Department of Justice, prepared statement of	196
Turner, Hon. Jim, a Representative in Congress from the State of Texas, prepared statement of	25
White, Daryl W., Chief Information Officer, Department of the Interior, prepared statement of	157
Willemssen, Joel, Director, Accounting and Information Management Division, U.S. General Accounting Office, prepared statement of	97

COMPUTER SECURITY REPORT CARD

MONDAY, SEPTEMBER 11, 2000

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn and Turner.

Staff present: J. Russell George, staff director and chief counsel; Randy Kaplan, counsel; Ben Ritt, professional staff member; Bonnie Heald, director of communications; Bryan Sisk, clerk; Elizabeth Seong, staff assistant; George Fraser, intern; Michelle Ash and Trey Henderson, minority counsels; and Jean Gosa, minority assistant clerk.

Mr. HORN. The quorum being present, this hearing of the Subcommittee on Government Management, Information, and Technology will come to order.

We're here today to discuss one of the Federal Government's most important and ongoing challenges, the security of government computers. Computers and the Internet are revolutionizing the way we do business, conduct research and communicate with friends and associates. The benefits are enormous as vast amounts of information flow instantly from business to business and individual to individual, but widespread access to computers and the Internet also carries the significant risk that personal, financial or business information can fall into the hands of computer hackers or others with more malicious intent.

Similarly, as the Federal Government becomes increasingly dependent on computers and the Internet, the computer systems and the sensitivity of information they contain come under an increasing number of attacks. Unlike the year 2000 or Y2K computer challenge, this threat has no deadline. Rather it is a day-to-day challenge created by an increasingly sophisticated technology. In order to guarantee the integrity of the Federal programs and to protect the personal privacy of all Americans, government leaders must focus their attention on the security of their vital computer systems.

Today the subcommittee is releasing its first report card on the status of the computer security at executive branch departments and agencies. These grades are based on self-reported evaluation of agency information, in addition to the results of audits conducted

by the General Accounting Office and the various agency inspectors general. This is the first time such governmentwide information has ever been compiled.

As you can see, only two agencies have made progress toward protecting their computers against invasion. Although auditors found some significant weaknesses at the Social Security Administration and National Science Foundation, both agencies received Bs, the highest grade awarded. But the rest of the picture is very dismal. Overall the government earned an average grade of D minus. More than one-quarter of the 24 major Federal agencies received a failing F; the Department of Labor, charged with maintaining vital employment statistics, an F; the Department of the Interior, which manages the Nation's public lands, an F; the Department of Health and Human Services that holds personal information on every citizen who receives Medicare, another F; Agriculture and Justice, the Small Business Administration, the Office of Personnel Management, the personnel office for the entire executive branch of the Federal Governments, all Fs.

Six other vital agencies nearly failed. The Department of Defense, whose computers carry some of the Nation's most sensitive secrets, earned only a D plus for its computer security program; Veterans Affairs and Treasury, along with the Environmental Protection Agency, General Services Administration and National Aeronautics and Space Administration, more Ds.

Four other government agencies received grades of incomplete. These vital agencies oversee key elements of the Nation's infrastructure and emergency services. They are the Departments of Energy and Transportation, the Nuclear Regulatory Commission and the Federal Emergency Management Agency [FEMA]. These agencies could not receive a grade because there has been insufficient auditor resources and scrutiny to validate the agencies' self-evaluations.

Obviously there is a great deal of work ahead. Regardless of grade, each agency must recognize that the daily challenges to their computer systems will continue to grow in number and sophistication. They must take the necessary steps to mitigate those threats. There is no room for complacency, for the stakes are simply too high.

We have with us today witnesses representing six of the agencies that were graded. They will discuss their agency's progress and plans to develop acceptable computer security procedures.

Mr. John Gilligan from the Department of Energy will also testify on behalf of the Chief Information Officers Council. In addition, we have the Honorable John Spotila from the Office of Management and Budget, which is charged with overseeing the agency's computer security efforts; and Mr. Joel Willemssen from the General Accounting Office, which works for the legislative branch, headed the Comptroller General of the United States. And I want to thank Comptroller General Walker and the staff for their excellent help in regard to the grades and everything else. I take the responsibility for the grades, but they sat for hours with us on making sure that we've been fair.

We have the ability, the government has the ability, to protect the integrity of the vital computer systems. As I look back, this is

sort of where we were on Y2K in April 1996. There are a lot of Fs, a lot of Ds, but the executive branch came through on midnight January 1 where it counted, and I am confident that the executive branch will do the same thing this time.

We welcome all of our witnesses, and we look forward to their testimony.

I now yield to the ranking member for an opening statement, the gentleman from Texas Mr. Turner.

[The prepared statement of Hon. Stephen Horn follows:]

DAN BURTON, INDIANA,
CHAIRMAN
BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
THOMAS M. DAVIS III, VIRGINIA
DA[illegible] McINTOSH, INDIANA
M[illegible] SOUDER, INDIANA
JO[illegible] RBOROUGH, FLORIDA
STEVEN C. LATOURETTE, OHIO
MARSHALL "MARK" SANFORD, SOUTH CAROLINA
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
ASA HUTCHINSON, ARKANSAS
LEE TERRY, NEBRASKA
JUDY BIGGERT, ILLINOIS
GREG WALDEN, OREGON
DOUG OSE, CALIFORNIA
PAUL RYAN, WISCONSIN
JOHN T. DOOLITTLE, CALIFORNIA
HELEN CHENOWETH, IDAHO

ONE HUNDRED SIXTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051
TTY (202) 225–6852

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER
TOM LANTOS, CALIFORNIA
ROBERT E. WISE, Jr., WEST VIRGINIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
GARY A. CONDIT, CALIFORNIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
CHAKA FATTAH, PENNSYLVANIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
HAROLD E. FORD, Jr., TENNESSEE

BERNARD SANDERS, VERMONT,
INDEPENDENT

Subcommitteen Government Management, Information, and Technology

Opening Statement
Chairman Stephen Horn, R-CA
September 11, 2000

"Computer Security: How Vulnerable Are Federal Computers?"

A quorum being present, this hearing of the Subcommittee on Government Management, Information, and Technology will come to order.

We are here today to discuss one of the federal government's most important and ongoing challenges: the security of government computers. Computers and the Internet are revolutionizing the way we do business, conduct research, and communicate with friends and associates. The benefits are enormous, as vast amounts of information flow instantly from business to business, and individual to individual. But widespread access to computers and the Internet also carries the significant risk that personal, financial, or business information can fall into the hands of computer hackers, or others with more malicious intent.

Similarly, as the federal government becomes increasingly dependent on computers and the Internet, its computer systems and the sensitive information they contain have come under an increasing number of attacks. Unlike the Year 2000 computer challenge, this threat has no deadline. Rather it is a day-to-day challenge created by an increasingly sophisticated technology. In order to guarantee the integrity of Federal programs and to protect the personal privacy of all Americans, government leaders must focus their attention on the security of their vital computer systems.

Today, the subcommittee is releasing its first report card on the status of computer security at executive branch departments and agencies. These grades are based on self-reported agency information in addition to the results of audits conducted by the General Accounting Office and agency Inspectors General.

This is the first time such government-wide information has ever been compiled.

As you can see, only two (2) agencies have made progress toward protecting their computers against invasion. Although auditors found some significant weaknesses at the Social Security Administration and National Science Foundation, both agencies received "B's" -- the highest grade awarded.

The rest of the picture, however, is extremely dismal. Overall, the government earned an average grade of "D-." More than one-quarter of the 24 major federal agencies received a failing "F."

The Department of Labor, charged with maintaining vital employment statistics -- an "F." The Department of the Interior, which manages the Nation's public lands -- an "F." The Department of Health and Human Services that holds personal information on every citizen who receives Medicare -- another "F." Agriculture and Justice, the Small Business Administration and the Office of Personnel Management, the personnel office for the entire federal government -- all "F's."

Six other vital government agencies nearly failed. The Department of Defense, whose computers carry some of the Nation's most sensitive secrets, earned only a "D-plus" for its computer security program. Veterans Affairs, and Treasury, along with the Environmental Protection Agency, General Services Administration and National Aeronautics and Space Administration -- more "D's."

Four government agencies received grades of "Incomplete." These vital agencies oversee key elements of the Nation's infrastructure and emergency services -- the departments of Energy and Transportation, the Nuclear Regulatory Commission and the Federal Emergency Management Agency. These agencies could not receive a grade because there has been insufficient auditor scrutiny to validate their self-evaluations.

Obviously, there is a great deal of work ahead. And regardless of grade, each agency must recognize that the daily challenges to their computer systems will continue to grow in number and sophistication. They must take the necessary steps to mitigate those threats. There is no room for complacency, for the stakes are simply too high.

We have with us today witnesses representing six of the agencies that were graded. They will discuss their agency's progress and plans to develop acceptable computer security procedures.

Mr. John Gilligan from the Department of Energy will also testify on behalf of the Chief Information Officers Council. In addition, we have the Honorable John Spotila from the Office of Management and Budget, which is charged with overseeing the agencies' computer security efforts, and Mr. Joel Willemssen from the General Accounting Office to offer his perspective of the government's ability to protect the integrity of its vital computer systems.

We welcome all of our witnesses, and look forward to their testimony.

First

REPORT CARD

On

COMPUTER SECURITY

at

Federal Departments and Agencies

Overall Grade: D-

September 11, 2000

Computer Security

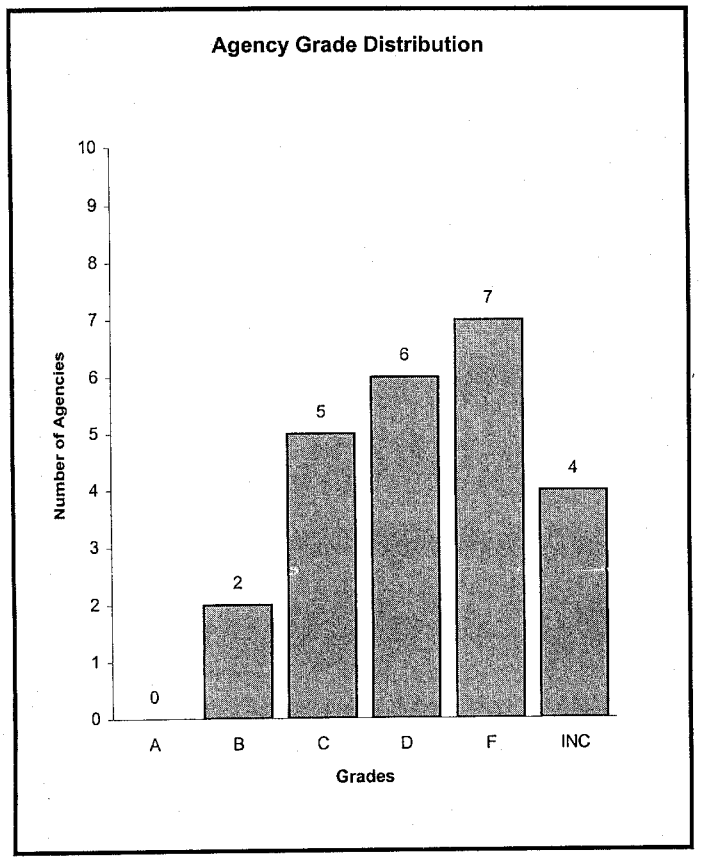
Departments and Agencies	Grade
Social Security Administration	B
National Science Foundation	B-
Education	C
State	C
Housing and Urban Development	C-
Commerce	C-
Agency for International Development	C-
Defense	D+
Veterans Affairs	D
Treasury	D
Environmental Protection Agency	D-
General Services Administration	D-
Nat. Aeronautics & Space Administration	D-

September 11, 2000

Department and Agencies	Grade
Office of Personnel Management	F
Health & Human Services	F
Agriculture	F
Small Business Administration	F
Justice	F
Labor	F
Interior	F
Energy	INC
Nuclear Regulatory Commission	INC
Transportation	INC
Federal Emergency Management Agency	INC
Government-wide Grade	D-

Prepared for Chairman Stephen Horn, Subcommittee on Government Management, Information, and Technology. Based on self-reported agency data and GAO and Inspectors General audit reports issued from July 1999 to August 2000.

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


Agency Grade Distribution
Number of Agencies
10
9
8
7
6
5
4
3
2
1
0
0
2
5
6
7
4
A
B
C
D
F
INC
Grades

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	**SYSTEM SOFTWARE:** Limit & Monitor Access to Programs That Control Or Secure Computers and Applications	**SEGREGATION OF DUTIES:** Limit Individual Responsibilities for Key Aspects of Computer-Related Operations	**SERVICE CONTINUITY:** Plan to Continue Critical Operations & Protect Data If Unexpected Events Occur
SSA Social Security Administration	Yes	Yes	No	Yes	No	Yes
DOE Department of Energy	Yes	Yes	?	?	?	?
NRC Nuclear Regulatory Commission	?	Yes	?	?	Yes	?
NSF National Science Foundation	Yes	Yes	Yes	?	Yes	Yes
Education Department of Education	Yes	Yes	Yes	Yes	No	Yes
State Department of State	Yes	Yes	Yes	Yes	Yes	Yes
HUD Department of Housing and Urban Development	Yes	Yes	Yes	Yes	Yes	Yes
DOT Department of Transportation	?	Yes	?	?	?	?
Commerce Department of Commerce	Yes	Yes	Yes	Yes	Yes	Yes
AID Agency for International Development	Yes	Yes	Yes	Yes	Yes	Yes
DOD Department of Defense	Yes	Yes	Yes	Yes	Yes	Yes
VA Department of Veterans Affairs	Yes	Yes	Yes	Yes	Yes	Yes
Treasury Department of the Treasury	Yes	Yes	Yes	Yes	Yes	Yes
EPA Environmental Protection Agency	Yes	Yes	Yes	Yes	?	Yes
GSA General Services Administration	Yes	Yes	Yes	Yes	Yes	Yes
FEMA Federal Emergency Management Agency	?	Yes	Yes	?	?	Yes
NASA National Aeronautics and Space Administration	Yes	Yes	Yes	?	Yes	Yes
OPM Office of Personnel Management	Yes	Yes	Yes	Yes	Yes	Yes
HHS Department of Health and Human Services	Yes	Yes	Yes	Yes	Yes	Yes
Agriculture Department of Agriculture	Yes	Yes	No	Yes	No	No
SBA Small Business Administration	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
Interior Department of the Interior	Yes	Yes	Yes	Yes	Yes	Yes

Source: Information security audit reports issued by the General Accounting Office and agency Inspectors General from July 1999 through August 2000.

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 Management, Information, and Technology
Subcommittee Home Page http://www.house.gov/reform/gmit

September 11, 2000

Computer Security Report Card

September 11, 2000

Departments and Agencies	Grade
Social Security Administration	B
National Science Foundation	B-
Education	C
State	C
Housing and Urban Development	C-
Commerce	C-
Agency for International Development	C-
Defense	D+
Veterans Affairs	D
Treasury	D
Environmental Protection Agency	D-
General Services Administration	D-
Nat. Aeronautics & Space Administration	D-

Department and Agencies	Grade
Office of Personnel Management	F
Health & Human Services	F
Agriculture	F
Small Business Administration	F
Justice	F
Labor	F
Interior	F
Energy	INC
Nucear Regulatory Commission	INC
Transportation	INC
Federal Emergency Management Agency	INC
Government-wide Grade	D-

Prepared for Chairman Stephen Horn, Subcommittee on Government Management, Information, and Technology. Based on self-reported agency data and GAO and Inspectors General audit reports issued from July 1999 to August 2000.

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

Survey Methodology and How Agency Grades Were Assigned

Computer security grades were primarily based on information agencies provided the Subcommittee on Government Management, Information, and Technology in a computer security questionnaire in August 2000.

The questionnaire, developed by the subcommittee, contained 29 questions, which were designed to provide a high-level view of an agency's overall computer security program and its implementation. The questions were based on current computer security policies or guidance issued by the Office of Management and Budget, the General Accounting Office, and the National Institute for Standards and Technology.

Questionnaires were sent to the 24 federal departments and agencies covered by the Chief Financial Officers Act (CFO Act) and an additional 30 component agencies or independent agencies. In some cases, a department incorporated its component agencies into a department-wide response. The agencies were asked to prepare responses based on their computer security policies, procedures, and activities as of August 1, 2000.

The subcommittee assigned weighted point values to each question, with a perfect score totaling 100 points. The subcommittee then considered the results of audits conducted by the U.S. General Accounting Office and agency Inspectors General during the past 12 months. Based on the audit results, the subcommittee adjusted an agency's score for a final grade.

The questions are organized into six major categories of computer general controls, which include the policies, procedures, and technical controls that apply to all or a large segment of an agency's information systems to help ensure their proper operation. The categories are as follows:

- **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. (9 questions; maximum of 29 points)

- **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. (10 questions; maximum of 26 points)

- **Application development and change controls** to prevent the unauthorized implementation of programs or modifications to existing programs. (2 questions; maximum of 12 points)

- **System software controls** to limit and monitor access to the basic operating system and sensitive files that control the computer hardware and secure the system's support applications. (3 questions; maximum of 12 points)

- **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 question; maximum of 3 points)

- **Service continuity controls** to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected. (4 questions; maximum of 18 points)

Maximum point values were assigned for questions according to their importance to an agency's computer security program. For yes/no questions, a "yes" answer received the maximum number of points and a "no" answer received zero (0) points. On questions that provided a range of responses (none/some/most/all), an increasing number of points were awarded, depending on the response. For example, agencies received zero (0) points for a response of "none," one point for "some," two points for "most," and three points for "all."

Some agencies provided narrative answers, rather than completing the form, or provided additional explanations. The subcommittee reviewed these responses and assigned appropriate point values. Rather than relying solely on agency-reported data, the subcommittee considered the results of information security audits reported by GAO and agency Inspectors General from July 1999 to August 2000.[1] As shown in the accompanying chart entitled, "Information Security Audit Results," significant weaknesses were identified for all agencies in some or all of six general control categories. These weaknesses indicate the extent to which agencies have actually implemented general controls.

Points were subtracted from the agency-based-data score for each control area where significant weaknesses were found. Conversely, if audit work did not identify significant weaknesses in a control area, the number of points corresponding to that category was added to the agency's score. The number of points assigned to each category approximately matches the point distribution of the questionnaire. These point values totaled 20 points and were distributed as follows:

- **Entity-wide security program planning and management** - 6 points (30 percent);
- **Access controls** - 5 points (25 percent);
- **Application development and change controls** - 2 points (10 percent);
- **System software controls** - 2 points (10 percent);
- **Segregation of duties controls** - 1 point (5 percent) and
- **Service continuity controls** - 4 points (20 percent).

Finally, some agencies have one or more control areas that have not been sufficiently audited. Because we do not know what significant weaknesses may or may not exist in these areas, a number of points equal to half the assigned point value was subtracted from an agency's score. An exception was made in the "separation of duties" category, where the full value of 1 was subtracted

[1] GAO routinely tracks the results of information security audit work for the 24 major departments and agencies covered by the Chief Financial Officers Act. Its report, Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies (GAO/AIMD-00-295, September 6, 2000) summarizes this work.

in order to prevent using fractions. These adjustments to the agency-reported data score produced the final numerical score. The scores and adjustments are shown on the accompanying work sheet.

The final numerical score was the basis for the agency letter grade. Letter grades for the 24 CFO Act 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

Scores that fell in the upper or lower portion of a grade range received a "plus" (+) or "minus" (-), respectively. Agencies with three or more general control categories that had not been audited were not assigned a letter grade. Their final numerical score is shown on the accompanying work sheet, but their grade in the report card is shown as "INC" for incomplete. The Government-wide grade was determined by averaging the final scores of all agencies that received a letter grade (agencies with "incomplete" were not included in calculating this average).

An additional 26 agencies and department component agencies, such as the Department of Justice's Federal Bureau of Investigation (FBI), also provided responses to the subcommittee. Because audit results are not routinely tracked for these agencies, their agency-reported scores could not be adjusted, and no letter grade was assigned. Some agencies, such as the FBI, are part of the composite department scores. These additional agency scores can be found on an accompanying work sheet.

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	**SYSTEM SOFTWARE:** Limit & Monitor Access to Programs That Control Or Secure Computers and Applications	**SEGREGATION OF DUTIES:** Limit Individual Responsibilities for Key Aspects of Computer-Related Operations	**SERVICE CONTINUITY:** Plan to Continue Critical Operations & Protect Data If Unexpected Events Occur
SSA Social Security Administration	Yes	Yes	No	Yes	No	Yes
DOE Department of Energy	Yes	Yes	?	?	?	?
NRC Nuclear Regulatory Commission	?	Yes	?	?	Yes	?
NSF National Science Foundation	Yes	Yes	Yes	?	Yes	Yes
Education Department of Education	Yes	Yes	Yes	Yes	No	Yes
State Department of State	Yes	Yes	Yes	Yes	Yes	Yes
HUD Department of Housing and Urban Development	Yes	Yes	Yes	Yes	Yes	Yes
DOT Department of Transportation	?	Yes	?	?	?	?
Commerce Department of Commerce	Yes	Yes	Yes	Yes	Yes	Yes
AID Agency for International Development	Yes	Yes	Yes	Yes	Yes	Yes
DOD Department of Defense	Yes	Yes	Yes	Yes	Yes	Yes
VA Department of Veterans Affairs	Yes	Yes	Yes	Yes	Yes	Yes
Treasury Department of the Treasury	Yes	Yes	Yes	Yes	Yes	Yes
EPA Environmental Protection Agency	Yes	Yes	Yes	Yes	?	Yes
GSA General Services Administration	Yes	Yes	Yes	Yes	Yes	Yes
FEMA Federal Emergency Management Agency	?	Yes	Yes	?	?	Yes
NASA National Aeronautics and Space Administration	Yes	Yes	Yes	?	Yes	Yes
OPM Office of Personnel Management	Yes	Yes	Yes	Yes	Yes	Yes
HHS Department of Health and Human Services	Yes	Yes	Yes	Yes	Yes	Yes
Agriculture Department of Agriculture	Yes	Yes	No	Yes	No	No
SBA Small Business Administration	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
Interior Department of the Interior	Yes	Yes	Yes	Yes	Yes	Yes

Source: Information security audit reports issued by the General Accounting Office and agency Inspectors General from July 1999 through August 2000.

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 Management, Information, and Technology
Subcommittee Home Page http://www.house.gov/reform/gmit

September 11, 2000

Computer Security Work Sheet
Federal Departments' and Agencies' Numerical Grades*

Agency	Score Based on Agency-Reported Data	Net Adjustment for Audit Findings	Score
Social Security Administration	100	-14	86
Department of Energy	98	-16	[82]
Nuclear Regulatory Commission	95	-13	[82]
National Science Foundation	99	-19	80
Department of Education	93	-18	75
Department of State	95	-20	75
Department of Housing and Urban Development	93	-20	73
Department of Transportation	86	-13	[73]
Department of Commerce	92	-20	72
Agency for International Development	92	-20	72
Department of Defense	89	-20	69
Department of Veterans Affairs	85	-20	65
Department of the Treasury	85	-20	65
Environmental Protection Agency	84	-20	64
General Services Administration	81	-20	61
Federal Emergency Management Agency	77	-16	[61]
National Aeronautics and Space Administration	79	-19	60
Office of Personnel Management	79	-20	59
Department of Health and Human Services	78	-20	58
Department of Agriculture	62	-6	56
Small Business Administration	75	-20	55
Department of Justice	72	-20	52
Department of Labor	58	-20	38
Department of the Interior	37	-20	17
Governmentwide Averages	**82.7**	**-18.1**	**62.6**

*See separate handout explaining how point values and adjustments were determined.

[Brackets] = Score not included in governmentwide average due to limited or non-existent audit work in three or more major control areas.

Computer Security Work Sheet
Numerical Grades* For Other Selected Agencies

Agency	Score Based on Agency-Reported Data
Drug Enforcement Agency (Justice)	97
Corporation for National Service	96
Federal Reserve Board	95
Federal Deposit Insurance Corporation	93
Immigration and Naturalization Service (Justice)	90
Federal Trade Commission	89
Federal Election Commission	89
Department of Commerce - NIST	89
US Patent and Trademark Office	88
Department of the Army	87
Internal Revenue Service (Treasury)	86
Federal Communications Commission	85
Customs Service (Treasury)	84
Bureau of Alcohol, Tobacco and Firearms (Treasury)	81
Railroad Retirement Board	78
Federal Bureau of Investigation (Justice)	78
International Trade Commission	78
Federal Maritime Commission	77
Pension Benefit Guaranty Corporation	76
Federal Energy Regulatory Commission	74
Merit Systems Protection Board	74
National Archives and Records Administration	73
Commodity Futures Trading Corporation	71
Overseas Private Investment Corporation	67
Peace Corps	59
National Labor Relations Board	45
Average for Agencies	**80.7**

*See separate handout explaining how point values and adjustments were determined.

September 11, 2000

SAMPLE -- Computer Security Questionnaire -- SAMPLE

August 2000

Pursuant to Rules X and XI of the Rules of the House of Representatives and the oversight responsibilities of the Subcommittee on Government Management, Information, and Technology, please complete the following questionnaire for your department or agency. The questionnaire contains high-level questions on your agency's computer security program, and is based on existing statutes and current computer security policy or guidance issued by the Office of Management and Budget, the General Accounting Office, and the National Institute for Standards and Technology.[1]

Please deliver the completed questionnaire (and an electronic copy if available) to the address below no later than **Friday, August 18, 2000**.

Subcommittee on Government Management,
Information, and Technology
ATTN: Ben Ritt
B-373 Rayburn House Office Building
Washington, D.C. 20515

If you have any questions or comments, please contact Ben Ritt of the Subcommittee staff at (202) 225-5147 or ben.ritt@mail.house.gov.

Part A - Agency Contacts

Department/Agency: _____

Chief Information Officer: _____

Phone: _____ e-mail: _____

Other Contact Point: _____

Title: _____

Phone: _____ e-mail: _____

[1] OMB Circular A-130, Revised February 8, 1996 (Transmittal Memorandum Number 3) Appendix III, Security of Federal Automated Information Systems; Federal Information System Controls Manual, U.S. General Accounting Office, GAO/AIMD-12.19.6, January 1999; and Generally Accepted Principles and Practices for Securing Information Technology Systems, Marianne Swanson and Barbara Guttman, National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-14, September 1996.

Part B - General Information

Please provide the following general information on your agency and its computer systems as of August 1, 2000:

Number of agency locations & sites (headquarters & field)	
Number of employees	
Number of contractor employees	
Number of data centers	
Number of general support systems As defined in Appendix III to OMB Circular No. A-130, "general support system" means an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.	
Number of major applications As defined in Appendix III to OMB Circular No. A-130, "major application" means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.	
Number of national security systems (Both those included above & other) Telecommunications and information systems that contain classified information or that support those critical national security missions.	

Please indicate the kinds of sensitive information processed by your systems/ applications.[2] *(Check all that apply)*

_____ Financial data (e.g., payments, contracts, payroll)

_____ Business sensitive or proprietary data

_____ Personal information on individuals other than employees (e.g., social security numbers, medical data, tax information)

_____ Mission-critical data that cannot be disrupted (e.g., air traffic control, military readiness)

_____ Others (please describe):

_____

_____

_____

[2] As defined in the Computer Security Act, sensitive information is *any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.*

Part C – Questions

1.	**Entity-wide Security Program** The following questions address 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.	
1.1	Have you implemented a process to perform and document independent risk assessments on a regular basis or whenever systems, facilities, or other conditions change?	3 Yes 0 No
1.2	Have you developed a security program plan that covers all major facilities, operations, and the topics prescribed by OMB Circular A-130? *If yes, please submit a copy of the current plan. If not, please explain why:* _____	2 Yes 0 No
1.3	Does the security program plan establish a central security office with adequate independence, authority, and expertise to implement and monitor the effectiveness of your security plan?	1 Yes 0 No
1.4	Have you developed security plans for each of your general support systems and major applications? Please indicate the number with plans implemented. **Number w/Plans Implemented** General Support Systems _____ Major Applications _____	0 None 1 Some 2 Most 3 All
1.5	Have you implemented a program for periodically testing your security controls to ensure that they are effective? Please indicate the number of systems tested: **Number Tested** **Since Aug. '99** **Since Aug. '98** General Support Systems _____ _____ Major Applications _____ _____	6 Yes 0 No
1.6	Has an incident response capability been implemented for your agency with characteristics suggested by NIST (e.g., virus identification software, links to other relevant groups)?	2 Yes 0 No
1.7	Have effective security-related personnel policies been implemented for hiring, transfer, termination, and performance? (Note: Include such things as requirements to contact references and perform background checks for prospective employees and termination and transfer procedures to conduct exit interviews; return property, keys, IDs; notify security management; and immediately escort terminated employees out.)	3 Yes 0 No

1.8	Do security management personnel have adequate training and expertise?	0 None 1 Some 2 Most 3 All
1.9	How many of your systems are accredited by a management official to formally accept the adequacy of a system's security? **Number w/Current Accreditation** General Support Systems _____ Major Applications _____	0 None 2 Some 4 Most 6 All
If the response to any question in the above section is "no," or "none," please explain.		
2.	**Access Control** The following questions address the implementation of basic controls that limit or detect access to computer resources (data, programs, equipment, and facilities) thereby protecting these resources against unauthorized modification, loss, and disclosure.	
2.1	Are information resources classified according to their criticality and sensitivity?	3 Yes 0 No
2.2	Have all significant threats to the physical well-being of sensitive and critical resources been identified and related risks determined?	3 Yes 0 No
2.3	Is physical access to sensitive facilities limited to individuals who routinely need access through the use of guards, identification badges, or entry devices such as key cards?	6 Yes 0 No
2.4	Have effective procedures been established for creating and periodically changing passwords?	1 Yes 0 No
2.5	Are password files encrypted?	1 Yes 0 No
2.6	Is security software used to restrict access?	2 Yes 0 No
2.7	Has communication software been implemented to provide logical controls over telecommunication access?	2 Yes 0 No
2.8	Has a firewall or set of firewalls been implemented that effectively monitors and, when appropriate, restricts unauthorized access to internal systems?	3 Yes 0 No
2.9	Has intrusion detection software been installed? Please indicate the numbers of intrusions detected: **1999** **2000 (to date)** Numbers of Intrusions Detected by Year _____ _____	2 Yes 0 No

2.10	Do security managers investigate security violations and report results to appropriate supervisory and management personnel?	3 Yes 0 No
If the response to any question in the above section is "no," please explain.		
3	**Application Development & Change Control** The following questions address application software development and change controls that prevent unauthorized programs or modifications to existing programs from being implemented.	
3.1	Are all changes to all programs controlled as they progress through testing to final approval?	6 Yes 0 No
3.2	Is access to all programs, including production code, source code, and extra program copies, protected by access control software and operating system features?	6 Yes 0 No
If the response to any question in the above section is "no," please explain.		
4.	**System software** The following questions address system software controls that limit and monitor access to the powerful programs and sensitive files that control the computer hardware and secure applications supported by the system.	
4.1	Have you limited access to critical operating system software to only the personnel needed to adequately maintain system operations?	6 Yes 0 No
4.2	Is operating system software configured to prevent circumvention of security software and application controls?	3 Yes 0 No
4.3	Have policies and techniques been implemented for using and monitoring the use of system utilities?	3 Yes 0 No
If the response to any question in the above section is "no," please explain.		
5.	**Segregation of Duties** The following questions address establishing policies, procedures, and an organizational structure such that one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records.	
5.1	Have incompatible duties been identified and policies been identified to segregate these duties? If "no," please explain.	3 Yes 0 No
6.	**Service Continuity** The following questions address implementing controls to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.	
6.1	Have critical and sensitive computerized operations and supporting resources for been identified and prioritized?	3 Yes 0 No

6.2	Have procedures to mitigate potential damage and interruption been implemented, such as periodically backing up files, programs, and critical documents; implementing fire suppression controls; providing for a back-up power supply; and arranging for remote backup facilities?	__6__ Yes __0__ No
6.3	Have comprehensive contingency plans been developed and documented?	__6__ Yes __0__ No
6.4	Have contingency plans been tested? If so, what was the date(s) of the most recent test(s): _____	__0__ None __1__ Some __2__ Most __3__ All
If the response to any question in the above section is "no" or "none," please explain.		

Please attach any documentation, comments, or additional explanations to the completed questionnaire.

Mr. TURNER. Thank you, Mr. Chairman.

As we all understand, our Federal agencies rely on computers and electronic data to perform functions that are essential to our national welfare and directly affect the lives of millions of Americans.

This technology greatly benefits Federal operations through the speed and accessibility it provides, but it also creates vulnerability to attack. Individuals, organizations and virtually anyone today with a computer and a modem has the potential to interrupt and to eavesdrop on government operations around the world. Many experts are predicting that future wars will be in the form of cyberattacks and fought out over a computer grid rather than a battlefield.

I want to commend the chairman for his interest and his work on this important issue. Computer security is without a doubt one of the most critical and difficult technical challenges facing our government. Like Y2K, this subcommittee has an important oversight role in holding our Federal agencies accountable for implementing computer security efforts, and while I commend the chairman's efforts to reduce the task to a simple report card grade, I also realize that improving computer security is a very complicated, timely and costly process.

Additionally, I do understand that the subjective format of our grading system could in some cases unfairly portray the significant efforts an agency has made to take corrective actions. I realize that some agency computer systems are critical to national security, while others may not be. I also realize that this Congress has an obligation to provide adequate funding to agencies so that they might meet the requirement that we have imposed on them.

While I want to commend the agencies that are moving forward, it is clear that the Federal Government has a long way to go before an effective, comprehensive Federal computer security system is in place. It is my hope that as a result of these hearings, we will be closer to achieving our mutual goal. We want to make sure that the Federal managers have the tools and the funds in place to be accountable for the protection of agency infrastructures.

Again, I thank the chairman for calling this hearing. I appreciate the good work that the committee and the staff has done, and I look forward to hearing from each of our witnesses.

Thank you, Mr. Chairman.

[The prepared statement of Hon. Jim Turner follows:]

STATEMENT OF THE HONORABLE JIM TURNER
GMIT HEARING: "COMPUTER SECURITY: HOW VULNERABLE ARE FEDERAL COMPUTERS?"
9/11/00

Thank you, Mr. Chairman. Federal agencies rely on computers and electronic data to perform functions that are essential to the national welfare and directly affect the lives of millions of Americans. This technology greatly benefits federal operations through the speed and accessibility it provides, but it also increases our vulnerability to attack. Individuals, organizations, or virtually anyone with a computer and modem now has the potential to interrupt or eavesdrop on government operations from anywhere in the world. Most experts are predicting that future wars will be in the form of cyberattacks and fought out over a computer grid rather than a battlefield.

Therefore, I want to commend the Chairman for his work on this issue. Computer security is without a doubt, one of the most critical technical challenges currently facing our government. Like Y2K, this Subcommittee has an important oversight role in holding our federal agencies accountable for implementing computer security measures.

And while I commend the Chairman's efforts, I also realize that this is a very complicated, timely, and costly process. Additionally, I do understand that the subjective format of the grading system could, in some cases, unfairly portray the significant efforts an agency has made to take corrective action. I realize that some agency computer systems are critical to national security while others are not. I also realize that Congress has an obligation to provide adequate funding to agencies so that they might meet the requirements we have imposed on them.

While I want to commend the agencies that have been moving forward, it is clear that the federal government has a long way to go before an effective, comprehensive federal computer security system is in place. It is my hope that as a result of these hearings we will closer to achieving this goal. We want to make sure that the federal managers have the tools and funds in place to be accountable for the protection of agency infrastructures. Again, I commend the Chairman for his work and welcome the witnesses here this morning.

Mr. HORN. Well, we thank you, and I agree with you. We need to be talking to the authorizers and the appropriators to make sure that what is needed will be there. So I imagine the next round we should have some improvement.

We will now start with the witnesses, and along the agenda the Honorable John Spotila is the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget, part of the President's Executive Office of the President, and he is speaking on behalf of OMB today.

So, Mr. Spotila.

STATEMENT OF JOHN T. SPOTILA, ADMINISTRATOR, OFFICE OF INFORMATION AND REGULATORY AFFAIRS, OFFICE OF MANAGEMENT AND BUDGET

Mr. SPOTILA. Good morning, Mr. Chairman and members of the committee. Thank you for inviting me here to discuss OMB's efforts in the vital area of computer security.

OMB policies build on a statutory framework requiring that Federal agencies adopt a set of risk-based management controls for all Federal computer systems. The agencies must periodically review their security controls to ensure continued effectiveness.

In an effort to identify strengths and weaknesses in agency security programs, OMB sought updated information from the agencies in June 1999 on their risk management processes. We are now focusing on the security posture of 43 high-impact government programs where good security is particularly important. These programs include Medicare, Medicaid, the air traffic control system, Social Security and Student Aid. In late May of this year, we asked the agencies to send us specific information regarding the management, operational and technical controls in place for each application or general support system sustaining these programs.

Our preliminary findings are illuminating. We have made significant progress, but can still do better. Agencies are working to integrate security into their capital planning and investment control processes. We have made this a high priority. Many agencies have completed a security review of their systems and have updated their security plans within the last 2 years. Many agencies develop and share their security plans with their partner organizations and other agencies. This promotes a comprehensive understanding of the interconnections prevalent in a shared risk environment.

Due to their extensive Y2K work, most agencies have tested their continuity of operations plans within the last 2 years. Most agencies have provided users and system administrators with IT security training within the last year. Most agencies update their virus detection and elimination software on an ongoing basis and have successfully implemented processes to confirm the testing and installation of software patches in a timely manner.

Nearly all agencies have documented incident handling procedures and have a formal incident response capability in place. More agencies need to install firewalls at external entry points to exclude unauthorized users and within their networks to ensure that authorized users do not exceed authorization.

Agencies can better protect the confidentiality of sensitive material through increased use of encryption for password files and per-

sonal information. Agencies should improve their intrusion detection capabilities and procedures. This should include increased involvement of agency privacy officers and legal counsel in reviewing the monitoring activities.

More agencies should ensure that agency managers specifically authorize the processing of each new or updated system before actual operations begin. More agencies should have independent review of their security plans.

We are working with the agencies on all of these areas. The President, his chief of staff and the Director of OMB have all taken a personal interest in enhancing security for our interconnected systems. This has gone a long way to establish senior management support at the agencies.

In February, OMB issued important guidance to the agencies on incorporating security and privacy requirements in each of their fiscal year 2002 information technology budget submissions.

A well-known computer security expert, Robert Courtney, once said, "Good security is the ultimate non-event." In that phrase, he summarized the difficulty of measuring effective security. We face a significant challenge. We must devise a method to assess security for the whole of government, its thousands of vastly diverse systems and millions of desktop computers. No other organization faces demands in this area that are as broad as those the government confronts.

Since last fall, OMB has worked with the CIO Council, NIST, GAO and the agencies to develop security performance measures against which agencies can assess their security programs. As you know, CIO Council and NIST representatives have met with your staff to discuss this effort. We have made great progress in a relatively short period of time, but, not surprisingly, there is more to be done. Even the private sector is struggling with this challenge.

Mr. Chairman, clearly you are focused on the need to assess agency security programs. While we appreciate your serious interest in security and your belief that grades will help the agencies improve their performance, we do have some concerns with this approach. We look forward to working closely with you to develop better ways of measuring progress in this area. We learned much from our collegial efforts with the committee, GAO and the agencies in developing good Y2K measurements. Ideally, we should work together to develop a similar workable set of measurements for assessing agency security programs.

Measuring agency security effectiveness is at least as complex as the Y2K measurement effort. We must assess programs and implementation at three different levels: the relatively uniform agency management or executive level; the expansive mix of individual programs where agency business operations take place; and at each of the thousands of government information systems that support actual agency program operations.

Cursory measurements can be misleading. A well-documented security program without the periodic evaluation of control effectiveness can give a false sense of security. A weak central organization can obscure highly effective component, program or system-level security. We must take a comprehensive approach to evaluating security if we are to generate meaningful results.

Our assessment approach begins with the premise that all agency programs and systems must include a continuing cycle of risk management, appropriate methods to evaluate and measure performance, and the ability to anticipate or quickly react to changes in the risk environment.

We are putting great emphasis on agency self-assessment. This fall all agencies will use a NIST-prepared questionnaire that focuses on overall agency programs as well as on specific management, operational and technical controls applied to each system or group of systems. Assessing the effectiveness of the program and the individual controls, not simply their existence, is vital to achieving and maintaining adequate security.

The NIST questionnaire will help agencies identify whether the program and controls are properly documented, implemented and continuously tested and reviewed. We can then determine a security level for an individual system, an agency or component, or an aggregated form, an entire agency.

Self-assessments improve security. They are less costly and can be performed more frequently than compliance inspections and audits. They can be performed by system users, thereby helping to promote buy-in and greater compliance. They promote openness and cooperation among all participants. They can also give us good information on a timely basis.

In seeking to measure security effectiveness, we should not equate it to our Y2K experience. While Y2K was a complex management challenge, it was a relatively straightforward technical one, and we could measure progress toward a known event. Security challenges, on the other hand, are unpredictable, ongoing, ever-changing and multidimensional. Security threats often arise from malicious parties who probe for vulnerabilities and risks. These threats can strike at the confidentiality of our information, the integrity of our systems and data, and our ability to ensure that information in systems will be ready for use when needed. These threats are ever-changing and our approach to security must be equally dynamic.

While a general progress report at an agency level can be valuable when used in the proper context, it is but a snapshot taken at a point in time. It may or may not even be a clear picture. Because a security program comprises physical, personnel, technical and other controls, accurately assessing a program is an extremely complex undertaking. In our view, the differences between the two call for different responses. Just as we must resist the simplicity of a one-size-fits-all security program for the wide variety of agency systems, we must also avoid a one-size-fits-all approach to measuring successes and shortfalls.

If we are to improve the government's approach to information security, we need to work together. We very much appreciate the committee's interest in this important area and look forward to continuing our close cooperation with you. We value our partnership with you and hope that this hearing will mark a further strengthening of our joint efforts on behalf of the American people. Thank you.

Mr. HORN. We thank you. And in courtesy to the executive branch, we let you go beyond the 5-minute rule.

Mr. SPOTILA. Thank you.

[The prepared statement of Mr. Spotila follows:]

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

STATEMENT OF THE HONORABLE JOHN T. SPOTILA
ADMINISTRATOR
OFFICE OF INFORMATION AND REGULATORY AFFAIRS
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES
September 11, 2000

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me here to discuss OMB's efforts in the area of computer security. We share your conviction that computer security is of vital concern. Government today relies increasingly on computer systems to support critical functions. Moreover, government and industry are now more interconnected than ever, operating in a shared risk environment, with our interdependence growing daily. The integrity and availability of our systems and, where appropriate, the confidentiality and privacy of information in those systems are today more important than ever.

Last July 26th, I appeared before this Committee and provided an overview on the Administration's efforts to enhance the security of Federal information systems and critical infrastructures. My testimony today will reiterate some of my remarks in July, while also adding further detail on what we are doing to measure more accurately agency security efforts.

As the Committee knows, we are currently in an important phase of this year's appropriations process. Congress is considering the funding of a number of key security initiatives that the President proposed in his FY 2001 budget. This budget recommended approximately $2.0 billion for agency critical infrastructure protection and computer security programs out of a total information technology budget of about $40 billion. This security total is a 15% increase over the FY 2000 enacted total of $1.8 billion. It includes funding to help detect computer attacks, coordinate research on security technology, hire and train more security experts, and create an internal expert review team for non-defense agencies. These initiatives are vitally important.

Mr. Chairman, you have expressed your personal support for increased funding in these areas and we appreciate your help. Regrettably, many of our requests for security funds still face

an uncertain future in the appropriations process. It has been particularly difficult to gain support for cross-cutting initiatives, despite their importance to our computer security efforts. We must be more open to innovative approaches in this area and look for opportunities for synergy and interagency cooperation.

Several important cross-cutting government initiatives are at risk in the appropriations process, but can still be implemented:

Department of Commerce

- $5 million at the National Institute for Standards and Technology (NIST) to establish an expert security review team to help agencies review their systems and programs, identify unacceptable risks, and assist in mitigating them. This program would operate in the context of NIST's statutory responsibilities under the Computer Security Act of 1987 and Clinger-Cohen Act of 1996 to issue security guidance to the agencies. We believe that this initiative is critical to NIST and OMB efforts to assess the security posture of agencies, individual programs, and to ensure that security programs and controls are effective and remain effective over time.

- $6.6 million for the Critical Infrastructure Assurance Office to continue its efforts to assist government agencies in identifying and prioritizing their critical assets and interdependencies and to continue cross-sectoral public-private partnerships.

- $50 million to create the Institute for Information Infrastructure Protection at NIST. The Institute would work collaboratively with industry and academia to fill research and development gaps for key security technologies. Industry often has no incentive to invest in long-term research and development without a clear market need. Research would be performed at private corporations, universities, and non-profit research institutes.

General Services Administration

- $5.4 million to maintain the Federal Computer Incident Response Capability (FedCIRC), the central government non-law enforcement focal point for responding to attacks, promoting incident reporting, and cross-agency sharing of data about common vulnerabilities. A portion of this funding will also continue government support of Carnegie-Mellon University's highly acclaimed Computer Emergency Response Team (CERT).

- $10 million for next generation intrusion detection. This funding would be used to establish the Federal Intrusion Detection Network (FIDNet) which would complement FedCIRC by standardizing ongoing agency computer intrusion detection activities, automating many of the cumbersome manual processes now employed, and providing a centralized expert analytic capability that does not exist at most agencies.

Department of Treasury

- $7 million at Treasury to complete the development of an interoperable government-wide infrastructure to permit authenticated electronic transactions and thus promote the electronic delivery of services to the public. In our traditional, paper-based world, government, industry, and the public rely on trusted and verifiable relationships, photo IDs, notarized signatures, and face-to-face contact to authenticate one another's identity prior to conducting business. We need a similar authentication capability in our new electronic world. This funding would translate paper-based relationships into similar trusted and verifiable electronic relationships.

Office of Personnel Management and the National Science Foundation

- $7 million at the Office of Personnel Management and $11.2 million at the National Science Foundation for Federal Cyber Services/Scholarships for Service. The Scholarship for Service effort will help develop the next generation of Federal information technology managers by awarding scholarships for the study of information assurance and computer security in exchange for Federal Service.

Administration Actions

In May 1998, the President issued Presidential Decision Directive 63, on "Critical Infrastructure Protection." This Directive provided a framework for government action. It pointed out that interconnected computer systems are necessary for the provision of essential national services. It recognized that a potential future attack against the United States might take the form of a cyberattack against our critical computer systems. It acknowledged that government and industry face essentially the same risk in this area and must work in close partnership to mitigate that risk.

The Directive also called on all Executive branch agencies to assess the vulnerabilities to their systems and the nation's critical infrastructures-- communications, energy, banking and finance, transportation, emergency services, and public health. It placed special emphasis on protection of the government's own critical assets and establishing the government as a model for information security. This is where OMB's primary role lies and where we have been concentrating our efforts.

To implement the Directive, the President appointed Richard Clarke of the National Security Council as the nation's first National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism. Later, the National Security Advisor announced the appointment of Jeffrey Hunker as Senior Director for Critical Infrastructure Protection, in the Office of Transnational Threats. Both have worked tirelessly to increase national awareness of the scope of the problems in this area, working closely with OMB to help formulate sound approaches to addressing these problems.

The Directive called for the development of a detailed National Plan for Information Systems protection, so that we could better defend against cyber disruptions. It also established a Critical Infrastructure Assurance Office (CIAO) at the Department of Commerce to coordinate government interaction with industry, develop the national plan, and assist federal agencies in identifying and prioritizing their own critical assets.

The Directive also established at the FBI the National Infrastructure Protection Center (NIPC) as a national focal point for gathering information on threats to the nation's critical infrastructures. NIPC's mission is largely to assess, respond, and investigate threats and attacks on our critical infrastructures. They support law enforcement efforts concerning cyber crimes and computer intrusion.

OMB's Role in Government Computer Security

We are very much committed to the protection of Federal computer systems. We recognize that security, or information assurance as it is sometimes called, consists of a number of separate components:

- Confidentiality -- assuring that information will be kept secret, with access limited to appropriate persons for authorized purposes;
- Integrity -- assuring that information is not accidentally or maliciously altered or destroyed, that systems are resistant to tampering, and that they operate as intended;
- Availability -- assuring that information and systems will be ready for use when needed;
- Reliability -- assuring that systems will perform consistently and at an acceptable level of quality; and
- Authentication -- assuring that users of systems and parties to transactions are verified and known so that the sender knows that data has been delivered and the recipient knows the sender's identity. With authentication comes nonrepudiation, since neither party can later deny having sent or received the data.

As I mentioned in my July testimony before this Committee, through the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), Congress has provided a sound legal framework for the Executive branch to address computer security needs. OMB policies build on this statutory framework.

OMB Circular A-130 sets forth government-wide polices for a wide variety of information and information resource management issues. The body of the Circular addresses agency management of information and information systems including capital planning and

investment control. Appendix I sets privacy policy. The soon to be issued Appendix II defines policy for information architectures and implementation of the Government Paperwork Elimination Act. Appendix III sets security policy.

Appendix III sets responsibilities for the confidentiality, availability, and integrity of all non-national security Federal information systems and the information processed by them. It also directs the Department of Commerce (through NIST) to issue appropriate security standards and guidance, provide security training guidelines, provide guidance for security planning, provide guidance and assistance to Federal agencies on appropriate security when interconnecting with other systems, evaluate new technologies, and apprise Federal agencies of their security vulnerabilities. NIST guidance is a mandatory companion to OMB's policies.

The Appendix also calls for NIST to coordinate agency incident response activities. However, due to funding difficulties and because NIST is not a service providing agency, that function (FEDCIRC), was transferred to GSA in 1998. We are working with GSA and the CIO Council to improve, within available resources, the operational effectiveness of FedCIRC. FedCIRC also coordinates the cross-government sharing of information regarding common vulnerabilities and works with the FBI, DOD, and others to assist agencies in responding to computer security incidents. In 1996, OMB designated FedCIRC as the primary avenue for agencies to fulfill their information sharing and incident handling responsibilities. FedCIRC has about 40 partner security organizations in government, industry, and academia and has an alert contact list comprising every Federal agency CIO and nearly 1,000 employees representing every Federal department and agency through which it can issue alerts.

Importantly, Appendix III also requires Federal agencies to adopt a minimum set of risk-based management controls for all Federal computer systems. Four controls are specifically described in the Appendix: assigning responsibility for security; security planning; management authorization; and, especially pertinent to today's hearing, periodic review of security controls. These controls are intentionally not technology dependent. Instead, they focus on the management controls agencies need to assure adequate security of the information technology now in the hands of millions of Federal users. Technical and operational controls to support these management controls are set forth in NIST guidance.

OMB policy also implements the Clinger-Cohen model by tying agency information resource management responsibilities, including security, to the capital planning and budgetary oversight process the agency engages in with OMB. When OMB reviews information technology investment plans generally, or when it examines specific information systems, it evaluates agency security planning and practices. Later in these remarks, I will discuss in more detail our recent guidance to the agencies on tying security and privacy to funding requests for information technology.

Are current policies effective?

In reviewing our recent efforts in the area of computer security, OMB has taken a close look at the effectiveness of our current policies. In general, we believe that our policies and

guidance for unclassified applications are adequate, although some updating and additional detail would be helpful. We plan to work with the CIO Council and others to provide additional detail in our upcoming revision to these policies. Indeed, reports from GAO, including its assessment of security practices of leading private sector organizations, show that OMB policies and NIST guidance are properly focused on a risk-based, cost effective approach and reflect the right balance between strong security and mission needs.

Again, OMB Circular A-130 establishes an overall framework for government information and information resource management. We must integrate security within this framework to ensure that it remains cost-effective, forms an integral part of agency business processes, enables rather than impedes agency missions, and operates effectively over time.

How can we ensure effective policies?

We recognize that security measures must function effectively in the real world of agency missions and business operations. To accomplish this, we focus on a number of key principles:

- We should consider widely diverse views and attempt to accommodate unique agency needs. Agency information management practices often affect the public, industry, and state and local governments. In considering new approaches to security we need an open and transparent process that encourages and makes good use of public comment.

- Although the views of the general security and national security community are essential in developing sound security policy, they are not the only ones we should consider. Agency CIOs, program officials, GAO, agency inspector generals, and others also have important perspectives and their views are essential in the policy development process.

- Ultimately, the responsibility for security of systems and programs should lie with each agency and with the specific program officials in each agency. Unless we develop policy that fits within that context, security will become an afterthought.

- Compliance improves when we build security into our systems and work processes in close coordination with the program officials that are closest to the affected operations.

- Funding and managing security apart from a program encourages program officials, system owners and users to ignore it. Separation sends a signal to them that security is not their job. If program officials and users do not take responsibility for security, then security officers and others must do so, often by employing resource intensive compliance inspections. This approach carries risk since the only time one knows the level of compliance is during or immediately following an inspection.

Good design and good planning are the keys to successful security. For good design, security must be compatible with and enable -- not unnecessarily impede -- system performance, business operations, and the mission. When security unnecessarily slows the system or hinders

the mission, users often work around it or ignore it completely. To work effectively, security must be part of the system architecture, built-in so that users will "buy-in."

Good planning requires that we fund security and privacy as part of the life-cycle costs for each system. To identify true system costs and adequately plan for future system or program operations, we must account for all of the resources necessary to operate the systems, including security. Indeed, attempting to fund security independent of the program or system within which it lives makes it far more difficult to build a business case for the security component. If it isn't tied to the mission, how can one demonstrate security's support of the mission?

Our approach provides maximum flexibility for agencies so that they can make appropriate, informed choices in applying necessary security controls that are consistent with their unique circumstances. It minimizes conflicts that could easily arise from any centralized approach to widely diverse agencies with a broad range of varied and shifting requirements.

How can we improve compliance?

As GAO, agency Inspectors General, our own program reviews, and industry and private security experts all agree, most security problems come not from a lack of policy, but rather from ineffective or incomplete implementation of existing policies and guidance and too infrequent reviews of control effectiveness. We are very much aware of this risk in the Federal context. In government, ineffective implementation can arise from inadequate resources, lack of management attention, and inadequate employee training. There is much more to be done before we reach full implementation of our existing security guidance.

We believe agencies must meet the following three goals to ensure successful security policy implementation:

- They must establish and maintain senior management support.
- They must achieve consensus and get user buy-in when initially setting policy so that the product will be better.
- They must tie security to their capital planning and investment control process and to their budgets.

To identify specific problems regarding implementation, we are collecting empirical data from the agencies. We began in June 1999 with a systematic review of agency risk management processes.

We are now focusing on the security posture of 43 high impact government programs that represent the major areas where the government connects to the public in areas often involving confidential information that needs appropriate security. We started here to focus on the most important areas to ensure good security. These include Medicare, Medicaid, the Air Traffic Control System, Social Security, and Student Aid. In late May we asked agencies to provide to

us specific information regarding the management, operational and technical controls in place for each application or general support system that sustains one of the programs for which they are responsible.

Our preliminary findings to date are illuminating. Overall, we see that while much work remains, especially for cross-cutting initiatives as discussed above, progress is being made. Agencies are working to improve their integration of security into their capital planning and investment control processes. We have also found the following:

- Many agencies have completed a security review of the systems and have updated their security plans within the last two years. Our current policy calls for updates as required, but no longer apart than every three years.

- A large number of agencies develop and share their security plans with their partner organizations and other agencies. This promotes a comprehensive understanding of interconnections that result in a shared risk environment.

- Due to the extensive Y2K work done by agencies, most of their continuity of operations plans have been tested within the last two years.

- The majority of agencies have provided users and system administrators with IT security training within the last year as required by existing policy.

- Most agencies update their virus detection and elimination software on an ongoing basis and have successfully implemented processes to confirm the testing and installation of software patches in a timely manner.

- Nearly all agencies have documented incident handling procedures and have a formal incident response capability in place.

We have also found that still more can be done:

- More agencies need to install firewalls at external entry points to exclude unauthorized users and within their networks to ensure authorized users do not exceed authorization.

- Increased use of encryption by agencies would help promote confidentiality of sensitive material, such as password files and personal information.

- Agencies need to improve their intrusion detection capabilities and procedures. This includes increased involvement of agency Privacy Officers and legal counsel in reviewing the monitoring activities.

- More agencies need to ensure that management authorizes system use consistent with security precautions.

- More agencies must have independent reviews of their security plans.

As we learn more, we will take appropriate steps to improve agency security further. In the interim, we are not waiting. Already we have acted on each of the three goals I mentioned above that seek to ensure successful security policy information. As I described in my July 26 testimony, the President and his Chief of Staff have taken a personal interest in enhancing security for our interconnected systems. This has gone a long way to establish senior management support at the agencies. Through our review of the 43 high impact programs, we have already seen evidence of increased user buy-in for the security needs of those programs. Finally, as I mentioned earlier, we have taken action to ensure that security is tied to agency capital planning and investment control.

In February, OMB Director Jacob Lew issued important guidance to the agencies on incorporating security and privacy requirements in each of their FY 2002 information technology budget submissions. We have been working with each of the agencies at the staff level to help them comply with this new guidance.

In the future, when requesting approval for information technology funds, agencies must demonstrate how they have built adequate security and privacy controls into the life-cycle maintenance and technical architectures of each of their systems. Without an adequate showing, the systems will not be funded. The criteria are set out below and apply to investments in the development of new or the continued operation of existing information systems. Agency investments must:

- Be tied to the agency's information architecture.

  Proposals should demonstrate that the security controls for components, applications, and systems are consistent with and an integral part of the information technology architecture of the agency.

- Be well-planned by:

  Demonstrating that the costs of security controls are understood and are explicitly incorporated in the life-cycle planning of the overall system in a manner consistent with OMB guidance for capital programming.

  Incorporating a security plan that discusses: 1) the rules of behavior for the system and the consequences for violating those rules; 2) personnel and technical controls for the system; 3) methods for identifying, appropriately limiting, and controlling interconnections with other systems and specific ways such limits will be monitored and managed; 4) procedures for the on-going training of individuals that are permitted access to the system; 5) procedures for the on-going monitoring of the effectiveness of security controls; 6) procedures for reporting and sharing with appropriate agency and government authorities indications of attempted and successful intrusions into agency systems; 7) provisions for the continuity of support in the event of system disruption or failure.

- Manage risks by:

  Demonstrating specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time.

  Demonstrating specific methods used to ensure that the security controls are commensurate with the risk and magnitude of harm that may result from the loss, misuse, or unauthorized access to or modification of the system itself or the information it manages.

  Identifying additional security controls that are necessary to minimize risks to and potential loss from those systems that promote or permit public access, other externally accessible systems, and those systems that are interconnected with systems over which program officials have little or no control.

- Protect privacy and confidentiality by:

  Deploying effective security controls and authentication tools consistent with the protection of privacy, such as public-key based digital signatures, for those systems that promote or permit public access.

  Ensuring that the handling of personal information is consistent with relevant government-wide and agency policies, such as privacy statements on the agency's web sites.

- Account for departures from NIST Guidance.

  For non-national security applications, to ensure the use of risk-based cost-effective security controls, describe each occasion when employing standards and guidance that are more stringent than those promulgated by the National Institute for Standards and Technology.

The Director's memo will promote funding security as an integral component of IT spending. Indeed, OMB supports funding well-conceived agency-specific budget requests for security initiatives and additionally OMB's budget preparation guidance to the agencies this year has added a requirement that they include, for each system, the percentage amount being spent for security. Over time, we believe this will give us better information on true security costs.

How can we measure effectiveness of agency security programs?

A well known computer security expert, Robert Courtney, once said, "Good security is the ultimate non-event." In that phrase he summarized the difficulty in measuring effective security. While security experts suggest a number of existing evaluation models and other

models are under development, we are faced with a significant challenge. We must devise a method to assess security for the whole of government, its thousands of vastly diverse systems, and millions of desktop computers. It is fair to say that no other organization faces demands in this area that are nearly as broad as those the government confronts.

Since last fall, OMB has worked with the CIO Council, NIST, GAO, and the agencies to develop security performance measures against which agencies can assess their security programs and take steps to mature them over time. As you know, CIO Council and NIST representatives have met with your staff to discuss this effort. We believe we have made great progress in a relatively short period of time. We should view this progress in context. In an effort to measure continuously its own security posture, a major financial institution, recognized as an industry leader in security, has recently spent three years developing an assessment framework that is quite comparable to ours.

We understand, Mr. Chairman, that you may plan to grade agency security programs as you did for agency Y2K efforts. We do look forward to working closely with you in this area, and as you know we worked with agencies to ensure a timely response to the questionnaire you sent out on their security position in the government. We certainly learned much from our collegial efforts with the Committee, GAO, and the agencies, in developing good Y2K measurements. We supported your effort in Y2K, where we had a single goal in a finite amount of time. Ideally, we should work together to develop a similar workable set of measurements for assessing agency security programs.

We have used what we learned in the Y2K measurement process as a head start in identifying objective ways to measure security performance. Measuring agency security effectiveness is at least as complex. We must measure programs and implementation at three different levels: 1) at the relatively uniform agency management or executive level; 2) at the expansive mix of individual programs where agency business operations take place; and 3) at each of the thousands of government information systems that support actual agency program operations. Cursory measurements can be misleading for a number of reasons. Indeed, a well documented security program without the periodic evaluation of control effectiveness can give a false sense of security while a weak central organization can obscure highly effective component, program, or system level security.

Our approach begins with the premise that all agency programs and systems must meet the minimum security requirements of OMB Circular A-130, Appendix III and associated NIST security guidance. These requirements include a continuing cycle of risk management as well as appropriate methods to evaluate and measure performance and react to changes in the risk environment.

Agencies will use a NIST prepared self-assessment questionnaire that focuses on the overall agency program as well as on specific management, operational, and technical controls applied to each system or group of systems. Assessing the effectiveness of the program and the individual controls, not simply their existence, is key to achieving and maintaining adequate security. The questionnaire will help agencies assess effectiveness by identifying whether the

program and the controls are properly documented, implemented, and continuously tested and reviewed. The questionnaire output will help determine the security level for an individual system, an agency component, or, in aggregated form, an entire agency.

I want to point out that first and foremost this approach is intended to foster agency self-assessment. While certainly OMB, the agency Inspectors General, GAO, and the Committee will continue to review agency security program effectiveness, we believe it is vitally important for agency officials to have tools to assess themselves. Self-assessments are less costly and can be performed more frequently than compliance inspections and audits. They can be performed by systems users helping to foster buy-in and greater compliance. Self-assessments promote openness and cooperation among participants versus an inspection's potential climate of distrust and adversarial relationships. Self-assessments can result in more effective security.

In seeking to measure security effectiveness, some have looked to the Y2K experience and have suggested that we measure agency progress in the same way. In applying lessons learned from the Y2K effort, however, we should recognize what it was – the Y2K effort was a project focused on fixing a finite problem which had a fixed, unmovable deadline. It was a vast management challenge, but it did not involve difficult technical challenges. Over the course of the effort, our understanding of how the problem might manifest itself grew, but the nature of the technical problem did not change. In this sense the problem was predictable and thus much simpler than other key IT challenges. Similarly, in the Y2K project there was no need to invest in research and development for the longer term. However, because of the changing technical threat, critical infrastructure protection and computer security need such investment. Thus the approach that worked for the Y2K problem may or may not be the most effective one for addressing other IT challenges. Rather, we must address each of them in their own context.

While a general progress report at an agency level can be valuable when used in the proper context, it is but a snapshot of a point in time and can be an unclear picture. Because a security program comprises physical, personnel, technical, and other controls, accurately assessing a program is an extremely complex undertaking. In our view the differences between the two call for different responses.

Just as we must resist the simplicity of a one-size-fits-all security program for the vast heterogeneity of agency systems, we must also avoid a one-size-fits-all approach to measuring successes and shortfalls.

Cross-Cutting Efforts

As I mentioned in my July testimony, we are engaged in a number of initiatives that seek to promote better security of government assets. We are working with the NSC, the CIO Council, NIST, GSA, and others on specific projects that include:

- Testing a systematic process of identifying, assessing, and sharing effective security practices. The CIO Council has developed a searchable database and website to facilitate this activity.

- Creating a formal process for coordinating the government-wide response to cyber incidents of national significance. This process includes the formation of a working group consisting of OMB, the FBI, Departments of Justice, Defense, and Commerce, the intelligence community, GSA, and the CIO Council, along with a senior level steering group consisting of senior officials from the above agencies, the NSC and OSTP.

- Using the FedCIRC organization to promote more timely agency installation of patches for known vulnerabilities. Many successful attacks against government and industry systems have been the result of old vulnerabilities for which vendor patches are readily available at no cost. Installing such patches is not, however, a trivial task; it requires considerable time and effort on the part of systems administrators who often are busy just keeping their systems up and running efficiently. We hope to provide some relief through this cross-cutting initiative if we can obtain necessary future funding.

- Reviewing security policies and practices of the national security community to see if they have applicability for those agencies that operate in an unclassified environment. Where appropriate, those policies and practices will be adapted for general agency use.

- Exploring with the CFO Council the viability of establishing a security benchmark or standard expectation for the security of agency financial systems. This effort may prove to be an effective pilot for establishing similar benchmarks for other discrete classes of information and systems. At the same time, we want to move carefully in this area to avoid the temptation to establish one-size-fits-all security requirements.

- Developing a government-wide Public Key Infrastructure (PKI) – a trusted digital signature infrastructure that will facilitate a broad range of services including tax filings, regulatory submissions, student and small business loans, benefit applications, grants, and many more. The PKI will be essential to agency implementation of the Paperwork Elimination Act. The Federal PKI Steering Committee, sponsored by the CIO Council, is working with government agencies and industry to field a comprehensive network-based infrastructure to support a federal PKI. Part of this task involves allowing digital signatures from different government agencies and different vendors to interoperate. A pilot, "Certificate Bridge Authority" successfully tested this interoperability in April and will be operational later this year. The PKI, through digital signature services and encryption, provides four of the basic security services I mentioned earlier -- confidentiality, integrity, authenticity, and non-repudiation. For all of these efforts, adequate future funding will be essential.

- Implementing a new methodology, Project Matrix, for prioritizing key nodes in complex information systems for investment in improved security. A major challenge in improving systems security is prioritizing where scarce resources should go first. Project Matrix was developed by the CIAO, and piloted on Department of Commerce systems such as those supporting the National Hurricane Center. OMB strongly supports a matrix like methodology for promoting an effective capital planning and investment control

process at the agencies, including security.

New Legislation

As I mentioned in my July testimony, we are very supportive of the Government Information Security Act of 2000, now part of the pending FY 2001 Defense Authorization Act. The Administration worked closely, in a non-partisan way, with the authors of this legislation. By taking elements directly from the Computer Security Act, the Paperwork Reduction Act, and Clinger-Cohen this legislation provides no new policy authority for OMB. It does, however, provide for some very important tools to evaluate agency security programs. It also establishes an annual reporting requirement that will assist OMB and Congress in monitoring progress in this area. The legislation would promote security as an essential management function and would do much to stimulate agencies into taking even greater steps to enhance the security of their systems.

It is clear that considerable resources are necessary to ensure the timely, ongoing, and comprehensive review of agency security programs. Acting under the umbrella of this legislation the agencies themselves can achieve the results we all seek. The Federal government has come a long way since the original Computer Security Act was passed in 1987. There have been significant technology and policy changes along the way. If it becomes law, the Government Information Security Act will update our statutory framework in a thoughtful and constructive manner. In addition, requiring agencies to give the CIO in each agency the authority to administer security functions, the act will promote the activities of CIOs and the CIO Council.

Conclusion

As I have said before, we appreciate your interest in this important area and look forward to continuing our close cooperation with the Committee. We value our partnership with you and hope that this hearing will mark a further strengthening of our joint efforts on behalf of the American people.

Thank you.

Mr. HORN. I will say for all the other witnesses after Mr. Willemssen, who speaks for the General Accounting Office of the legislative branch, that we would like you to summarize, and we will bring the gavel down every 5 minutes now or we're not going to be out of here, and we want to be out of here by roughly 11:45. I know a number of you have commitments.

What I would like to put in the record at this point for the hearing record—and tell me if there's anything else that ought to go into it, or some of these are classified, just to redact them, as the saying goes—Presidential Directive 63; OMB–A130, the Budget Director Mr. Lew's guidance, to agencies; the appendix 3 and associated NIST—what was once the Bureau of Standards and Security—guidance. And I would like these simply as appendices to your testimony, and if there's a problem, work it out with staff.

Mr. SPOTILA. That's fine.

[The information referred to follows:]

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

ADMINISTRATOR
OFFICE OF
INFORMATION AND
REGULATORY AFFAIRS

→ Ben Ritt GMIT
For insert as
part of Spotila's
presentation in
today's hearing,
September 11,
2000

July 27, 2000

The Honorable Steven Horn
Chairman, Subcommittee on Government
Management, Information and Technology
Committee on Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

We appreciate your offer to help gain support for funding cross-cutting Administration initiatives to promote greater computer security. These initiatives are critically important to our information assurance efforts. They will enhance secure information technology at a time of increasingly networked information systems. They will also play a vital role in our collective effort to see that electronic government and electronic commerce reach their full potential.

At the Committee's security hearing yesterday, we discussed the need for increased funding for cross-government security initiatives. Attached to this letter is a concise summary explaining this need in more detail; all of these amounts were requested in the President's Budget for FY 2001. I was pleased to hear that the General Accounting Office agreed yesterday that sufficient funding is vital if agencies are to protect against risks to their systems. As my testimony indicated, this is an area where it is important for us all to work together.

Thank you for offering to assist us in seeking funds for these important initiatives. If you have a need for any further information, please let us know.

Sincerely,

John T. Spotila

Enclosure

FY 2001 Cross-Cutting Security Initiatives

General Services Administration

- $5.4 million to maintain the Federal Incident Response Capability (FedCIRC) the central government non-law enforcement focal point for responding to attacks, promoting incident reporting, and cross-agency sharing of data about common vulnerabilities. A significant portion of this funding is also to continue government support of Carnegie-Mellon University's highly acclaimed Computer Emergency Response Team (CERT).

- $10 million for next generation intrusion detection. This funding would be used top establish the Federal Intrusion Detection Network (FIDNet) which would compliment FedCIRC by standardizing ongoing agency computer intrusion detection activities, automating many of the cumbersome manual processes now employed, and providing a centralized expert analytic capability that does not exist at most agencies.

Department of Commerce

- $5 million at the National Institute for Standards and Technology (NIST) to establish an expert security review team to help agencies review their systems and programs, identify unacceptable risks, and assist in mitigating them. This program is in the context of NIST's statutory responsibilities under the Computer Security Act of 1987 and Clinger-Cohen Act of 1996 to issue security guidance to the agencies.

- $6.6 million for the Critical Infrastructure Assurance Office to continue its efforts to assist government agencies in identifying and prioritizing their critical assets and interdependencies and to continue cross-sectoral public-private partnerships.

- $50 million to create the Institute for Information Infrastructure Protection at NIST. The Institute would work collaboratively with industry and academia to fill research and development gaps for key security technologies. Industry often has no incentive to invest in long-term research and development without a clear market need. Research would be performed at private corporations, universities, and non-profit research institutes.

Department of Treasury

- $7 million at Treasury to perfect the development of an interoperable government-wide infrastructure to permit authenticated electronic transactions and thus promote the electronic delivery of services to the public. In the paper-based world, government, industry, and the public rely on trusted and verifiable relationships, photo IDs, notarized signatures, and face-to-face contact to authenticate one another's identify prior to conducting business. This funding would translate those paper-based relationships into similar trusted and verifiable electronic relationships.

Office of Personnel Management and the National Science Foundation

- $7 million at the Office of Personnel Management and $11.2 million at the National Science Foundation for Federal Cyber Services/Scholarships for Service. The Scholarship for Service effort is intended to develop the next generation of Federal information technology managers by awarding scholarships for the study of information assurance and computer security in exchange for Federal Service.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

February 28, 2000

THE DIRECTOR

M-00-07

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

From: Jacob J. Lew
Director

Subject: Incorporating and Funding Security in Information Systems Investments

This memorandum reminds agencies of the Office of Management and Budget's (OMB) principles for incorporating and funding security as part of agency information technology systems and architectures and of the decision criteria that will be used to evaluate security for information systems investments. The principles and decision criteria are designed to highlight our existing policy and thereby foster improved compliance with existing security obligations; this memorandum does not constitute new security policy. OMB plans to use the principles as part of the FY 2002 budget process to determine whether an agency's information systems investments include adequate security plans.

Protecting the information and systems that the Federal government depends on is important as agencies increasingly rely on new technology. Agencies are working to preserve the integrity, reliability, availability, and confidentiality of important information while maintaining their information systems. The most effective way to protect information and systems is to incorporate security into the architecture of each. This approach ensures that security supports agency business operations, thus facilitating those operations, and that plans to fund and manage security are built into life-cycle budgets for information systems.

This memorandum is written pursuant to the Information Technology Management Reform Act (the Clinger-Cohen Act) which directs OMB to develop, as part of the budget process, a mechanism to analyze, track, and evaluate the risks and results of major capital investments made by an executive agency for information systems. Additionally, the Clinger-Cohen Act calls for OMB to issue clear and concise direction to ensure that the information security policies, processes, and practices of the agencies are adequate. These criteria will be incorporated into future revisions of OMB Circular A-130 ("Management of Federal Information Resources") and should be used in conjunction with previous OMB guidance on sound capital planning and investment control in OMB Memorandum 97-02, "Funding Information Systems Investments"; OMB Memorandum 97-16, "Information Technology Architectures"; and subsequent updates.

Security programs and controls implemented under this memorandum should be consistent with the Computer Security Act, the Paperwork Reduction Act, the Clinger-Cohen Act, and OMB Circular A-130. They should also be consistent with security guidance issued by the National Institute of Standards and Technology (NIST). Security controls for national security telecommunications and information systems should be implemented in accordance with appropriate national security directives.

Principles

The principles outlined below will support more effective agency implementation of both agency computer security and critical information infrastructure protection programs. In terms of Federal information systems, critical infrastructure protection starts with an effort to prioritize key systems (e.g., those that are most critical to agency operations). Once systems are prioritized, agencies apply OMB policies and, for non-national security applications, NIST guidance to achieve adequate security commensurate with the level of risk and magnitude of likely harm.

Agencies should develop security programs and incorporate security and privacy into information systems with attention to the following principles:

- Effective security is an essential element of all information systems.

- Effective privacy protections are essential to all information systems, especially those that contain substantial amounts of personally identifiable information. The use of new information technologies should sustain, and not erode, the privacy protections provided in all statutes and policies relating to the collection, use, and disclosure of personal information.

- The increase in efficiency and effectiveness that flows from the use of interconnected computers and networks has been accompanied by increased risks and potential magnitude of loss. The protection of Federal computer resources must be commensurate with the risk of harm resulting from any misuse or unauthorized access to such systems and the information flowing through them.

- Security risks and incidents must be managed in a way that complements and does not unnecessarily impede agency business operations. By understanding risks and implementing an appropriate level of cost-effective controls, agencies can reduce risk and potential loss significantly.

- A strategy to manage security is essential. Such a strategy should be based on an ongoing cycle of risk management and should be developed in coordination with and implemented by agency program officials. It should identify significant risks, clearly establish responsibility for reducing them, and ensure that risk management remains effective over time.

- Agency program officials must understand the risk to systems under their control and determine the acceptable level of risk, ensure that adequate security is maintained to support and assist the programs under their control, and ensure that security controls comport with program needs and appropriately accommodate operational necessities. In addition, program officials should work in conjunction with Chief Information Officers and other appropriate agency officials so that security measures support agency information architectures.

Policy

Security should be built into and funded as part of the system architecture. Agencies should make security's role explicit in information technology investments and capital programming. These actions are entirely consistent with and build upon the principles outlined in OMB Memorandum 97-02. Accordingly, investments in the development of new or the continued operation of existing information systems, both general support systems and major applications, proposed for funding in the President's budget must:

1. Be tied to the agency's information architecture. Proposals should demonstrate that the security controls for components, applications, and systems are consistent with and an integral part of the information technology architecture of the agency.

2. Be well-planned, by:

a) Demonstrating that the costs of security controls are understood and are explicitly incorporated in the life-cycle planning of the overall system in a manner consistent with OMB guidance for capital programming.

b) Incorporating a security plan that discusses:
- the rules of behavior for the system and the consequences for violating those rules;
- personnel and technical controls for the system;
- methods for identifying, appropriately limiting, and controlling interconnections with other systems and specific ways such limits will be monitored and managed;
- procedures for the on-going training of individuals that are permitted access to the system;
- procedures for the on-going monitoring of the effectiveness of security controls;
- procedures for reporting and sharing with appropriate agency and government authorities indications of attempted and successful intrusions into agency systems;
- provisions for the continuity of support in the event of system disruption or failure.

3. Manage risks, by:

   a) Demonstrating specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time.

   b) Demonstrating specific methods used to ensure that the security controls are commensurate with the risk and magnitude of harm that may result from the loss, misuse, or unauthorized access to or modification of the system itself or the information it manages.

   c) Identifying additional security controls that are necessary to minimize risks to and potential loss from those systems that promote or permit public access, other externally accessible systems, and those systems that are interconnected with systems over which program officials have little or no control.

4. Protect privacy and confidentiality, by:

   a) Deploying effective security controls and authentication tools consistent with the protection of privacy, such as public-key based digital signatures, for those systems that promote or permit public access.

   b) Ensuring that the handling of personal information is consistent with relevant government-wide and agency policies, such as privacy statements on the agency's web sites.

5. Account for departures from NIST Guidance. For non-national security applications, to ensure the use of risk-based cost-effective security controls, describe each occasion when employing standards and guidance that are more stringent than those promulgated by the National Institute for Standards and Technology.

In general, OMB will consider new or continued funding only for those system investments that satisfy these criteria and will consider funding information technology investments only upon demonstration that existing agency systems meet these criteria. Agencies should begin now to identify any existing systems that do not meet these decision criteria. They should then work with their OMB representatives to arrive at a reasonable process and timetable to bring such systems into compliance. Agencies should begin with externally accessible systems and those interconnected systems that are critical to agency operations. OMB staff are available to work with you if you or your staff have questions or need further assistance in meeting these requirements.

WHITE PAPER

The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63

May 22, 1998

WHITE PAPER
The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63
May 22, 1998

This White Paper explains key elements of the Clinton Administration's policy on critical infrastructure protection. It is intended for dissemination to all interested parties in both the private and public sectors. It will also be used in U.S. Government professional education institutions, such as the National Defense University and the National Foreign Affairs Training Center, for coursework and exercises on interagency practices and procedures. Wide dissemination of this unclassified White Paper is encouraged by all agencies of the U.S. Government.

I. A Growing Potential Vulnerability

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.

II. President's Intent

It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. President Clinton intends that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

III. A National Goal

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services;
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.

IV. A Public-Private Partnership to Reduce Vulnerability

Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sector. To succeed, this partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.

For each of the major sectors of our economy that are vulnerable to infrastructure attack, the Federal Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison Officials, after discussions and coordination with private sector entities of their infrastructure sector, will identify a private sector counterpart (Sector Coordinator) to represent their sector.

Together these two individuals and the departments and corporations they represent shall contribute to a sectoral National Infrastructure Assurance Plan by:

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing attempted major attacks;

- developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council, shall ensure their overall coordination and the integration of the various sectoral plans, with a particular focus on interdependencies.

V. Guidelines

In addressing this potential vulnerability and the means of eliminating it, President Clinton wants those involved to be mindful of the following general principles and concerns.

- We shall consult with, and seek input from, the Congress on approaches and programs to meet the objectives set forth in this directive.

- The protection of our critical infrastructures is necessarily a shared responsibility and partnership between owners, operators and the government. Furthermore, the Federal Government shall encourage international cooperation to help manage this increasingly global problem.

- Frequent assessments shall be made of our critical infrastructures' existing reliability, vulnerability and threat environment because, as technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive.

- The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people. In such cases, agencies shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, or providing information upon which choices can be made by the private sector. These incentives, along with other actions, shall be designed to help harness the latest technologies, bring about global solutions to international problems, and enable private sector owners and operators to achieve and maintain the maximum feasible security.

- The full authorities, capabilities and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness shall be available, as appropriate, to ensure that critical infrastructure protection is achieved and maintained.

- Care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably.

- The Federal Government shall, through its research, development and procurement, encourage the introduction of increasingly capable methods of infrastructure protection.

- The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the extent feasible, distribute the results of its endeavors.

- We must focus on preventative measures as well as threat and crisis management. To that end, private sector owners and operators should be encouraged to provide maximum feasible security for the infrastructures they control and to provide the government necessary information to assist them in that task. In order to engage the private sector fully, it is preferred that participation by owners and operators in a national infrastructure protection system be voluntary.

- Close cooperation and coordination with state and local governments and first responders is essential for a robust and flexible infrastructure protection program. All critical infrastructure protection plans and actions shall take into consideration the needs, activities and responsibilities of state and local governments and first responders.

VI. Structure and Organization

The Federal Government will be organized for the purposes of this endeavor around four components (elaborated in Annex A).

1. Lead Agencies for Sector Liaison: For each infrastructure sector that could be a target for significant cyber or physical attacks, there will be a single U.S. Government department which will serve as the lead agency for liaison. Each Lead Agency will designate one individual of Assistant Secretary rank or higher to be the Sector Liaison Official for that area and to cooperate with the private sector representatives (Sector Coordinators) in addressing problems related to critical infrastructure protection and, in particular, in recommending components of the National Infrastructure Assurance Plan. Together, the Lead Agency and the private sector counterparts will develop and implement a Vulnerability Awareness and Education Program for their sector.

2. Lead Agencies for Special Functions: There are, in addition, certain functions related to critical infrastructure protection that must be chiefly performed by the Federal Government (national defense, foreign affairs, intelligence, law enforcement). For each of those special functions, there shall be a Lead Agency which will be responsible for coordinating all of the activities of the United States Government in that area. Each lead agency will appoint a senior officer of Assistant Secretary rank or higher to serve as the Functional Coordinator for that function for the Federal Government.

3. Interagency Coordination: The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies, including the National Economic Council, will meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure

Coordination Group (CICG), chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The National Coordinator will be appointed by and report to the President through the Assistant to the President for National Security Affairs, who shall assure appropriate coordination with the Assistant to the President for Economic Affairs. Agency representatives to the CICG should be at a senior policy level (Assistant Secretary or higher). Where appropriate, the CICG will be assisted by extant policy structures, such as the Security Policy Board, Security Policy Forum and the National Security and Telecommunications and Information System Security Committee.

4. National Infrastructure Assurance Council: On the recommendation of the Lead Agencies, the National Economic Council and the National Coordinator, the President will appoint a panel of major infrastructure providers and state and local government officials to serve as the National Infrastructure Assurance Council. The President will appoint the Chairman. The National Coordinator will serve as the Council's Executive Director. The National Infrastructure Assurance Council will meet periodically to enhance the partnership of the public and private sectors in protecting our critical infrastructures and will provide reports to the President as appropriate. Senior Federal Government officials will participate in the meetings of the National Infrastructure Assurance Council as appropriate.

VII. Protecting Federal Government Critical Infrastructures

Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computer and physical systems. The Department of Justice shall establish legal guidelines for providing for such authorizations.

No later than 180 days from issuance of this directive, every department and agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems. The National Coordinator shall be responsible for coordinating analyses required by the departments and agencies of inter-governmental dependencies and the mitigation of those dependencies. The Critical Infrastructure Coordination Group (CICG) shall sponsor an expert review process for those plans. No later than two years from today, those plans shall have been implemented and shall be updated every two years. In meeting this schedule, the Federal Government shall present a model to the private sector on how best to protect critical infrastructure.

VIII. Tasks

Within 180 days, the Principals Committee should submit to the President a schedule for completion of a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks.

1. Vulnerability Analyses: For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector.

2. Remedial Plan: Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities and funding.

3. Warning: A national center to warn of significant infrastructure attacks will be established immediately (see Annex A). As soon thereafter as possible, we will put in place an enhanced system for detecting and analyzing such attacks, with maximum possible participation of the private sector.

4. Response: A system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage.

5. Reconstitution: For varying levels of successful infrastructure attacks, we shall have a system to reconstitute minimum required capabilities rapidly.

6. Education and Awareness: There shall be Vulnerability Awareness and Education Programs within both the government and the private sector to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cyber systems.

7. Research and Development: Federally-sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable.

8. Intelligence: The Intelligence Community shall develop and implement a plan for enhancing collection and analysis of the foreign threat to our national infrastructure, to include but not be limited to the foreign cyber/information warfare threat.

9. International Cooperation: There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations.

10. Legislative and Budgetary Requirements: There shall be an evaluation of the executive branch's legislative authorities and budgetary priorities regarding critical infrastructure, and ameliorative recommendations shall be made to the President as necessary. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB.

The CICG shall also review and schedule the taskings listed in Annex B.

IX. Implementation

In addition to the 180-day report, the National Coordinator, working with the National Economic Council, shall provide an annual report on the implementation of this directive to the President and the heads of departments and agencies, through the Assistant to the President for National Security Affairs. The report should include an updated threat assessment, a status report on achieving the milestones identified for the National Plan and additional policy, legislative and budgetary recommendations. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB. In addition, following the establishment of an initial operating capability in the year 2000, the National Coordinator shall conduct a zero-based review.

Annex A: Structure and Organization

Lead Agencies: Clear accountability within the U.S. Government must be designated for specific sectors and functions. The following assignments of responsibility will apply.

Lead Agencies for Sector Liaison:

Commerce	Information and communications
Treasury	Banking and finance
EPA	Water supply
Transportation	Aviation Highways (including trucking and intelligent transportation systems) Mass transit Pipelines Rail Waterborne commerce
Justice/FBI	Emergency law enforcement services
FEMA	Emergency fire service Continuity of government services
HHS	Public health services, including prevention, surveillance, laboratory services and personal health services
Energy	Electric power Oil and gas production and storage

Lead Agencies for Special Functions:

Justice/FBI	Law enforcement and internal security
CIA	Foreign intelligence
State	Foreign affairs
Defense	National defense

In addition, OSTP shall be responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council. Furthermore, while Commerce is the lead agency for information and communication, the Department of Defense will retain its Executive Agent responsibilities for the National

Communications System and support of the President's National Security Telecommunications Advisory Committee.

National Coordinator: The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism shall be responsible for coordinating the implementation of this directive. The National Coordinator will report to the President through the Assistant to the President for National Security Affairs. The National Coordinator will also participate as a full member of Deputies or Principals Committee meetings when they meet to consider infrastructure issues. Although the National Coordinator will not direct Departments and Agencies, he or she will ensure interagency coordination for policy development and implementation, and will review crisis activities concerning infrastructure events with significant foreign involvement. The National Coordinator will provide advice, in the context of the established annual budget process, regarding agency budgets for critical infrastructure protection. The National Coordinator will chair the Critical Infrastructure Coordination Group (CICG), reporting to the Deputies Committee (or, at the call of its chair, the Principals Committee). The Sector Liaison Officials and Special Function Coordinators shall attend the CICG's meetings. Departments and agencies shall each appoint to the CICG a senior official (Assistant Secretary level or higher) who will regularly attend its meetings. The National Security Advisor shall appoint a Senior Director for Infrastructure Protection on the NSC staff.

A National Plan Coordination (NPC) staff will be contributed on a non-reimbursable basis by the departments and agencies, consistent with law. The NPC staff will integrate the various sector plans into a National Infrastructure Assurance Plan and coordinate analyses of the U.S. Government's own dependencies on critical infrastructures. The NPC staff will also help coordinate a national education and awareness program, and legislative and public affairs.

The Defense Department shall continue to serve as Executive Agent for the Commission Transition Office, which will form the basis of the NPC, during the remainder of FY98. Beginning in FY99, the NPC shall be an office of the Commerce Department. The Office of Personnel Management shall provide the necessary assistance in facilitating the NPC's operations. The NPC will terminate at the end of FY01, unless extended by Presidential directive.

Warning and Information Centers

As part of a national warning and information sharing system, the President immediately authorizes the FBI to expand its current organization to a full scale National Infrastructure Protection Center (NIPC). This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. During the initial period of six to twelve months, the President also directs the National Coordinator and the Sector Liaison Officials, working together with the Sector Coordinators, the Special Function Coordinators and representatives from the National Economic Council, as appropriate, to consult with owners and operators of the critical infrastructures to encourage the creation of a private sector sharing and analysis center, as described below.

National Infrastructure Protection Center (NIPC): The NIPC will include FBI, USSS, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community and Lead Agencies. It will be linked electronically to the rest of the Federal Government, including other warning and operations centers, as well as any private sector sharing and analysis centers. Its mission will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response.

All executive departments and agencies shall cooperate with the NIPC and provide such assistance, information and advice that the NIPC may request, to the extent permitted by law. All executive departments shall also share with the NIPC information about threats and warning of attacks and about actual attacks on critical government and private sector infrastructures, to the extent permitted by law. The NIPC will include elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach and development and application of technical tools. In addition, it will establish its own relations directly with others in the private sector and with any information sharing and analysis entity that the private sector may create, such as the Information Sharing and Analysis Center described below.

The NIPC, in conjunction with the information originating agency, will sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant federal, state and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity. Before disseminating national security or other information that originated from the intelligence community, the NIPC will coordinate fully with the intelligence community through existing procedures. Whether as sanitized or unsanitized reports, the NIPC will issue attack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators. These warnings may also include guidance regarding additional protection measures to be taken by owners and operators. Except in extreme emergencies, the NIPC shall coordinate with the National Coordinator before issuing public warnings of imminent attacks by international terrorists, foreign states or other malevolent foreign powers.

The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts. Depending on the nature and level of a foreign threat/attack, protocols established between special function agencies (DOJ/DOD/CIA), and the ultimate decision of the President, the NIPC may be placed in a direct support role to either DOD or the Intelligence Community.

Information Sharing and Analysis Center (ISAC): The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government. Within 180 days of this directive, the

National Coordinator, with the assistance of the CICG including the National Economic Council, shall identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government.

As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive interchanges with the private and non-federal sectors. Under such a model, the ISAC would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility and acceptability.

Annex B: Additional Taskings

Studies

The National Coordinator shall commission studies on the following subjects:

- Liability issues arising from participation by private sector companies in the information sharing process.

- Existing legal impediments to information sharing, with an eye to proposals to remove these impediments, including through the drafting of model codes in cooperation with the American Legal Institute.

- The necessity of document and information classification and the impact of such classification on useful dissemination, as well as the methods and information systems by which threat and vulnerability information can be shared securely while avoiding disclosure or unacceptable risk of disclosure to those who will misuse it.

- The improved protection, including secure dissemination and information handling systems, of industry trade secrets and other confidential business data, law enforcement information and evidentiary material, classified national security information, unclassified material disclosing vulnerabilities of privately owned infrastructures and apparently innocuous information that, in the aggregate, it is unwise to disclose.

- The implications of sharing information with foreign entities where such sharing is deemed necessary to the security of United States infrastructures.

- The potential benefit to security standards of mandating, subsidizing, or otherwise assisting in the provision of insurance for selected critical infrastructure providers and requiring insurance tie-ins for foreign critical infrastructure providers hoping to do business with the United States.

Public Outreach

In order to foster a climate of enhanced public sensitivity to the problem of infrastructure protection, the following actions shall be taken:

- The White House, under the oversight of the National Coordinator, together with the relevant Cabinet agencies shall consider a series of conferences: (1) that will bring together national leaders in the public and private sectors to propose programs to increase the commitment to information security; (2) that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field; (3) on the issues around computer ethics as these relate to the K through 12 and general university populations.

- The National Academy of Sciences and the National Academy of Engineering shall consider a round table bringing together federal, state and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security.

- The intelligence community and law enforcement shall expand existing programs for briefing infrastructure owners and operators and senior government officials.

- The National Coordinator shall (1) establish a program for infrastructure assurance simulations involving senior public and private officials, the reports of which might be distributed as part of an awareness campaign; and (2) in coordination with the private sector, launch a continuing national awareness campaign, emphasizing improving infrastructure security.

Internal Federal Government Actions

In order for the Federal Government to improve its infrastructure security, these immediate steps shall be taken:

- The Department of Commerce, the General Services Administration, and the Department of Defense shall assist federal agencies in the implementation of best practices for information assurance within their individual agencies.

- The National Coordinator shall coordinate a review of existing federal, state and local bodies charged with information assurance tasks, and provide recommendations on how these institutions can cooperate most effectively.

- All federal agencies shall make clear designations regarding who may authorize access to their computer systems.

- The Intelligence Community shall elevate and formalize the priority for enhanced collection and analysis of information on the foreign cyber/information warfare threat to our critical infrastructure.

- The Federal Bureau of Investigation, the Secret Service and other appropriate agencies shall: (1) vigorously recruit undergraduate and graduate students with the relevant computer-related technical skills for full-time employment as well as for part-time work with regional computer crime squads; and (2) facilitate the hiring and retention of qualified personnel for technical analysis and investigation involving cyber attacks.

- The Department of Transportation, in consultation with the Department of Defense, shall undertake a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System. This evaluation shall include sponsoring an independent, integrated assessment of risks to civilian users of GPS-based

systems, with a view to basing decisions on the ultimate architecture of the modernized NAS on these evaluations.

- The Federal Aviation Administration shall develop and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions and attacks.

- GSA shall identify large procurements (such as the new Federal Telecommunications System, FTS 2000) related to infrastructure assurance, study whether the procurement process reflects the importance of infrastructure protection and propose, if necessary, revisions to the overall procurement process to do so.

- OMB shall direct federal agencies to include assigned infrastructure assurance functions within their Government Performance and Results Act strategic planning and performance measurement framework.

- The NSA, in accordance with its National Manager responsibilities in NSD-42, shall provide assessments encompassing examinations of U.S. Government systems to interception and exploitation; disseminate threat and vulnerability information; establish standards; conduct research and development; and conduct issue security product evaluations.

Assisting the Private Sector

In order to assist the private sector in achieving and maintaining infrastructure security:

- The National Coordinator and the National Infrastructure Assurance Council shall propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems.

- The Department of Commerce and the Department of Defense shall work together, in coordination with the private sector, to offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards.

- The Department of Justice and Department of the Treasury shall sponsor a comprehensive study compiling demographics of computer crime, comparing state approaches to computer crime and developing ways of deterring and responding to computer crime by juveniles.

federal register

Tuesday
February 20, 1996

Part III

Office of Management and Budget

Management of Federal Information Resources; Notice

OFFICE OF MANAGEMENT AND BUDGET

Management of Federal Information Resources

AGENCY: Office of Management and Budget, Executive Office of the President.

ACTION: Revision of OMB Circular No. A–130, Transmittal No. 3, Appendix III, "Security of Federal Automated Information Resources."

SUMMARY: The Office of Management and Budget (OMB) is revising Appendix III, "Security of Federal Information Systems," of Circular No. A–130, "Management of Federal Automated Information Resources." This is the third stage of planned revisions to Circular A–130. Enactment of the Information Technology Management Reform Act of 1996 (Division E of the National Defense Authorization Act for Fiscal Year 1996) will require OMB to issue additional guidance on capital planning, investment control, and the management of information technology. A plan for those revisions will be announced in the Spring.

Transmittal 1 to Circular A–130, effective June 25, 1993, and published on July 2, 1993 (58 FR 36068) addressed the Information Management Policy section of the Circular (Section 8a), as well as Appendix I, "Federal Agency Responsibilities for Maintaining Records About Individuals." That issuance dealt primarily with how the Federal government manages its information holdings, particularly information exchange with the public.

Transmittal 2 to Circular A–130, effective July 15, 1994, and published on July 25, 1994 (59 FR 37906) addressed agency management practices for information systems and information technology (Section 8b). That issuance was intended to (1) promote agency investments in information technology that improve service delivery to the public, reduce burden on the public, and lower the cost of Federal programs administration, and (2) encourage agencies to use information technology as a strategic resource to improve Federal work processes and organization.

This Transmittal 3 is intended to guide agencies in securing government information resources as they increasingly rely on an open and interconnected National Information Infrastructure. It stresses management controls, such as individual responsibility, awareness and training, and accountability, and explains how they can be supported by technical controls. Among other things, it requires agencies to assure that risk-based rules of behavior are established, that employees are trained in them, and that the rules are enforced. The revision also integrates security into program and mission goals, reduces the centralized reporting of security plans, emphasizes the management of risk rather than its measurement, and revises government-wide security responsibilities to be consistent with the Computer Security Act and the Paperwork Reduction Act of 1995.

This transmittal also makes minor technical revisions to Section 9 ("Assignment of Responsibilities") and Section 10 ("Oversight") to reflect the Paperwork Reduction Act of 1995 (Pub. L. 104–13). One substantive change has been made to Appendix I in Section 3.a. changing the annual requirement to review recordkeeping practices, training, violations, and notices to a biennial review, in accordance with other regular agency reviews not required by statute. Several minor changes have been made, none of which are intended to be substantive. In Section 2.c., a portion of the definition of "nonfederal agency" which has been inadvertently omitted has been added to reflect the current practice in state-federal matching programs. In Section 3.a., extraneous and confusing language referring to source or matching agencies was removed because the provision applies to any agency that participates in a matching program. The example's in 4.c.(1) were updated for clarity. Other editorial and organizational changes were made throughout the appendix.

Appendix IV has been changed to include material from OMB Memorandum M–95–22, "Implementing the Information Dissemination Provisions of the Paperwork Reduction Act of 1995" (September 29, 1995), and to delete some outdated or otherwise already implemented guidance from the discussion of Sections 9 and 10.

ELECTRONIC AVAILABILITY: This document is available on the OMB Home page of Welcome to the White House World Wide Web site (http://www.whitehouse.gov) as http://www1.whitehouse.gov/White-House/EOP/OMB/html/omb-a130.html. This document is also available on the Internet via anonymous File Transfer Protocol (FTP) from the National Institute of Standards and Technology (NIST) Computer Security Resource Clearinghouse at csrc.ncsl.nist.gov as /pub/secplcy/a130.txt (do not use any capital letters in the file name) or via the World Wide Web from http://csrc.ncsl.nist.gov/secplcy as a130.txt. Appendix III, "Security of Federal Automated Information Resources" can be separately obtained as a130app3.txt. The clearinghouse can also be reached using dial-in access at 301–948–5717. For those who do not have file transfer capability, the document can be retrieved via mail query by sending an electronic mail message to docserver@csrc.ncsl.nist.gov with no subject and with send a130.txt (or a130app3.txt for only the security appendix) as the first line of the body of the message. Paper copies may also be obtained by writing to the Publications Office, Office of Management and Budget, Room 2200 NEOB, Washington, D.C. 20503 or by telephone at (202) 395–7332.

FOR FURTHER INFORMATION CONTACT: Information Policy and Technology Branch, Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10236, New Executive Office Building, Washington, D.C. 20503. Telephone: (202) 395–3785.

SUPPLEMENTARY INFORMATION:

Since December 30, 1985, Appendix III of Office of Management and Budget (OMB) Circular No. A–130, "Security of Federal Automated Information Systems," has defined a minimum set of controls for the security of Federal automated information systems (50 FR 52730). That Appendix, and its predecessor, Transmittal Memorandum No. 1 to OMB Circular No. A–71, (July 27, 1978), defined controls that were considered effective in a centralized processing environment which ran primarily custom-developed application software.

Today's computing environment is significantly different. It is characterized by open, widely distributed processing systems which frequently operate with commercial off-the-shelf software. While effective use of information technology often reduces risks to the Federal program being administered (e.g., risks from fraud or errors), the risk to and vulnerability of Federal information resources has increased. Greater risks result from increasing quantities of valuable information being committed to Federal systems, and from agencies being critically dependent on those systems to perform their missions. Greater vulnerabilities exist because virtually every Federal employee has access to Federal systems, and because these systems now interconnect with outside systems.

In part because of these trends, Congress enacted the Computer Security Act of 1987 (Pub. L. 100–235). That Act requires agencies to improve the

security of Federal computer systems, plan for the security of sensitive systems, and provide mandatory awareness and training in security for all individuals with access to computer systems.

To assist agencies in implementing the Computer Security Act, OMB issued Bulletin No. 88–16, "Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information" (July 6, 1988), and OMB Bulletin No. 90–08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information" (July 9, 1990). This revision of Appendix III to OMB Circular A–130 incorporates and updates the policies set out in those Bulletins and supersedes them.

The report of the National Performance Review, "Creating a Government that Works Better & Costs Less: Reengineering through Information Technology" (September 1993), recommended that Circular A–130 be revised to: (1) Require an information security plan to be part of each agency's strategic information technology (IT) plan; (2) require that if computer security does not meet established thresholds, it be identified as a material weakness in the Federal Managers' Financial Integrity Act report; (3) require awareness and training of employees and contractors; (4) require that agencies improve planning for contingencies; and (5) establish and employ formal emergency response capabilities. Those recommendations are incorporated in this revision.

Since its establishment by the Computer Security Act, the Computer System Security and Privacy Advisory Board has recommended changes in Circular A–130 to: (1) Require that agencies establish computer emergency response teams; and (2) link oversight of Federal computer security activities more closely to the oversight established pursuant to the Federal Manager's Financial Integrity Act (FMFIA), Public Law 97–255. This revision incorporates both of those recommendations.

Subsequent to issuance of Bulletin 90–08, OMB, the National Institute of Standards and Technology (NIST), and the National Security Agency (NSA) met with 28 Federal departments and agencies to review their computer security programs. In February 1993, OMB, NIST and NSA issued a report ("Observations of Agency Computer Security Practices and Implementation of OMB Bulletin No. 90–08") which summarized those meetings and proposed several changes in OMB Circular A–130 as next steps to improving the Federal computer security program. Those proposed changes are incorporated in this revision.

The revised Appendix clarifies the relationship between requirements to protect information classified pursuant to an Executive Order and the requirements in this Appendix. Where an agency processes information which is controlled for national security reasons pursuant to an Executive Order or statute, security measures required by appropriate directives should be included in agency systems. Those policies, procedures, and practices will be coordinated with the U.S. Security Policy Board as directed by the President.

On May 22, 1995, the President signed into law the Paperwork Reduction Act of 1995, Public Law 104–13. That Act, in 44 U.S.C. 3505 and 3506, requires agencies to establish computer security programs, and it tasks OMB to develop and oversee the implementation of policies, principles, standards and guidelines on security. It also requires Federal agencies to identify and provide security protection consistent with the Computer Security Act of 1987 (40 U.S.C. 759 note). This revision is intended to implement those OMB responsibilities.

Comments on the Proposed Appendix

On April 3, 1995, the revised Appendix was proposed for public comment (60 FR 16970). It was also sent directly to Federal agencies for comment and made available for comment via the Internet. Thirty-two comments were received. The comments supported the approach proposed in the revised Appendix. They also made a number of suggestions to improve it. The principal issues raised in comments and our response to them are set forth below.

1. Most of the comments stated that the preamble accompanying the proposed Appendix was useful in their understanding of the Appendix itself. They suggested that the information in the preamble be incorporated in the final Appendix for improved future understanding.

We agree with this suggestion, and have incorporated the preamble, as revised to accommodate changes made to the proposed Appendix, as part B of the final Appendix.

2. Many comments suggested that the terminology of the Appendix should be more directive.

We generally agree with this comment, and have changed part A of the Appendix to be directive, while leaving the descriptive material in part B as explanatory.

3. A number of comments noted that there is a difference between making individuals aware of security needs and training them. They suggested that the Appendix should clarify this distinction and the requirements associated with each.

We agree, and have made changes in the Appendix and the descriptive information in part B to clarify that the requirements for training are consistent with the Computer Security Act (i.e., for increasing computer security awareness and training in accepted security practice).

We have also added a clarification that training for members of the public who are given access to general support systems should normally be accomplished in the context of the application to which they are given access. As was pointed out in comments, members of the public should not be given direct access to general support systems, except through authorized use of an application. We have also added descriptive language in part B to address the need to train members of the public with access to major applications.

4. Several comments raised a concern about the proposed requirement to limit access to systems until a new employee has been trained in security responsibilities. They suggested that training be required to be completed within a certain amount of time after access is granted (e.g., 60 days).

We disagree. Understanding the security requirements that are integral to a system is a fundamental responsibility of each individual who accesses the system. It should not be delayed for administrative convenience. Furthermore, security training should be included as part of general training in use of the system for an employee. Initial awareness and training need not be accomplished through formal classroom training; in some cases it may be through interactive sessions of reading well-written and understandable rules. The critical factor is for the initial and subsequent awareness and training to be commensurate with the risk and magnitude of harm that could occur. Therefore, new employees can and should be trained in their security responsibilities before access is granted. The final Appendix includes this requirement.

5. Several comments expressed concern about the proposed removal of the requirement for agencies to prepare formal risk analyses. They point out that such analyses assist in identifying

threats, vulnerabilities, and risks to a system. They expressed a concern that without such analyses it would be difficult to convince senior management of the need for security. Other comments said that without risk analysis as the basis of decisions, security measures will not be effective. On the other hand, several comments supported the removal of this requirement, which they found not cost-effective.

We agree that security measures must be risk-based. The Computer Security Act requires that security controls be commensurate with the risk and magnitude of harm that could occur. Implicit in that approach is a need to assess the risk to each system. However, given the complexity and detail such formal analyses often entail, a formal risk analysis is not appropriate for every system. Therefore, the Appendix does not require that a formal risk analysis be performed.

At the same time, risk assessment is an essential element in ensuring adequate security. NIST recently issued a handbook, "An Introduction to Computer Security: The NIST Handbook" (March 16, 1995), which contains guidance on computer security risk management and provides a flexible framework for performing meaningful risk assessments. Part B references the NIST handbook.

6. Several comments asked about the relation between the rules of behavior required in the Appendix and operating policies prescribed in the NIST Handbook. Other comments made suggestions about the kind and scope of rules that should be included in the security plan.

We have added language to part B to describe the kinds of rules we believe are appropriate and to clarify that rules of behavior in the Appendix should be consistent with the system-specific policies described in the NIST handbook.

7. Several comments raised a concern about the effectiveness of reviews of security controls unless they are performed by independent reviewers.

An independent review can improve the objectivity of the review, as well as its value to top management in assessing the need for corrective action. Therefore, we have added language to the discussion in part B of the Appendix that clarifies that reviews of major applications, because of their higher risk, should be independent. We have not, however, required that reviews of all general support systems be independent. Nevertheless, given the value of an independent review, agencies may elect to use this approach, particularly where a system supports a high-risk agency function.

In addition, we understand that the U.S. General Accounting Office is developing guidance which provides a structured approach for performing reviews. We have also revised the Appendix to be consistent with OMB Circular No. A–123, "Management Accountability and Control" (June 21, 1995).

8. Several comments requested additional guidance on enforcement of the rules of behavior, either from the Department of Justice or the Office of Personnel Management (OPM).

The presumption in requiring rules of behavior is that they would be enforced as are other behavioral rules within an agency. Therefore, we are not proposing to have central guidance developed by either Justice or OPM. However, we expect that agencies will share their various approaches through inter-agency forums, such as the Computer Security Program Managers' Forum. We have added a brief discussion of this point to part B.

9. Several comments concerned the protection of shared information and requested that additional guidance be provided. We have clarified our intent in the discussion in part B.

10. One comment raised a concern about the Appendix's apparent subordination of technical controls to management controls. While we are stressing the importance of management controls, we have added preamble language to clarify that both types of controls must be in place to be effective.

11. A number of comments raised a concern about whether adequate funding would be forthcoming to implement the requirements of the Appendix.

Implicit in issuing the Appendix is our presumption that a system is created and maintained with adequate security or it should not be created or maintained. Security costs should therefore be factored into the normal capital planning and investment controls process for information technology, consistent with the information systems and information technology management requirements in Section 8b of this circular.

12. A number of comments concerned the government-wide role of the Security Policy Board. Several favored expanding that role, others proposed that it be more limited. Still others said the Appendix should be silent on national security directives.

We have revised the language in the Appendix to clarify the role of the Security Policy Board regrading security of information technology used to process classified information. We have also added language to the preamble which clarifies that Circular No. A–130 and the Appendix exclude certain mission critical systems, the so-called "Warner systems" from coverage, and to describe the Department of Defense's responsibilities pursuant to existing Presidential directives. The Appendix does not attempt to interpret the language of the directives. Rather, it clarifies that requirements issued pursuant to those directives should be used in place of the requirements of the Appendix with respect to the protection of classified information. The discussion of national security directives is included to assist in the coordination of security activities among various security communities.

Accordingly, Circular A–130 is revised as set forth below.

Sally Katzen,

Administrator, Office of Information and Regulatory Affairs.

Executive Office of the President

Office of Management and Budget

February 8, 1996.

Circular No. A–130, Revised (Transmittal Memorandum No. 3)

Memorandum for Heads of Executive Departments and Establishments

Subject: Management of Federal Information Resources.

Circular No. A–130 provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35. This Transmittal Memorandum contains updated guidance on the "Security of Federal Automated Information Systems," Appendix III and makes minor technical revisions to the Circular to reflect the Paperwork Reduction Act of 1995 (Pub. L. 104–13). The Circular is reprinted in its entirety for convenience.

Alice M. Rivlin,

Director.

Attachment

Circular No. A–130 Revised (Transmittal Memorandum No. 3)

Memorandum for Heads of Executive Departments and Establishments

Subject: Management of Federal Information Resources.

1. Purpose: This Circular establishes policy for the management of Federal information resources. Procedural and analytic guidelines for implementing specific aspects of these policies are included as appendices.

2. Rescissions: This Circular rescinds OMB Circulars No. A–3, A–71, A–90, A–108, A–114, and A–121, and all Transmittal Memoranda to those circulars.

3. Authorities: This Circular is issued pursuant to the Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter

35); the Privacy Act, as amended (5 U.S.C. 552a); the Chief Financial Officers Act (31 U.S.C. 3512 et seq.); the Federal Property and Administrative Services Act, as amended (40 U.S.C. 759 and 487); the Computer Security Act (40 U.S.C. 759 note); the Budget and Accounting Act, as amended (31 U.S.C. Chapter 11); Executive Order No. 12046 of March 27, 1978; and Executive Order No. 12472 of April 3, 1984.

4. Applicability and Scope:

a. The policies in this Circular apply to the information activities of all agencies of the executive branch of the Federal government.

b. Information classified for national security purposes should also be handled in accordance with the appropriate national security directives. National security emergency preparedness activities should be conducted in accordance with Executive Order No. 12472.

5. Background: The Paperwork Reduction Act establishes a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner. To assist agencies in an integrated approach to information resources management, the Act requires that the Director of OMB develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information resources management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

6. Definitions:

a. The term "agency" means any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the Federal government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only OMB and the Office of Administration.

b. The term "audiovisual production" means a unified presentation, developed according to a plan or script, containing visual imagery, sound or both, and used to convey information.

c. The term "dissemination" means the government initiated distribution of information to the public. Not considered dissemination within the meaning of this Circular is distribution limited to government employees or agency contractors or grantees, intra- or inter-agency use or sharing of government information, and responses to requests for agency records under the Freedom of Information Act (5 U.S.C. 552) or Privacy Act.

d. The term "full costs," when applied to the expenses incurred in the operation of an information processing service organization (IPSO), is comprised of all direct, indirect, general, and administrative costs incurred in the operation of an IPSO. These costs include, but are not limited to, personnel, equipment, software, supplies, contracted services from private sector providers, space occupancy, intra-agency services from within the agency, inter-agency services from other Federal agencies, other services that are provided by State and local governments, and Judicial and Legislative branch organizations.

e. The term "government information" means information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

f. The term "government publication" means information which is published as an individual document at government expense, or as required by law. (44 U.S.C. 1901)

g. The term "information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

h. The term "information dissemination product" means any book, paper, map, machine-readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, disseminated by an agency to the public.

i. The term "information life cycle" means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

j. The term "information management" means the planning, budgeting, manipulating, and controlling of information throughout its life cycle.

k. The term "information resources" includes both government information and information technology.

l. The term "information processing services organization" (IPSO) means a discrete set of personnel, information technology, and support equipment with the primary function of providing services to more than one agency on a reimbursable basis.

m. The term "information resources management" means the process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.

n. The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

o. The term "information system life cycle" means the phases through which an information system passes, typically characterized as initiation, development, operation, and termination.

p. The term "information technology" means the hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal government to accomplish a Federal function, regardless of the technology involved, whether computers, telecommunications, or others. It includes automatic data processing equipment as that term is defined in Section 111(a)(2) of the Federal Property and Administrative Services Act of 1949. For the purposes of this Circular, automatic data processing and telecommunications activities related to certain critical national security missions, as defined in 44 U.S.C. 3502(2) and 10 U.S.C. 2315, are excluded.

q. The term "major information system" means an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

r. The term "records" means all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included. (44 U.S.C. 3301)

s. The term "records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2))

t. The term "service recipient" means an agency organizational unit, programmatic entity, or chargeable account that receives information processing services from an information processing service organization (IPSO). A service recipient may be either internal or external to the organization responsible for providing information resources services, but normally does not report either to the manager or director of the IPSO or to the same immediate supervisor.

7. Basic Considerations and Assumptions:

a. The Federal Government is the largest single producer, collector, consumer, and disseminator of information in the United States. Because of the extent of the government's information activities, and the dependence of those activities upon public cooperation, the management of Federal information resources is an issue of continuing importance to all Federal agencies, State and local governments, and the public.

b. Government information is a valuable national resource. It provides the public with knowledge of the government, society, and economy—past, present, and future. It is a means to ensure the accountability of government, to manage the government's operations, to maintain the healthy performance of the economy, and is itself a commodity in the marketplace.

c. The free flow of information between the government and the public is essential to a democratic society. It is also essential that the government minimize the Federal paperwork burden on the public, minimize the cost of its information activities, and maximize the usefulness of government information.

d. In order to minimize the cost and maximize the usefulness of government information, the expected public and private benefits derived from government information should exceed the public and private costs of the information, recognizing that the benefits to be derived from government information may not always be quantifiable.

e. The nation can benefit from government information disseminated both by Federal agencies and by diverse nonfederal parties, including State and local government agencies, educational and other not-for-profit institutions, and for-profit organizations.

f. Because the public disclosure of government information is essential to the operation of a democracy, the management of Federal information resources should protect the public's right of access to government information.

g. The individual's right to privacy must be protected in Federal Government information activities involving personal information.

h. Systematic attention to the management of government records is an essential component of sound public resources management which ensures public accountability. Together with records preservation, it protects the government's historical record and guards the legal and financial rights of the government and the public.

i. Agency strategic planning can improve the operation of government programs. The application of information resources should support an agency's strategic plan to fulfill its mission. The integration of IRM planning with agency strategic planning promotes the appropriate application of Federal information resources.

j. Because State and local governments are important producers of government information for many areas such as health, social welfare, labor, transportation, and education, the Federal Government must cooperate with these governments in the management of information resources.

k. The open and efficient exchange of scientific and technical government information, subject to applicable national security controls and the proprietary rights of others, fosters excellence in scientific research and effective use of Federal research and development funds.

l. Information technology is not an end in itself. It is one set of resources that can improve the effectiveness and efficiency of Federal program delivery.

m. Federal Government information resources management policies and activities can affect, and be affected by, the information policies and activities of other nations.

n. Users of Federal information resources must have skills, knowledge, and training to manage information resources, enabling the Federal government to effectively serve the public through automated means.

o. The application of up-to-date information technology presents opportunities to promote fundamental changes in agency structures, work processes, and ways of interacting with the public that improve the effectiveness and efficiency of Federal agencies.

p. The availability of government information in diverse media, including electronic formats, permits agencies and the public greater flexibility in using the information.

q. Federal managers with program delivery responsibilities should recognize the importance of information resources management to mission performance.

8. Policy

a. Information Management Policy:

(1) Information Management Planning. Agencies shall plan in an integrated manner for managing information throughout its life cycle. Agencies shall:

(a) Consider, at each stage of the information life cycle, the effects of decisions and actions on other stages of the life cycle, particularly those concerning information dissemination;

(b) Consider the effects of their actions on members of the public and ensure consultation with the public as appropriate;

(c) Consider the effects of their actions on State and local governments and ensure consultation with those governments as appropriate;

(d) Seek to satisfy new information needs through interagency or intergovernmental sharing of information, or through commercial sources, where appropriate, before creating or collecting new information;

(e) Integrate planning for information systems with plans for resource allocation and use, including budgeting, acquisition, and use of information technology;

(f) Train personnel in skills appropriate to management of information;

(g) Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information;

(h) Use voluntary standards and Federal Information Processing Standards where appropriate or required;

(i) Consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented;

(j) Record, preserve, and make accessible sufficient information to ensure the management and accountability of agency programs, and to protect the legal and financial rights of the Federal Government;

(k) Incorporate records management and archival functions into the design, development, and implementation of information systems;

(l) Provide for public access to records where required or appropriate.

(2) Information Collection. Agencies shall collect or create only that information necessary for the proper performance of agency functions and which has practical utility.

(3) Electronic Information Collection. Agencies shall use electronic collection techniques where such techniques reduce burden on the public, increase efficiency of government programs, reduce costs to the government and the public, and/or provide better service to the public. Conditions favorable to electronic collection include:

(a) The information collection seeks a large volume of data and/or reaches a large proportion of the public;

(b) The information collection recurs frequently;

(c) The structure, format, and/or definition of the information sought by the information collection does not change significantly over several years;

(d) The agency routinely converts the information collected to electronic format;

(e) A substantial number of the affected public are known to have ready access to the necessary information technology and to maintain the information in electronic form;

(f) Conversion to electronic reporting, if mandatory, will not impose substantial costs or other adverse effects on the public, especially State and local governments and small business entities.

(4) Records Management. Agencies shall:

(a) Ensure that records management programs provide adequate and proper documentation of agency activities;

(b) Ensure the ability to access records regardless of form or medium;

(c) In a timely fashion, establish, and obtain the approval of the Archivist of the United States for, retention schedules for Federal records; and

(d) Provide training and guidance as appropriate to all agency officials and employees and contractors regarding their Federal records management responsibilities.

(5) Providing Information to the Public. Agencies have a responsibility to provide information to the public consistent with their missions. Agencies shall discharge this responsibility by:

(a) Providing information, as required by law, describing agency organization, activities, programs, meetings, systems of records, and other information holdings, and how the public may gain access to agency information resources;

(b) Providing access to agency records under provisions of the Freedom of Information Act and the Privacy Act, subject to the protections and limitations provided for in these Acts;

(c) Providing such other information as is necessary or appropriate for the proper performance of agency functions; and

(d) In determining whether and how to disseminate information to the public, agencies shall:

(i) Disseminate information in a manner that achieves the best balance between the goals of maximizing the usefulness of the information and minimizing the cost to the government and the public;

(ii) Disseminate information dissemination products on equitable and timely terms;

(iii) Take advantage of all dissemination channels, Federal and nonfederal, including State and local governments, libraries and private sector entities, in discharging agency information dissemination responsibilities;

(iv) Help the public locate government information maintained by or for the agency.

(6) Information Dissemination Management System. Agencies shall maintain and

implement a management system for all information dissemination products which shall, at a minimum:

(a) Assure that information dissemination products are necessary for proper performance of agency functions (44 U.S.C. 1108);

(b) Consider whether an information dissemination product available from other Federal or nonfederal sources is equivalent to an agency information dissemination product and reasonably fulfills the dissemination responsibilities of the agency;

(c) Establish and maintain inventories of all agency information dissemination products;

(d) Develop such other aids to locating agency information dissemination products including catalogs and directories, as may reasonably achieve agency information dissemination objectives;

(e) Identify in information dissemination products the source of the information, if from another agency;

(f) Ensure that members of the public with disabilities whom the agency has a responsibility to inform have a reasonable ability to access the information dissemination products;

(g) Ensure that government publications are made available to depository libraries through the facilities of the Government Printing Office, as required by law (44 U.S.C. Part 19);

(h) Provide electronic information dissemination products to the Government Printing Office for distribution to depository libraries;

(i) Establish and maintain communications with members of the public and with State and local governments so that the agency creates information dissemination products that meet their respective needs;

(j) Provide adequate notice when initiating, substantially modifying, or terminating significant information dissemination products; and

(k) Ensure that, to the extent existing information dissemination policies or practices are inconsistent with the requirements of this Circular, a prompt and orderly transition to compliance with the requirements of this Circular is made.

(7) Avoiding Improperly Restrictive Practices. Agencies shall:

(a) Avoid establishing, or permitting others to establish on their behalf, exclusive, restricted, or other distribution arrangements that interfere with the availability of information dissemination products on a timely and equitable basis;

(b) Avoid establishing restrictions or regulations, including the charging of fees or royalties, on the reuse, resale, or redissemination of Federal information dissemination products by the public; and,

(c) Set user charges for information dissemination products at a level sufficient to recover the cost of dissemination but no higher. They shall exclude from calculation of the charges costs associated with original collection and processing of the information. Exceptions to this policy are:

(i) Where statutory requirements are at variance with the policy;

(ii) Where the agency collects, processes, and disseminates the information for the benefit of a specific identifiable group beyond the benefit to the general public;

(iii) Where the agency plans to establish user charges at less than cost of dissemination because of a determination that higher charges would constitute a significant barrier to properly performing the agency's functions, including reaching members of the public whom the agency has a responsibility to inform; or

(iv) Where the Director of OMB determines an exception is warranted.

(8) Electronic Information Dissemination. Agencies shall use electronic media and formats, including public networks, as appropriate and within budgetary constraints, in order to make government information more easily accessible and useful to the public. The use of electronic media and formats for information dissemination is appropriate under the following conditions:

(a) The agency develops and maintains the information electronically;

(b) Electronic media or formats are practical and cost effective ways to provide public access to a large, highly detailed volume of information;

(c) The agency disseminates the product frequently;

(d) The agency knows a substantial portion of users have ready access to the necessary information technology and training to use electronic information dissemination products;

(e) A change to electronic dissemination, as the sole means of disseminating the product, will not impose substantial acquisition or training costs on users, especially State and local governments and small business entities.

(9) Safeguards. Agencies shall:

(a) Ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information;

(b) Limit the collection of information which identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions;

(c) Limit the sharing of information that identifies individuals or contains proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists;

(d) Provide individuals, upon request, access to records about them maintained in Privacy Act systems of records, and permit them to amend such records as are in error consistent with the provisions of the Privacy Act.

b. Information Systems and Information Technology Management

(1) Evaluation and Performance Measurement. Agencies shall promote the appropriate application of Federal information resources as follows:

(a) Seek opportunities to improve the effectiveness and efficiency of government programs through work process redesign and the judicious application of information technology;

(b) Prepare, and update as necessary throughout the information system life cycle, a benefit-cost analysis for each information system:

(i) At a level of detail appropriate to the size of the investment;

(ii) Consistent with the methodology described in OMB Circular No. A–94, "Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs;" and

(iii) that relies on systematic measures of mission performance, including the:

(a) Effectiveness of program delivery;

(b) Efficiency of program administration; and

(c) Reduction in burden, including information collection burden, imposed on the public;

(c) Conduct benefit-cost analyses to support ongoing management oversight processes that maximize return on investment and minimize financial and operational risk for investments in major information systems on an agency-wide basis; and

(d) Conduct post-implementation reviews of information systems to validate estimated benefits and document effective management practices for broader use.

(2) Strategic Information Resources Management (IRM) Planning. Agencies shall establish and maintain strategic information resources management planning processes which include the following components:

(a) Strategic IRM planning that addresses how the management of information resources promotes the fulfillment of an agency's mission. This planning process should support the development and maintenance of a strategic IRM plan that reflects and anticipates changes in the agency's mission, policy direction, technological capabilities, or resource levels;

(b) Information planning that promotes the use of information throughout its life cycle to maximize the usefulness of information, minimize the burden on the public, and preserve the appropriate integrity, availability, and confidentiality of information. It shall specifically address the planning and budgeting for the information collection burden imposed on the public as defined by 5 CFR 1320;

(c) Operational information technology planning that links information technology to anticipated program and mission needs, reflects budget constraints, and forms the basis for budget requests. This planning should result in the preparation and maintenance of an up-to-date five-year plan, as required by 44 U.S.C. 3506, which includes:

(i) A listing of existing and planned major information systems;

(ii) A listing of planned information technology acquisitions;

(iii) An explanation of how the listed major information systems and planned information technology acquisitions relate to each other and support the achievement of the agency's mission; and

(iv) A summary of computer security planning, as required by Section 6 of the Computer Security Act of 1987 (40 U.S.C. 759 note); and

(d) Coordination with other agency planning processes including strategic, human resources, and financial resources.

(3) Information Systems Management Oversight. Agencies shall establish information system management oversight mechanisms that:

(a) Ensure that each information system meets agency mission requirements;

(b) Provide for periodic review of information systems to determine:

(i) How mission requirements might have changed;

(ii) Whether the information system continues to fulfill ongoing and anticipated mission requirements; and

(iii) What level of maintenance is needed to ensure the information system meets mission requirements cost effectively;

(c) Ensure that the official who administers a program supported by an information system is responsible and accountable for the management of that information system throughout its life cycle;

(d) Provide for the appropriate training for users of Federal information resources;

(e) Prescribe Federal information system requirements that do not unduly restrict the prerogatives of State, local, and tribal governments;

(f) Ensure that major information systems proceed in a timely fashion towards agreed-upon milestones in an information system life cycle, meet user requirements, and deliver intended benefits to the agency and affected publics through coordinated decision making about the information, human, financial, and other supporting resources; and

(g) Ensure that financial management systems conform to the requirements of OMB Circular No. A–127, "Financial Management Systems."

(4) **USE OF INFORMATION RESOURCES.** Agencies shall create and maintain management and technical frameworks for using information resources that document linkages between mission needs, information content, and information technology capabilities. These frameworks should guide both strategic and operational IRM planning. They should also address steps necessary to create an open systems environment. Agencies shall implement the following principles:

(a) Develop information systems in a manner that facilitates necessary interoperability, application portability, and scalability of computerized applications across networks of heterogeneous hardware, software, and communications platforms;

(b) Ensure that improvements to existing information systems and the development of planned information systems do not unnecessarily duplicate information systems available within the same agency, from other agencies, or from the private sector;

(c) Share available information systems with other agencies to the extent practicable and legally permissible;

(d) Meet information technology needs through intra-agency and inter-agency sharing, when it is cost effective, before acquiring new information technology resources;

(e) For Information Processing Service Organizations (IPSOs) that have costs in excess of $5 million per year, agencies shall:

(i) Account for the full costs of operating all IPSOs; (ii) Recover the costs incurred for providing IPSO services to all service recipients on an equitable basis commensurate with the costs required to provide those services; and

(iii) Document sharing agreements between service recipients and IPSOs; and

(f) Establish a level of security for all information systems that is 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 these information systems.

(5) **ACQUISITION OF INFORMATION TECHNOLOGY.** Agencies shall:

(a) Acquire information technology in a manner that makes use of full and open competition and that maximizes return on investment;

(b) Acquire off-the-shelf software from commercial sources, unless the cost effectiveness of developing custom software to meet mission needs is clear and has been documented;

(c) Acquire information technology in accordance with OMB Circular No. A–109, "Acquisition of Major Systems," where appropriate; and

(d) Acquire information technology in a manner that considers the need for accommodations of accessibility for individuals with disabilities to the extent that needs for such access exist.

9. **ASSIGNMENT OF RESPONSIBILITIES**

a. **ALL FEDERAL AGENCIES.** The head of each agency shall:

(1) Have primary responsibility for managing agency information resources;

(2) Ensure that the information policies, principles, standards, guidelines, rules, and regulations prescribed by OMB are implemented appropriately within the agency;

(3) Develop internal agency information policies and procedures and oversee, evaluate, and otherwise periodically review agency information resources management activities for conformity with the policies set forth in this Circular;

(4) Develop agency policies and procedures that provide for timely acquisition of required information technology;

(5) Maintain an inventory of the agencies' major information systems, holdings and information dissemination products, as required by 44 U.S.C. 3511.

(6) Implement and enforce applicable records management policies and procedures, including requirements for archiving information maintained in electronic format, particularly in the planning, design and operation of information systems.

(7) Identify to the Director, OMB, statutory, regulatory, and other impediments to efficient management of Federal information resources and recommend to the Director legislation, policies, procedures, and other guidance to improve such management;

(8) Assist OMB in the performance of its functions under the PRA including making services, personnel, and facilities available to OMB for this purpose to the extent practicable;

(9) Appoint a senior official, as required by 44 U.S.C. 3506(a), who shall report directly to the agency head to carry out the responsibilities of the agency under the PRA. The head of the agency shall keep the Director, OMB, advised as to the name, title, authority, responsibilities, and organizational resources of the senior official. For purposes of this paragraph, military departments and the Office of the Secretary of Defense may each appoint one official.

(10) Direct the senior official appointed pursuant to 44 U.S.C. 3506(a) to monitor agency compliance with the policies, procedures, and guidance in this Circular. Acting as an ombudsman, the senior official shall consider alleged instances of agency failure to comply with this Circular and recommend or take corrective action as appropriate. The senior official shall report annually, not later than February 1st of each year, to the Director those instances of alleged failure to comply with this Circular and their resolution.

b. **DEPARTMENT OF STATE.** The Secretary of State shall:

(1) Advise the Director, OMB, on the development of United States positions and policies on international information policy issues affecting Federal Government information activities and ensure that such positions and policies are consistent with Federal information resources management policy;

(2) Ensure, in consultation with the Secretary of Commerce, that the United States is represented in the development of international information technology standards, and advise the Director, OMB, of such activities.

c. **DEPARTMENT OF COMMERCE.** The Secretary of Commerce shall:

(1) Develop and issue Federal Information Processing Standards and guidelines necessary to ensure the efficient and effective acquisition, management, security, and use of information technology;

(2) Advise the Director, OMB, on the development of policies relating to the procurement and management of Federal telecommunications resources;

(3) Provide OMB and the agencies with scientific and technical advisory services relating to the development and use of information technology;

(4) Conduct studies and evaluations concerning telecommunications technology, and concerning the improvement, expansion, testing, operation, and use of Federal telecommunications systems and advise the Director, OMB, and appropriate agencies of the recommendations that result from such studies;

(5) Develop, in consultation with the Secretary of State and the Director of OMB, plans, policies, and programs relating to international telecommunications issues affecting government information activities;

(6) Identify needs for standardization of telecommunications and information processing technology, and develop standards, in consultation with the Secretary of Defense and the Administrator of General Services, to ensure efficient application of such technology;

(7) Ensure that the Federal Government is represented in the development of national and, in consultation with the Secretary of

State, international information technology standards, and advise the Director, OMB, of such activities.

c. **DEPARTMENT OF DEFENSE.** The Secretary of Defense shall develop, in consultation with the Administrator of General Services, uniform Federal telecommunications standards and guidelines to ensure national security, emergency preparedness, and continuity of government.

e. **GENERAL SERVICES ADMINISTRATION.** The Administrator of General Services shall:

(1) Advise the Director, OMB, and agency heads on matters affecting the procurement of information technology;

(2) Coordinate and, when required, provide for the purchase, lease, and maintenance of information technology required by Federal agencies;

(3) Develop criteria for timely procurement of information technology and delegate procurement authority to agencies that comply with the criteria;

(4) Provide guidelines and regulations for Federal agencies, as authorized by law, on the acquisition, maintenance, and disposition of information technology, and for implementation of Federal Information Processing Standards;

(5) Develop policies and guidelines that facilitate the sharing of information technology among agencies as required by this Circular;

(6) Manage the Information Technology Fund in accordance with the Federal Property and Administrative Services Act as amended;

f. **OFFICE OF PERSONNEL MANAGEMENT.** The Director, Office of Personnel Management, shall:

(1) Develop and conduct training programs for Federal personnel on information resources management including end-user computing;

(2) Evaluate periodically future personnel management and staffing requirements for Federal information resources management;

(3) Establish personnel security policies and develop training programs for Federal personnel associated with the design, operation, or maintenance of information systems.

g. National Archives and Records Administration. The Archivist of the United States shall:

(1) Administer the Federal records management program in accordance with the National Archives and Records Act;

(2) Assist the Director, OMB, in developing standards and guidelines relating to the records management program.

h. Office of Management and Budget. The Director of the Office of Management and Budget shall:

(1) Provide overall leadership and coordination of Federal information resources management within the executive branch;

(2) Serve as the President's principal adviser on procurement and management of Federal telecommunications systems, and develop and establish policies for procurement and management of such systems;

(3) Issue policies, procedures, and guidelines to assist agencies in achieving integrated, effective, and efficient information resources management;

(4) Initiate and review proposals for changes in legislation, regulations, and agency procedures to improve Federal information resources management;

(5) Review and approve or disapprove agency proposals for collection of information from the public, as defined by 5 CFR 1320.3;

(6) Develop and maintain a Governmentwide strategic plan for information resources management.

(7) Evaluate agencies' information resources management and identify cross-cutting information policy issues through the review of agency information programs, information collection budgets, information technology acquisition plans, fiscal budgets, and by other means;

(8) Provide policy oversight for the Federal records management function conducted by the National Archives and Records Administration, coordinate records management policies and programs with other information activities, and review compliance by agencies with records management requirements;

(9) Review agencies' policies, practices, and programs pertaining to the security, protection, sharing, and disclosure of information, in order to ensure compliance, with respect to privacy and security, with the Privacy Act, the Freedom of Information Act, the Computer Security Act and related statutes;

(10) Resolve information technology procurement disputes between agencies and the General Services Administration pursuant to Section 111 of the Federal Property and Administrative Services Act;

(11) Review proposed U.S. Government Position and Policy statements on international issues affecting Federal Government information activities and advise the Secretary of State as to their consistency with Federal information resources management policy.

(12) Coordinate the development and review by the Office of Information and Regulatory Affairs of policy associated with Federal procurement and acquisition of information technology with the Office of Federal Procurement Policy.

10. Oversight:

a. The Director, OMB, will use information technology planning reviews, fiscal budget reviews, information collection budget reviews, management reviews, and such other measures as the Director deems necessary to evaluate the adequacy and efficiency of each agency's information resources management and compliance with this Circular.

b. The Director, OMB, may, consistent with statute and upon written request of an agency, grant a waiver from particular requirements of this Circular. Requests for waivers must detail the reasons why a particular waiver is sought, identify the duration of the waiver sought, and include a plan for the prompt and orderly transition to full compliance with the requirements of this Circular. Notice of each waiver request shall be published promptly by the agency in the **Federal Register**, with a copy of the waiver request made available to the public on request.

11. Effectiveness: This Circular is effective upon issuance. Nothing in this Circular shall be construed to confer a private right of action on any person.

12. Inquiries: All questions or inquiries should be addressed to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503. Telephone: (202) 395-3785.

13. Sunset Review Date: OMB will review this Circular three years from the date of issuance to ascertain its effectiveness.

Appendix I to OMB Circular No. A-130—Federal Agency Responsibilities for Maintaining Records About Individuals

1. Purpose and Scope

This Appendix describes agency responsibilities for implementing the reporting and publication requirements of the Privacy Act of 1974, 5 U.S.C. 552a, as amended (hereinafter "the Act"). It applies to all agencies subject to the Act. Note that this Appendix does not rescind other guidance OMB has issued to help agencies interpret the Privacy Act's provisions, e.g., Privacy Act Guidelines (40 FR 28949–28978, July 9, 1975), or Final Guidance for Conducting Matching Programs (54 FR at 25819, June 19, 1989).

2. Definitions

a. The terms "agency," "individual," "maintain," "matching program," "record," "system of records," and "routine use," as used in this Appendix, are defined in the Act (5 U.S.C. 552a(a)).

b. Matching Agency. Generally, the Recipient Federal agency (or the Federal source agency in a match conducted by a nonfederal agency) is the matching agency and is responsible for meeting the reporting and publication requirements associated with the matching program. However, in large, multi-agency matching programs, where the recipient agency is merely performing the matches and the benefit accrues to the source agencies, the partners should assign responsibility for compliance with the administrative requirements in a fair and reasonable way. This may mean having the matching agency carry out these requirements for all parties, having one participant designated to do so, or having each source agency do so for its own matching program(s).

c. Nonfederal Agency. Nonfederal agencies are State or local governmental agencies receiving or providing records in a matching program with a Federal agency.

d. Recipient Agency. Recipient agencies are Federal agencies or their contractors receiving automated records from the Privacy Act systems of records of other Federal agencies, or from State or local governments, to be used in a matching program as defined in the Act.

e. Source Agency. A source agency is a Federal agency that discloses automated records from a system of records to another Federal agency or to a State or local agency to be used in a matching program. It is also a State or local agency that discloses records to a Federal agency for use in a matching program.

3. Assignment of Responsibilities

a. All Federal Agencies. In addition to meeting the agency requirements contained in the Act and the specific reporting and publication requirements detailed in this Appendix, the head of each agency shall ensure that the following reviews are conducted as often as specified below, and be prepared to report to the Director, OMB, the results of such reviews and the corrective action taken to resolve problems uncovered. The head of each agency shall:

(1) Section (m) Contracts. Review every two years a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to accomplish an agency function, in order to ensure that the wording of each contract makes the provisions of the Act binding on the contractor and his or her employees. (See 5 U.S.C. 552a(m)(1)).

(2) Recordkeeping Practices. Review biennially agency recordkeeping and disposal policies and practices in order to assure compliance with the Act, paying particular attention to the maintenance of automated records.

(3) Routine Use Disclosures. Review every four years the routine use disclosures associated with each system of records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency collected the information.

(4) Exemption of Systems of Records. Review every four years each system of records for which the agency has promulgated exemption rules pursuant to Section (j) or (k) of the Act in order to determine whether such exemption is still needed.

(5) Matching Programs. Review annually each ongoing matching program in which the agency has participated during the year in order to ensure that the requirements of the Act, the OMB guidance, and any agency regulations, operating instructions, or guidelines have been met.

(6) Privacy Act Training. Review biennially agency training practices in order to ensure that all agency personnel are familiar with the requirements of the Act, with the agency's implementing regulation, and with any special requirements of their specific jobs.

(7) Violations. Review biennially the actions of agency personnel that have resulted either in the agency being found civilly liable under Section (g) of the Act, or an employee being found criminally liable under the provisions of Section (i) of the Act, in order to determine the extent of the problem, and to find the most effective way to prevent recurrence of the problem.

(8) Systems of Records Notices. Review biennially each system of records notice to ensure that it accurately describes the system of records. Where minor changes are needed, e.g., the name of the system manager, ensure that an amended notice is published in the **Federal Register**. Agencies may choose to make one annual comprehensive publication consolidating such minor changes. This requirement is distinguished from and in addition to the requirement to report to OMB and Congress significant changes to systems of records and to publish those changes in the **Federal Register** (See paragraph 4c of this Appendix).

b. Department of Commerce. The Secretary of Commerce shall, consistent with guidelines issued by the Director, OMB, develop and issue standards and guidelines for ensuring the security of information protected by the Act in automated information systems.

c. The Department of Defense, General Services Administration, and National Aeronautics and Space Administration. These agencies shall, consistent with guidelines issued by the Director, OMB, ensure that instructions are issued on what agencies must do in order to comply with the requirements of Section (m) of the Act when contracting for the operation of a system of records to accomplish an agency purpose.

d. Office of Personnel Management. The Director of the Office of Personnel Management shall, consistent with guidelines issued by the Director, OMB:

(1) Develop and maintain government-wide standards and procedures for civilian personnel information processing and recordkeeping directives to assure conformance with the Act.

(2) Develop and conduct Privacy Act training programs for agency personnel, including both the conduct of courses in various substantive areas (e.g., administrative, information technology) and the development of materials that agencies can use in their own courses. The assignment of this responsibility to OPM does not affect the responsibility of individual agency heads for developing and conducting training programs tailored to the specific needs of their own personnel.

e. National Archives and Records Administration. The Archivist of the United States through the Office of the Federal Register, shall, consistent with guidelines issued by the Director, OMB:

(1) Issue instructions on the format of the agency notices and rules required to be published under the Act.

(2) Compile and publish every two years, the rules promulgated under 5 U.S.C. 552a(f) and agency notices published under 5 U.S.C. 552a(e)(4) in a form available to the public at low cost.

(3) Issue procedures governing the transfer of records to Federal Records Centers for storage, processing, and servicing pursuant to 44 U.S.C. 3103. For purposes of the Act, such records are considered to be maintained by the agency that deposited them. The Archivist may disclose deposited records only according to the access rules established by the agency that deposited them.

f. Office of Management and Budget. The Director of the Office of Management and Budget will:

(1) Issue guidelines and directives to the agencies to implement the Act.

(2) Assist the agencies, at their request, in implementing their Privacy Act programs.

(3) Review new and altered system of records and matching program reports submitted pursuant to Section (o) of the Act.

(4) Compile the biennial report of the President to Congress in accordance with Section (s) of the Act.

(5) Compile and issue a biennial report on the agencies' implementation of the computer matching provisions of the Privacy Act, pursuant to Section (u)(6) of the Act.

4. Reporting Requirements. The Privacy Act requires agencies to make the following kinds of reports:

Report	When Due	Recipient**
Biennial Privacy Act Report	June 30, 1996, 1998, 2000, 2002	Administrator, OIRA.
Biennial Matching Activity Report	June 30, 1996, 1998, 2000, 2002	Administrator, OIRA.
New System of Records Report	When establishing a system of records—at least 40 days before operating the system*.	Administrator, OIRA, Congress.
Altered System of Records Report.	When adding a new routine use, exemption, or otherwise significantly altering an existing system of records—at least 40 days before change to system takes place.	*Administrator, OIRA, Congress.
New Matching Program Report	When establishing a new matching program—at least 40 days before operating the program*.	Administrator, OIRA, Congress.
Renewal of Existing Matching Program.	At least 40 days prior to expiration of any one year extension of the original program—treat as a new program.	Administrator, OIRA, Congress.
Altered Matching Program	When making a significant change to an existing matching program—at least 40 days before operating an altered program*.	Administrator, OIRA, Congress.
Matching Agreements	At least 40 days prior to the start of a matching program*	Congress.

*Review Period: Note that the statutory reporting requirement is 30 days prior; the additional ten days will ensure that OMB and Congress have sufficient time to review the proposal. Agencies should therefore ensure that reports are mailed expeditiously after being signed.

**Recipient Addresses: At bottom of envelope print "Privacy Act Report".

House of Representatives: The Chair of the House Committee on Government Reform and Oversight, 2157 RHOB, Washington, D.C. 20515–6143.

Senate: The Chair of the Senate Committee on Governmental Affairs, 340 SDOB, Washington, D.C. 20510–6250.

Office of Management and Budget: The Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, ATTN: Docket Library, NEOB Room 10012, Washington, D.C. 20503.

a. Biennial Privacy Act Report. To provide the necessary information for the biennial report of the President, agencies shall submit a biennial report to OMB, covering their Privacy Act activities for the calendar years covered by the reporting period. The exact format of the report will be established by OMB. At a minimum, however, agencies should collect and be prepared to report the following data on a calendar year basis:

(1) A listing of publication activity during the year showing the following:

*Total Number of Systems of Records (Exempt/NonExempt)
*Number of New Systems of Records Added (Exempt/NonExempt)
*Number Routine Uses Added
*Number Exemptions Added to Existing Systems
*Number Exemptions Deleted from Existing Systems
*Total Number of Automated Systems of Records (Exempt/NonExempt)

The agency should provide a brief narrative describing those activities in detail, e.g., "the Department added a (k)(1) exemption to an existing system of records entitled "Investigative Records of the Office of Investigations;" or "the agency added a new routine use to a system of records entitled 'Employee Health Records' that would permit disclosure of health data to researchers under contract to the agency to perform workplace risk analysis."

(2) A brief description of any public comments received on agency publication and implementation activities, and agency response.

(3) Number of access and amendment requests from record subjects citing the Privacy Act that were received during the calendar year of the report. Also the disposition of requests from any year that were completed during the calendar year of the report:

*Total Number of Access Requests
Number Granted in Whole
Number Granted in Part
Number Wholly Denied
Number For Which No Record Found
*Total Amendment Requests
Number Granted in Whole
Number Granted in Part
Number Wholly Denied
*Number of Appeals of Denials of Access
Number Granted in Whole
Number Granted in Part
Number Wholly Denied
Number For Which No Record Found
*Number of Appeals of Denials of Amendment
Number Granted in Whole
Number Granted in Part
Number Wholly Denied

(4) Number of instances in which individuals brought suit under section (g) of the Privacy Act against the agency and the results of any such litigation that resulted in a change to agency practices or affected guidance issued by OMB.

(5) Results of the reviews undertaken in response to paragraph 3a of this Appendix.

(6) Description of agency Privacy Act training activities conducted in accordance with paragraph 3a(6) of this Appendix.

b. Biennial Matching Activity Report (See 5 U.S.C. 552a(u)(3)(D)). At the end of each calendar year, the Data Integrity Board of each agency that has participated in a matching program will collect data summarizing that year's matching activity. The Act requires that such activity be reported every two years. OMB will establish the exact format of the report, but agencies' Data Integrity Boards should be prepared to report the data identified below both to the agency head and to OMB:

(1) A listing of the names and positions of the members of the Data Integrity Board and showing separately the name of the Board Secretary, his or her agency mailing address, and telephone number. Also show and explain any changes in membership or structure occurring during the reporting year.

(2) A listing of each matching program, by title and purpose, in which the agency participated during the reporting year. This listing should show names of participant agencies, give a brief description of the program, and give a page citation and the date of the **Federal Register** notice describing the program.

(3) For each matching program, an indication of whether the cost/benefit analysis performed resulted in a favorable ratio. The Data Integrity Board should explain why the agency proceeded with any matching program for which an unfavorable ratio was reached.

(4) For each program for which the Board waived a cost/benefit analysis, the reasons for the waiver and the results of the match, if tabulated.

(5) A description of any matching agreement the Board rejected and an explanation of the rejection.

(6) A listing of any violations of matching agreements that have been alleged or identified, and a discussion of any action taken.

(7) A discussion of any litigation involving the agency's participation in any matching program.

(8) For any litigation based on allegations of inaccurate records, an explanation of the steps the agency used to ensure the integrity of its data as well as the verification process it used in the matching program, including an assessment of the adequacy of each.

c. New and Altered System of Records Report. The Act requires agencies to publish notices in the **Federal Register** describing new or altered systems of records, and to submit reports to OMB, and to the Chair of the Committee on Government Reform and Oversight of the House of Representatives, and the Chair of the Committee on Governmental Affairs of the Senate. The reports must be transmitted at least 40 days prior to the operation of the new system of records or the date on which the alteration to an existing system takes place.

(1) Which Alterations Require a Report. Minor changes to systems of records need not be reported. For example, a change in the designation of the system manager due to a reorganization would not require a report, so long as an individual's ability to gain access to his or her records is not affected. Other examples include changing applicable safeguards as a result of a risk analysis or deleting a routine use when there is no longer a need for the disclosure. The following changes are those for which a report is required:

(a) A significant increase in the number, type, or category of individuals about whom records are maintained. For example, a system covering physicians that has been expanded to include other types of health care providers, e.g., nurses, technicians, etc., would require a report. Increases attributable to normal growth should not be reported.

(b) A change that expands the types or categories of information maintained. For example, a benefit system which originally included only earned income information that has been expanded to include unearned income information.

(c) A change that alters the purpose for which the information is used.

(d) A change to equipment configuration (either hardware or software) that creates substantially greater access to the records in the system of records. For example, locating interactive terminals at regional offices for accessing a system formerly accessible only at the headquarters would require a report.

(e) The addition of an exemption pursuant to Section (j) or (k) of the Act. Note that, in examining a rulemaking for a Privacy Act exemption as part of a report of a new or altered system of records, OMB will also review the rule under applicable regulatory review procedures and agencies need not make a separate submission for that purpose.

(f) The addition of a routine use pursuant to 5 U.S.C. 552a(b)(3).

(2) Reporting Changes to Multiple Systems of Records. When an agency makes a change to an information technology installation or a telecommunication network, or makes any other general changes in information collection, processing, dissemination, or storage that affect multiple systems of records, it may submit a single, consolidated report, with changes to existing notices and supporting documentation included in the submission.

(3) Contents of the New or Altered System Report. The report for a new or altered system has three elements: a transmittal letter, a narrative statement, and supporting documentation.

(a) Transmittal Letter. The transmittal letter should be signed by the senior agency official responsible for implementation of the Act within the agency and should contain the name and telephone number of the individual who can best answer questions about the system of records. The letter should contain the agency's assurance that the proposed system does not duplicate any existing agency or government-wide systems of records. The letter sent to OMB may also include a request for waiver of the time

period for the review. The agency should indicate why it cannot meet the established review period and the consequences of not obtaining the waiver. (See paragraph 4e below.) There is no prescribed format for the letter.

(b) Narrative Statement. There is also no prescribed format for the narrative statement, but it should be brief. It should make reference, as appropriate, to information in the supporting documentation rather than restating such information. The statement should:

1. Describe the purpose for which the agency is establishing the system of records.

2. Identify the authority under which the system of records is maintained. The agency should avoid citing housekeeping statutes, but rather cite the underlying programmatic authority for collecting, maintaining, and using the information. When the system is being operated to support an agency housekeeping program, e.g., a carpool locator, the agency may, however, cite a general housekeeping statute that authorizes the agency head to keep such records as necessary.

3. Provide the agency's evaluation of the probable or potential effect of the proposal on the privacy of individuals.

4. Provide a brief description of the steps taken by the agency to minimize the risk of unauthorized access to the system of records. A more detailed assessment of the risks and specific administrative, technical, procedural, and physical safeguards established shall be made available to OMB upon request.

5. Explain how each proposed routine use satisfies the compatibility requirement of subsection (a)(7) of the Act. For altered systems, this requirement pertains only to any newly proposed routine use.

6. Provide OMB Control Numbers, expiration dates, and titles of any information collection requests (e.g., forms, surveys, etc.) contained in the system of records and approved by OMB under the Paperwork Reduction Act. If the request for OMB clearance of an information collection is pending, the agency may simply state the title of the collection and the date it was submitted for OMB clearance.

(c) Supporting Documentation. Attach the following to all new or altered system of records reports:

1. A copy of the new or altered system of records notice consistent with the provisions of 5 U.S.C. 552a(e)(4). The notice must appear in the format prescribed by the Office of the Federal Register's *Document Drafting Handbook*. For proposed altered systems the agency should supply a copy of the original system of records notice to ensure that reviewers can understand the changes proposed. If the sole change to an existing system of records is to add a routine use, the agency should either republish the entire system of records notice, a condensed description of the system of records, or a citation to the last full text **Federal Register** publication.

2. A copy in **Federal Register** format of any new exemption rules or changes to published rules (consistent with the provisions of 5 U.S.C. 552a(f),(j), or (k)) that the agency proposes to issue for the new or altered system.

(4) OMB Review. OMB will review reports under 5 U.S.C. 552a(r) and provide comments if appropriate. Agencies may assume that OMB concurs in the Privacy Act aspects of their proposal if OMB has not commented within 40 days from the date the transmittal letter was signed. Agencies should ensure that letters are transmitted expeditiously after they are signed.

(5) Timing of Systems of Records Reports. Agencies may publish system of records and routine use notices as well as proposed exemption rules in the **Federal Register** at the same time that they send the new or altered system report to OMB and Congress. The period for OMB and congressional review and the notice and comment period for routine uses and exemptions will then run concurrently. Note that exemptions must be published as final rules before they are effective.

d. New or Altered Matching Program Report. The Act requires agencies to publish notices in the **Federal Register** describing new or altered matching programs, and to submit reports to OMB, and to Congress. The report must be received at least 40 days prior to the initiation of any matching activity carried out under a new or substantially altered matching program. For renewals of continuing programs, the report must be dated at least 40 days prior to the expiration of any existing matching agreement.

(1) When to Report Altered Matching Programs. Agencies need not report minor changes to matching programs. The term "minor change to a matching program" means a change that does not significantly alter the terms of the agreement under which the program is being carried out. Examples of significant changes include:

(a) Changing the purpose for which the program was established.

(b) Changing the matching population, either by including new categories of record subjects or by greatly increasing the numbers of records matched.

(c) Changing the legal authority covering the matching program.

(d) Changing the source or recipient agencies involved in the matching program.

(2) Contents of New or Altered Matching Program Report. The report for a new or altered matching program has three elements: a transmittal letter, a narrative statement, and supporting documentation that includes a copy of the proposed **Federal Register** notice.

(a) Transmittal Letter. The transmittal letter should be signed by the senior agency official responsible for implementation of the Privacy Act within the agency and should contain the name and telephone number of the individual who can best answer questions about the matching program. The letter should state that a copy of the matching agreement has been distributed to Congress as the Act requires. The letter to OMB may also include a request for waiver of the review time period. (See 4e below.)

(b) Narrative Statement. There is no prescribed format for the narrative statement, but it should be brief. It should make reference, as appropriate, to information in the supporting documentation rather than restating such information. The statement should provide:

1. A description of the purpose of the matching program and the authority under which it is being carried out.

2. A description of the security safeguards used to protect against any unauthorized access or disclosure of records used in the match.

3. If the cost/benefit analysis required by Section (u)(4)(A) indicated an unfavorable ratio or was waived pursuant to OMB guidance, an explanation of the basis on which the agency justifies conducting the match.

(c) Supporting Documentation. Attach the following:

1. A copy of the **Federal Register** notice describing the matching program. The notice must appear in the format prescribed by the Office of the Federal Register's *Document Drafting Handbook*. (See 5b (3).)

2. For the Congressional report only, a copy of the matching agreement.

(3) OMB Review. OMB will review reports under 5 U.S.C. 552a(r) and provide comments if appropriate. Agencies may assume that OMB concurs in the Privacy Act aspects of their proposal if OMB has not commented within 40 days from the date the transmittal letter was signed.

(4) Timing of Matching Program Reports. Agencies should ensure that letters are transmitted expeditiously after they are signed. Agencies may publish matching program notices in the **Federal Register** at the same time that they send the matching program report to OMB and Congress. The period for OMB and congressional review and the notice and comment period will then run concurrently.

e. Expedited Review. The Director, OMB, may grant a waiver of the 40-day review period for either systems of records or matching program reviews. The agency must ask for the waiver in the transmittal letter and demonstrate compelling reasons. When a waiver is granted, the agency is not thereby relieved of any other requirement of the Act. If no waiver is granted, agencies may presume concurrence at the expiration of the 40 day review period if OMB has not commented by that time. Note that OMB cannot waive time periods specifically established by the Act such as the 30 days notice and comment period required for the adoption of a routine use proposal pursuant to Section (b)(3) of the Act.

5. Publication Requirements. The Privacy Act requires agencies to publish notices or rules in the **Federal Register** in the following circumstances: when adopting a new or altered system of records, when adopting a routine use, when adopting an exemption for a system of records, or when proposing to carry out a new or altered matching program. (See paragraph 4c(1) and 4d(1) above on what constitutes an alteration requiring a report to OMB and the Congress.)

a. Publishing New or Altered Systems of Records Notices and Exemption Rules.

(1) Who Publishes. The agency responsible for operating the system of records makes the necessary publication. Publication should be carried out at the departmental or agency level. Even where a system of records is to

be operated exclusively by a component, the department rather than the component should publish the notice. Thus, for example, the Department of the Treasury would publish a system of records notice covering a system operated exclusively by the Internal Revenue Service. Note that if the agency is proposing to exempt the system under Section (j) or (k) of the Act, it must publish a rule in addition to the system of records notice.

(a) Government-wide Systems of Records. Certain agencies publish systems of records containing records for which they have government-wide responsibilities. The records may be located in other agencies, but they are being used under the authority of and in conformance with the rules mandated by the publishing agency. The Office of Personnel Management, for example, has published a number of government-wide systems of records relating to the operation of the government's personnel program. Agencies should not publish systems of records that wholly or partly duplicate existing government-wide systems of records.

(b) Section (m) Contract Provisions. When an agency provides by contract for the operation of a system of records, it should ensure that a system of records notice describing the system has been published. It should also review the notice to ensure that it contains a routine use under Section (e)(4)(D) of the Act permitting disclosure to the contractor and his or her personnel.

(2) When to Publish.

(a) System Notice. The system of records notice must appear in the **Federal Register** before the agency begins to operate the system, e.g., collect and use the information.

(b) Routine Use. A routine use must be published in the **Federal Register** 30 days before the agency discloses records pursuant to its terms. (Note that the addition of a routine use to an existing system of records requires a report to OMB and Congress, and that the review period for this report is 40 days.)

(c) Exemption Rule. A rule exempting a system of records under (j) or (k) or the Act must be established through informal rulemaking pursuant to the Administrative Procedure Act. This process generally requires publication of a proposed rule, a period during which the public may comment, publication of a final rule, and the adoption of the final rule. Agencies may not withhold records under an exemption until these requirements have been met.

(3) Format. Agencies should follow the publication format contained in the Office of the Federal Register's *Document Drafting Handbook* which may be obtained from the Government Printing Office.

b. Publishing Matching Notices.

(1) Who Publishes. Generally, the recipient Federal agency (or the Federal source agency in a match conducted by a nonfederal agency) is responsible for publishing in the **Federal Register** a notice describing the new or altered matching program. However, in large, multi-agency matching programs, where the recipient agency is merely performing the matches, and the benefit accrues to the source agencies, the partners should assign responsibility for compliance with the administrative requirements in a fair and reasonable way. This may mean having the matching agency carry out these requirements for all parties, having one participant designated to do so, or having each source agency do so for its own matching program(s).

(2) Timing. Publication must occur at least 30 days prior to the initiation of any matching activity carried out under a new or substantially altered matching program. For renewals of programs agencies wish to continue past the 30 month period of initial eligibility (i.e., the initial 18 months plus a one year extension), publication must occur at least 30 days prior to the expiration of the existing matching agreement. (But note that a report to OMB and the Congress is also required with a 40 day review period).

(3) Format. The matching notice shall be in the format prescribed by the Office of the Federal Register's Document Drafting Handbook and contain the following information:

(a) The name of the Recipient Agency.

(b) The Name(s) of the Source Agencies.

(c) The beginning and ending dates of the match.

(d) A brief description of the matching program, including its purpose; the legal authorities authorizing its operation; categories of individuals involved; and identification of records used, including name(s) of Privacy Act Systems of records.

(e) The identification, address, and telephone number of a Recipient Agency official who will answer public inquiries about the program.

Appendix II to OMB Circular No. A–130—Cost Accounting, Cost Recovery, and Interagency Sharing of Information Technology Facilities

[The guidance formerly found in Appendix II has been revised and placed in Section 8b. See, Transmittal No. 2, 59 FR 37906. Appendix II has been deleted and is reserved for future topics.]

Appendix III to OMB Circular No. A–130—Security of Federal Automated Information Resources

A. Requirements

1. *Purpose*

This Appendix establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A–123. The Appendix revises procedures formerly contained in Appendix III to OMB Circular No. A–130 (50 FR 52730; December 24, 1985), and incorporates requirements of the Computer Security Act of 1987 (P.L. 100–235) and responsibilities assigned in applicable national security directives.

2. *Definitions*

The term:

a. "Adequate security" means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

b. "Application" means the use of information resources (information and information technology) to satisfy a specific set of user requirements.

c. "General support system" or "system" means an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

d. "Major application" means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

3. *Automated Information Security Programs.* Agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

Each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration and the Office of Personnel Management (OPM). Different or more stringent requirements for securing national security information should be incorporated into agency programs as required by appropriate national security directives. At a minimum, agency programs shall include the following controls in their general support systems and major applications:

a. Controls for general support systems.

(1) *Assign Responsibility for Security.* Assign responsibility for security in each system to an individual knowledgeable in the information technology used in the system and in providing security for such technology.

(2) *System Security Plan.* Plan for adequate security of each general support system as part of the organization's information resources management (IRM) planning process. The security plan shall be consistent

with guidance issued by the National Institute of Standards and Technology (NIST). Independent advice and comment on the security plan shall be solicited prior to the plan's implementation. A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35) and Section 8(b) of this circular. Security plans shall include:

(a) *Rules of the System.* Establish a set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system. The rules shall be based on the needs of the various users of the system. The security required by the rules shall be only as stringent as necessary to provide adequate security for information in the system. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the system. They shall also include appropriate limits on interconnections to other systems and shall define service provision and restoration priorities. Finally, they shall be clear about the consequences of behavior not consistent with the rules.

(b) *Training.* Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise them about available assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system.

(c) *Personnel Controls.* Screen individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause. Such screening shall occur prior to an individual being authorized to bypass controls and periodically thereafter.

(d) *Incident Response Capability.* Ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations, consistent with NIST coordination, and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance.

(e) *Continuity of Support.* Establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system.

(f) *Technical Security.* Ensure that cost-effective security products and techniques are appropriately used within the system.

(g) *System Interconnection.* Obtain written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems. Where connection is authorized, controls shall be established which are consistent with the rules of the system and in accordance with guidance from NIST.

(3) *Review of Security Controls.* Review the security controls in each system when significant modifications are made to the system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system. Depending on the potential risk and magnitude of harm that could occur, consider identifying a deficiency pursuant to OMB Circular No. A–123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act (FMFIA), if there is no assignment of security responsibility, no security plan, or no authorization to process for a system.

(4) *Authorize Processing.* Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system shall be re-authorized at least every three years.

b. Controls for Major Applications.

(1) *Assign Responsibility for Security.* Assign responsibility for security of each major application to a management official knowledgeable in the nature of the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect it. This official shall assure that effective security products and techniques are appropriately used in the application and shall be contacted when a security incident occurs concerning the application.

(2) *Application Security Plan.* Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan shall be consistent with guidance issued by NIST. Advice and comment on the plan shall be solicited from the official responsible for security in the primary system in which the application will operate prior to the plan's implementation. A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act. Application security plans shall include:

(a) *Application Rules.* Establish a set of rules concerning use of and behavior within the application. The rules shall be as stringent as necessary to provide adequate security for the application and the information in it. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the application. In addition, the rules shall be clear about the consequences of behavior not consistent with the rules.

(b) *Specialized Training.* Before allowing individuals access to the application, ensure that all individuals receive specialized training focused on their responsibilities and the application rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application).

(c) *Personnel Security.* Incorporate controls such as separation of duties, least privilege and individual accountability into the application and application rules as appropriate. In cases where such controls cannot adequately protect the application or information in it, screen individuals commensurate with the risk and magnitude of the harm they could cause. Such screening shall be done prior to the individuals' being authorized to access the application and periodically thereafter.

(d) *Contingency Planning.* Establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support.

(e) *Technical Controls.* Ensure that appropriate security controls are specified, designed into, tested, and accepted in the application in accordance with appropriate guidance issued by NIST.

(f) *Information Sharing.* Ensure that information shared from the application is protected appropriately, comparable to the protection provided when information is within the application.

(g) *Public Access Controls.* Where an agency's application promotes or permits public access, additional security controls shall be added to protect the integrity of the application and the confidence the public has in the application. Such controls shall include segregating information made directly accessible to the public from official agency records.

(3) *Review of Application Controls.* Perform an independent review or audit of the security controls in each application at least every three years. Consider identifying a deficiency pursuant to OMB Circular No. A–123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act if there is no assignment of responsibility for security, no security plan, or no authorization to process for the application.

(4) *Authorize Processing.* Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application.

4. *Assignment of Responsibilities*

a. *Department of Commerce.* The Secretary of Commerce shall:

(1) Develop and issue appropriate standards and guidance for the security of sensitive information in Federal computer systems.

(2) Review and update guidelines for training in computer security awareness and accepted computer security practice, with assistance from OPM.

(3) Provide agencies guidance for security planning to assist in their development of application and system security plans.

(4) Provide guidance and assistance, as appropriate, to agencies concerning cost-effective controls when interconnecting with other systems.

(5) Coordinate agency incident response activities to promote sharing of incident response information and related vulnerabilities.

(6) Evaluate new information technologies to assess their security vulnerabilities, with technical assistance from the Department of Defense, and apprise Federal agencies of such vulnerabilities as soon as they are known.

b. *Department of Defense.* The Secretary of Defense shall:

(1) Provide appropriate technical advice and assistance (including work products) to the Department of Commerce.

(2) Assist the Department of Commerce in evaluating the vulnerabilities of emerging information technologies.

c. *Department of Justice.* The Attorney General shall:

(1) Provide appropriate guidance to agencies on legal remedies regarding security incidents and ways to report and work with law enforcement concerning such incidents.

(2) Pursue appropriate legal actions when security incidents occur.

d. *General Services Administration.* The Administrator of General Services shall:

(1) Provide guidance to agencies on addressing security considerations when acquiring automated data processing equipment (as defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949, as amended).

(2) Facilitate the development of contract vehicles for agencies to use in the acquisition of cost-effective security products and services (e.g., back-up services).

(3) Provide appropriate security services to meet the needs of Federal agencies to the extent that such services are cost-effective.

e. *Office of Personnel Management.* The Director of the Office of Personnel Management shall:

(1) Assure that its regulations concerning computer security training for Federal civilian employees are effective.

(2) Assist the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and accepted computer security practice.

f. *Security Policy Board.* The Security Policy Board shall coordinate the activities of the Federal government regarding the security of information technology that processes classified information in accordance with applicable national security directives;

5. *Correction of Deficiencies and Reports*

a. *Correction of Deficiencies.* Agencies shall correct deficiencies which are identified through the reviews of security for systems and major applications described above.

b. *Reports on Deficiencies.* In accordance with OMB Circular No. A–123, "Management Accountability and Control", if a deficiency in controls is judged by the agency head to be material when weighed against other agency deficiencies, it shall be included in the annual FMFIA report. Less significant deficiencies shall be reported and progress on corrective actions tracked at the appropriate agency level.

c. *Summaries of Security Plans.* Agencies shall include a summary of their system security plans and major application plans in the strategic plan required by the Paperwork Reduction Act (44 U.S.C. 3506).

B. Descriptive Information

The following descriptive language is explanatory. It is included to assist in understanding the requirements of the Appendix.

The Appendix re-orients the Federal computer security program to better respond to a rapidly changing technological environment. It establishes government-wide responsibilities for Federal computer security and requires Federal agencies to adopt a minimum set of management controls. These management controls are directed at individual information technology users in order to reflect the distributed nature of today's technology.

For security to be most effective, the controls must be part of day-to-day operations. This is best accomplished by planning for security not as a separate activity, but as an integral part of overall planning.

"Adequate security" is defined as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act.

The Appendix no longer requires the preparation of formal risk analyses. In the past, substantial resources have been expended doing complex analyses of specific risks to systems, with limited tangible benefit in terms of improved security for the systems. Rather than continue to try to precisely measure risk, security efforts are better served by generally assessing risks and taking actions to manage them. While formal risk analyses need not be performed, the need to determine adequate security will require that a risk-based approach be used. This risk assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. Additional guidance on effective risk assessment is available in "An Introduction to Computer Security: The NIST Handbook" (March 16, 1995).

Discussion of the Appendix's Major Provisions. The following discussion is provided to aid reviewers in understanding the changes in emphasis in the Appendix.

Automated Information Security Programs. Agencies are required to establish controls to assure adequate security for all information processed, transmitted, or stored in Federal automated information systems. This Appendix emphasizes management controls affecting individual users of information technology. Technical and operational controls support management controls. To be effective, all must interrelate. For example, authentication of individual users is an important management control, for which password protection is a technical control. However, password protection will only be effective if both a strong technology is employed, and it is managed to assure that it is used correctly.

Four controls are set forth: assigning responsibility for security, security planning, periodic review of security controls, and management authorization. The Appendix requires that these management controls be applied in two areas of management responsibility: one for general support systems and one for major applications.

The terms "general support system" and "major application" were used in OMB Bulletins Nos. 88–16 and 90–08. A general support system is "an interconnected set of information resources under the same direct management control which shares common functionality." Such a system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. Normally, the purpose of a general support system is to provide processing or communications support.

A major application is a use of information and information technology to satisfy a specific set of user requirements that requires special management attention to security due to the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of the information in the application. All applications require some level of security, and adequate security for most of them should be provided by security of the general support systems in which they operate. However, certain applications, because of the nature of the information in them, require special management oversight and should be treated as major. Agencies are expected to exercise management judgement in determining which of their applications are major.

The focus of OMB Bulletins Nos. 88–16 and 90–08 was on identifying and securing both general support systems and applications which contained sensitive information. The Appendix requires the establishment of security controls in all general support systems, under the presumption that all contain some sensitive information, and focuses extra security controls on a limited number of particularly high-risk or major applications.

a. *General Support Systems.* The following controls are required in all general support systems:

(1) *Assign Responsibility for Security.* For each system, an individual should be a focal point for assuring there is adequate security within the system, including ways to prevent, detect, and recover from security problems. That responsibility should be assigned in writing to an individual trained in the technology used in the system and in providing security for such technology, including the management of security controls such as user identification and authentication.

(2) *Security Plan.* The Computer Security Act requires that security plans be developed for all Federal computer systems that contain sensitive information. Given the expansion of distributed processing since passage of the Act, the presumption in the Appendix is that all general support systems contain some sensitive information which requires protection to assure its integrity, availability, or confidentiality, and therefore all systems require security plans.

Previous guidance on security planning was contained in OMB Bulletin No. 90–08. This Appendix supersedes OMB Bulletin 90–08 and expands the coverage of security plans from Bulletin 90–08 to include rules of individual behavior as well as technical security. Consistent with OMB Bulletin 90–08, the Appendix directs NIST to update and expand security planning guidance and issue it as a Federal Information Processing Standard (FIPS). In the interim, agencies should continue to use the Appendix of OMB Bulletin No. 90–08 as guidance for the technical portion of their security plans.

The Appendix continues the requirement that independent advice and comment on the security plan for each system be sought. The intent of this requirement is to improve the plans, foster communication between managers of different systems, and promote the sharing of security expertise.

This Appendix also continues the requirement from the Computer Security Act that summaries of security plans be included in agency strategic information resources management plans. OMB will provide additional guidance about the contents of those strategic plans, pursuant to the Paperwork Reduction Act of 1995.

The following specific security controls should be included in the security plan for a general support system:

(a) *Rules.* An important new requirement for security plans is the establishment of a set of rules of behavior for individual users of each general support system. These rules should clearly delineate responsibilities of and expectations for all individuals with access to the system. They should be consistent with system-specific policy as described in "An Introduction to Computer Security: The NIST Handbook" (March 16, 1995). In addition, they should state the consequences of non-compliance. The rules should be in writing and will form the basis for security awareness and training.

The development of rules for a system must take into consideration the needs of all parties who use the system. Rules should be as stringent as necessary to provide adequate security. Therefore, the acceptable level of risk for the system must be established and should form the basis for determining the rules.

Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, and individual accountability. Often rules should reflect technical security controls in the system. For example, rules regarding password use should be consistent with technical password features in the system. Rules may be enforced through administrative sanctions specifically related to the system (e.g. loss of system privileges) or through more general sanctions as are imposed for violating other rules of conduct. In addition, the rules should specifically address restoration of service as a concern of all users of the system.

(b) *Training.* The Computer Security Act requires Federal agencies to provide for the 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 a Federal computer system within or under the supervision of the Federal agency. This includes contractors as well as employees of the agency. Access provided to members of the public should be constrained by controls in the applications through which access is allowed, and training should be within the context of those controls. The Appendix enforces such mandatory training by requiring its completion prior to granting access to the system. Each new user of a general support system in some sense introduces a risk to all other users. Therefore, each user should be versed in acceptable behavior—the rules of the system—before being allowed to use the system. Training should also inform the individual how to get help in the event of difficulty with using or security of the system.

Training should be tailored to what a user needs to know to use the system securely, given the nature of that use. Training may be presented in stages, for example as more access is granted. In some cases, the training should be in the form of classroom instruction. In other cases, interactive computer sessions or well-written and understandable brochures may be sufficient, depending on the risk and magnitude of harm.

Over time, attention to security tends to dissipate. In addition, changes to a system may necessitate a change in the rules or user procedures. Therefore, individuals should periodically have refresher training to assure that they continue to understand and abide by the applicable rules.

To assist agencies, the Appendix requires NIST, with assistance from the Office of Personnel Management (OPM), to update its existing guidance. It also proposes that OPM assure that its rules for computer security training for Federal civilian employees are effective.

(c) *Personnel Controls.* It has long been recognized that the greatest harm has come from authorized individuals engaged in improper activities, whether intentional or accidental. In every general support system, a number of technical, operational, and management controls are used to prevent and detect harm. Such controls include individual accountability, "least privilege," and separation of duties.

Individual accountability consists of holding someone responsible for his or her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. This may be done, for example, by looking for patterns of behavior by users.

Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job.

Separation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such a control keeps a single individual from subverting a critical process.

Nevertheless, in some instances, individuals may be given the ability to bypass some significant technical and operational controls in order to perform system administration and maintenance functions (e.g., LAN administrators or systems programmers). Screening such individuals in positions of trust will supplement technical, operational, and management controls, particularly where the risk and magnitude of harm is high.

(d) *Incident Response Capability.* Security incidents, whether caused by viruses, hackers, or software bugs, are becoming more common. When faced with a security incident, an agency should be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. To address this concern, agencies should establish formal incident response mechanisms. Awareness and training for individuals with access to the system should include how to use the system's incident response capability.

To be fully effective, incident handling must also include sharing information concerning common vulnerabilities and threats with those in other systems and other agencies. The Appendix directs agencies to effectuate such sharing, and tasks NIST to coordinate those agency activities government-wide.

The Appendix also directs the Department of Justice to provide appropriate guidance on pursuing legal remedies in the case of serious incidents.

(e) *Continuity of Support.* Inevitably, there will be service interruptions. Agency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system. Manual procedures are generally NOT a viable back-up option. When automated support is not available, many functions of the organization will effectively cease. Therefore, it is important to take cost-effective steps to manage any disruption of service.

Decisions on the level of service needed at any particular time and on priorities in service restoration should be made in consultation with the users of the system and incorporated in the system rules. Experience has shown that recovery plans that are periodically tested are substantially more viable than those that are not. Moreover, untested plans may actually create a false sense of security.

(f) *Technical Security.* Agencies should assure that each system appropriately uses effective security products and techniques, consistent with standards and guidance from NIST. Often such techniques will correspond with system rules of behavior, such as in the proper use of password protection.

The Appendix directs NIST to continue to issue computer security guidance to assist agencies in planning for and using technical security products and techniques. Until such guidance is issued, however, the planning guidance included in OMB Bulletin 90–08 can assist in determining techniques for

effective security in a system and in addressing technical controls in the security plan.

(g) *System Interconnection.* In order for a community to effectively manage risk, it must control access to and from other systems. The degree of such control should be established in the rules of the system and all participants should be made aware of any limitations on outside access. Technical controls to accomplish this should be put in place in accordance with guidance issued by NIST.

There are varying degrees of how connected a system is. For example, some systems will choose to isolate themselves, others will restrict access such as allowing only e-mail connections or remote access only with sophisticated authentication, and others will be fully open. The management decision to interconnect should be based on the availability and use of technical and non-technical safeguards and consistent with the acceptable level of risk defined in the system rules.

(3) *Review of Security Controls.* The security of a system will degrade over time, as the technology evolves and as people and procedures change. Reviews should assure that management, operational, personnel, and technical controls are functioning effectively. Security controls may be reviewed by an independent audit or a self review. The type and rigor of review or audit should be commensurate with the acceptable level of risk that is established in the rules for the system and the likelihood of learning useful information to improve security. Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest patches), and penetration testing can assist in the on-going review of different facets of systems. However, these tools are no substitute for a formal management review at least every three years. Indeed, for some high-risk systems with rapidly changing technology, three years will be too long.

Depending upon the risk and magnitude of harm that could result, weaknesses identified during the review of security controls should be reported as deficiencies in accordance with OMB Circular No. A–123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act. In particular, if a basic management control such as assignment of responsibility, a workable security plan, or management authorization are missing, then consideration should be given to identifying a deficiency.

(4) *Authorize Processing.* The authorization of a system to process information, granted by a management official, provides an important quality control (some agencies refer to this authorization as accreditation). By authorizing processing in a system, a manager accepts the risk associated with it. Authorization is not a decision that should be made by the security staff.

Both the security official and the authorizing management official have security responsibilities. In general, the security official is closer to the day-to-day operation of the system and will direct or perform security tasks. The authorizing official will normally have general responsibility for the organization supported by the system.

Management authorization should be based on an assessment of management, operational, and technical controls. Since the security plan establishes the security controls, it should form the basis for the authorization, supplemented by more specific studies as needed. In addition, the periodic review of controls should also contribute to future authorizations. Some agencies perform "certification reviews" of their systems periodically. These formal technical evaluations lead to a management accreditation, or "authorization to process." Such certifications (such as those using the methodology in FIPS Pub 102 "Guideline for Computer Security Certification and Accreditation") can provide useful information to assist management in authorizing a system, particularly when combined with a review of the broad behavioral controls envisioned in the security plan required by the Appendix.

Re-authorization should occur prior to a significant change in processing, but at least every three years. It should be done more often where there is a high risk and potential magnitude of harm.

b. *Controls in Major Applications.* Certain applications require special management attention due to the risk and magnitude of harm that could occur. For such applications, the controls of the support system(s) in which they operate are likely to be insufficient. Therefore, additional controls specific to the application are required. Since the function of applications is the direct manipulation and use of information, controls for securing applications should emphasize protection of information and the way it is manipulated.

(1) *Assign Responsibility for Security.* By definition, major applications are high risk and require special management attention. Major applications usually support a single agency function and often are supported by more than one general support system. It is important, therefore, that an individual be assigned responsibility in writing to assure that the particular application has adequate security. To be effective, this individual should be knowledgeable in the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect the application.

(2) *Application Security Plans.* Security for each major application should be addressed by a security plan specific to the application. The plan should include controls specific to protecting information and should be developed from the application manager's perspective. To assist in assuring its viability, the plan should be provided to the manager of the primary support system which the application uses for advice and comment. This recognizes the critical dependence of the security of major applications on the underlying support systems they use. Summaries of application security plans should be included in strategic information resource management plans in accordance with this Circular.

(a) *Application Rules.* Rules of behavior should be established which delineate the responsibilities and expected behavior of all individuals with access to the application. The rules should state the consequences of inconsistent behavior. Often the rules will be associated with technical controls implemented in the application. Such rules should include, for example, limitations on changing data, searching databases, or divulging information.

(b) *Specialized Training.* Training is required for all individuals given access to the application, including members of the public. It should vary depending on the type of access allowed and the risk that access represents to the security of the application and information in it. This training will be in addition to that required for access to a support system.

(c) *Personnel Security.* For most major applications, management controls such as individual accountability requirements, separation of duties enforced by access controls, or limitations on the processing privileges of individuals, are generally more cost-effective personnel security controls than background screening. Such controls should be implemented as both technical controls and as application rules. For example, technical controls to ensure individual accountability, such as looking for patterns of user behavior, are most effective if users are aware that there is such a technical control. If adequate audit or access controls (through both technical and non-technical methods) cannot be established, then it may be cost-effective to screen personnel, commensurate with the risk and magnitude of harm they could cause. The change in emphasis on screening in the Appendix should not affect background screening deemed necessary because of other duties that an individual may perform.

(d) *Contingency Planning.* Normally the Federal mission supported by a major application is critically dependent on the application. Manual processing is generally NOT a viable back-up option. Managers should plan for how they will perform their mission and/or recover from the loss of existing application support, whether the loss is due to the inability of the application to function or a general support system failure. Experience has demonstrated that testing a contingency plan significantly improves its viability. Indeed, untested plans or plans not tested for a long period of time may create a false sense of ability to recover in a timely manner.

(e) *Technical Controls.* Technical security controls, for example tests to filter invalid entries, should be built into each application. Often these controls will correspond with the rules of behavior for the application. Under the previous Appendix, application security was focused on the process by which sensitive, custom applications were developed. While that process is not addressed in detail in this Appendix, it remains an effective method for assuring that security controls are built into applications. Additionally, the technical security controls defined in OMB Bulletin No. 90–08 will continue, until that guidance is replaced by NIST's security planning guidance.

(f) *Information Sharing.* Assure that information which is shared with Federal

organizations, State and local governments, and the private sector is appropriately protected comparable to the protection provided when the information is within the application. Controls on the information may stay the same or vary when the information is shared with another entity. For example, the primary user of the information may require a high level of availability while the secondary user does not, and can therefore relax some of the controls designed to maintain the availability of the information. At the same time, however, the information shared may require a level of confidentiality that should be extended to the secondary user. This normally requires notification and agreement to protect the information prior to its being shared.

(g) *Public Access Controls.* Permitting public access to a Federal application is an important method of improving information exchange with the public. At the same time, it introduces risks to the Federal application. To mitigate these risks, additional controls should be in place as appropriate. These controls are in addition to controls such as "firewalls" that are put in place for security of the general support system.

In general, it is more difficult to apply conventional controls to public access systems, because many of the users of the system may not be subject to individual accountability policies. In addition, public access systems may be a target for mischief because of their higher visibility and published access methods.

Official records need to be protected against loss or alteration. Official records in electronic form are particularly susceptible since they can be relatively easy to change or destroy. Therefore, official records should be segregated from information made directly accessible to the public. There are different ways to segregate records. Some agencies and organizations are creating dedicated information dissemination systems (such as bulletin boards or World Wide Web servers) to support this function. These systems can be on the outside of secure gateways which protect internal agency records from outside access.

In order to secure applications that allow direct public access, conventional techniques such as least privilege (limiting the processing capability as well as access to data) and integrity assurances (such as checking for viruses, clearly labeling the age of data, or periodically spot checking data) should also be used. Additional guidance on securing public access systems is available from NIST Computer Systems Laboratory Bulletin "Security Issues in Public Access Systems" (May, 1993).

(3) *Review of Application Controls.* At least every three years, an independent review or audit of the security controls for each major application should be performed. Because of the higher risk involved in major applications, the review or audit should be independent of the manager responsible for the application. Such reviews should verify that responsibility for the security of the application has been assigned, that a viable security plan for the application is in place, and that a manager has authorized the processing of the application. A deficiency in any of these controls should be considered a deficiency pursuant to the Federal Manager's Financial Integrity Act and OMB Circular No. A–123, "Management Accountability and Control."

The review envisioned here is different from the system test and certification process required in the current Appendix. That process, however, remains useful for assuring that technical security features are built into custom-developed software applications. While the controls in that process are not specifically called for in this Appendix, they remain in Bulletin No. 90–08, and are recommended in appropriate circumstances as technical controls.

(4) *Authorize Processing.* A major application should be authorized by the management official responsible for the function supported by the application at least every three years, but more often where the risk and magnitude of harm is high. The intent of this requirement is to assure that the senior official whose mission will be adversely affected by security weaknesses in the application periodically assesses and accepts the risk of operating the application. The authorization should be based on the application security plan and any review(s) performed on the application. It should also take into account the risks from the general support systems used by the application.

4. *Assignment of Responsibilities.* The Appendix assigns government-wide responsibilities to agencies that are consistent with their missions and the Computer Security Act.

a. *Department of Commerce.* The Department of Commerce, through NIST, is assigned the following responsibilities consistent with the Computer Security Act.

(1) Develop and issue security standards and guidance.

(2) Review and update, with assistance from OPM, the guidelines for security training issued in 1988 pursuant to the Computer Security Act to assure they are effective.

(3) Replace and update the technical planning guidance in the appendix to OMB Bulletin 90–08 This should include guidance on effective risk-based security absent a formal risk analysis.

(4) Provide agencies with guidance and assistance concerning effective controls for systems when interconnecting with other systems, including the Internet. Such guidance on, for example, so-called "firewalls" is becoming widely available and is critical to agencies as they consider how to interconnect their communications capabilities.

(5) Coordinate agency incident response activities. Coordination of agency incident response activities should address both threats and vulnerabilities as well as improve the ability of the Federal government for rapid and effective cooperation in response to serious security breaches.

(6) Assess security vulnerabilities in new information technologies and apprise Federal agencies of such vulnerabilities. The intent of this new requirement is to help agencies understand the security implications of technology before they purchase and field it. In the past, there have been too many instances where agencies have acquired and implemented technology, then found out about vulnerabilities in the technology and had to retrofit security measures. This activity is intended to help avoid such difficulties in the future.

b. *Department of Defense.* The Department, through the National Security Agency, should provide technical advice and assistance to NIST, including work products such as technical security guidelines, which NIST can draw upon for developing standards and guidelines for protecting sensitive information in Federal computers.

Also, the Department, through the National Security Agency, should assist NIST in evaluating vulnerabilities in emerging technologies. Such vulnerabilities may present a risk to national security information as well as to unclassified information.

c. *Department of Justice.* The Department of Justice should provide appropriate guidance to Federal agencies on legal remedies available to them when serious security incidents occur. Such guidance should include ways to report incidents and cooperate with law enforcement.

In addition, the Department should pursue appropriate legal actions on behalf of the Federal government when serious security incidents occur.

d. *General Services Administration.* The General Services Administration should provide agencies guidance for addressing security considerations when acquiring information technology products or services. This continues the current requirement.

In addition, where cost-effective to do so, GSA should establish government-wide contract vehicles for agencies to use to acquire certain security services. Such vehicles already exist for providing system back-up support and conducting security analyses.

GSA should also provide appropriate security services to assist Federal agencies to the extent that provision of such services is cost-effective. This includes providing, in conjunction with the Department of Defense and the Department of Commerce, appropriate services which support Federal use of the National Information Infrastructure (e.g., use of digital signature technology).

e. *Office of Personnel Management.* In accordance with the Computer Security Act, OPM should review its regulations concerning computer security training and assure that they are effective.

In addition, OPM should assist the Department of Commerce in the review and update of its computer security awareness and training guidelines. OPM worked closely with NIST in developing the current guidelines and should work with NIST in revising those guidelines.

f. *Security Policy Board.* The Security Policy Board is assigned responsibility for national security policy coordination in accordance with the appropriate Presidential directive. This includes policy for the security of information technology used to process classified information.

Circular A–130 and this Appendix do not apply to information technology that supports certain critical national security

missions, as defined in 44 U.S.C. 3502 (9) and 10 U.S.C. 2315. Policy and procedural requirements for the security of national security systems (telecommunications and information systems that contain classified information or that support those critical national security missions (44 U.S.C. 3502 (9) and 10 U.S.C. 2315)) is assigned to the Department of Defense pursuant to Presidential directive. The Circular clarifies that information classified for national security purposes should also be handled in accordance with appropriate national security directives. Where classified information is required to be protected by more stringent security requirements, those requirements should be followed rather than the requirements of this Appendix.

5. *Reports.* The Appendix requires agencies to provide two reports to OMB:

The first is a requirement that agencies report security deficiencies and material weaknesses within their FMFIA reporting mechanisms as defined by OMB Circular No. A–123, "Management Accountability and Control," and take corrective actions in accordance with that directive.

The second, defined by the Computer Security Act, requires that a summary of agency security plans be included in the information resources management plan required by the Paperwork Reduction Act.

Appendix IV to OMB Circular No. A–130—Analysis of Key Sections

1. Purpose

The purpose of this Appendix is to provide a general context and explanation for the contents of the key Sections of the Circular.

2. Background

The Paperwork Reduction Act (PRA) of 1980, Public Law 96–511, as amended by the Paperwork Reduction Act of 1995, Public Law 104–13, codified at Chapter 35 of Title 44 of the United States Code, establishes a broad mandate for agencies to perform their information activities in an efficient, effective, and economical manner. Section 3504 of the Act provides authority to the Director, OMB, to develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information management practices in order to determine their adequacy and efficiency, and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

The Circular implements OMB authority under the PRA with respect to Section 3504(b), general information resources management policy, Section 3504(d), information dissemination, Section 3504(f), records management, Section 3504(g), privacy and security, and Section 3504(h), information technology. The Circular also implements certain provisions of the Privacy Act of 1974 (5 U.S.C. 552a); the Chief Financial Officers Act (31 U.S.C. 3512 et seq.); Sections 111 and 206 of the Federal Property and Administrative Services Act of 1949, as amended (40 U.S.C. 759 and 487, respectively); the Computer Security Act (40 U.S.C. 759 note); the Budget and Accounting Act of 1921 (31 U.S.C. 1 et seq.); and Executive Order No. 12046 of March 27, 1978, and Executive Order No. 12472 of April 3, 1984, Assignment of National Security and Emergency Telecommunications Functions. The Circular complements 5 CFR Part 1320, Controlling Paperwork Burden on the Public, which implements other Sections of the PRA dealing with controlling the reporting and recordkeeping burden placed on the public.

In addition, the Circular revises and consolidates policy and procedures in seven previous OMB directives and rescinds those directives, as follows:

A–3—Government Publications.

A–71—Responsibilities for the Administration and Management of Automatic Data Processing Activities Transmittal Memorandum No. 1 to Circular No. A–71—Security of Federal Automated Information Systems.

A–90—Cooperating with State and Local Governments to Coordinate and Improve Information Systems.

A–108—Responsibilities for the Maintenance of Records about Individuals by Federal Agencies

A–114—Management of Federal Audiovisual Activities

A–121—Cost Accounting, Cost Recovery, and Interagency Sharing of Data Processing Facilities

3. Analysis

Section 6, Definitions. Access and Dissemination. The original Circular No. A–130 distinguished between the terms "access to information" and "dissemination of information" in order to separate statutory requirements from policy considerations. The first term means giving members of the public, at their request, information to which they are entitled by a law such as the FOIA. The latter means actively distributing information to the public at the initiative of the agency. The distinction appeared useful at the time Circular No. A–130 was written, because it allowed OMB to focus discussion on Federal agencies' responsibilities for actively distributing information. However, popular usage and evolving technology have blurred differences between the terms "access" and "dissemination" and readers of the Circular were confused by the distinction. For example, if an agency "disseminates" information via an on-line computer system, one speaks of permitting users to "access" the information, and on-line "access" becomes a form of "dissemination."

Thus, the revision defines only the term "dissemination." Special considerations based on access statutes such as the Privacy Act and the FOIA are explained in context.

Government Information. The definition of "government information" includes information created, collected, processed, disseminated, or disposed of both by and for the Federal Government. This recognizes the increasingly distributed nature of information in electronic environments. Many agencies, in addition to collecting information for government use and for dissemination to the public, require members of the public to maintain information or to disclose it to the public. Sound information resources management dictates that agencies consider the costs and benefits of a full range of alternatives to meet government objectives. In some cases, there is no need for the government actually to collect the information itself, only to assure that it is made publicly available. For example, banks insured by the FDIC must provide statements of financial condition to bank customers on request. Particularly when information is available in electronic form, networks make the physical location of information increasingly irrelevant.

The inclusion of information created, collected, processed, disseminated, or disposed of for the Federal Government in the definition of "government information" does not imply that responsibility for implementing the provisions of the Circular itself extends beyond the executive agencies to other entities. Such an interpretation would be inconsistent with Section 4, Applicability, and with existing law. For example, the courts have held that requests to Federal agencies for release of information under the FOIA do not always extend to those performing information activities under grant or contract to a Federal agency. Similarly, grantees may copyright information where the government may not. Thus the information responsibilities of grantees and contractors are not identical to those of Federal agencies except to the extent that the agencies make them so in the underlying grants or contracts. Similarly, agency information resources management responsibilities do not extend to other entities.

Information Dissemination Product. This notice defines the term "information dissemination product" to include all information that is disseminated by Federal agencies. While the provision of access to on-line databases and search software included on compact disk, read-only memory (CD-ROM) are often called information services rather than products, there is no clear distinction and, moreover, no real difference for policy purposes between the two. Thus, the term "information dissemination product" applies to both products and services, and makes no distinction based on how the information is delivered.

Section 8a(1). Information Management Planning. Parallel to new Section 7, Basic Considerations and Assumptions, Section 8a begins with information resources management planning. Planning is the process of establishing a course of action to achieve desired results with available resources. Planners translate organizational missions into specific goals and, in turn, into measurable objectives.

The PRA introduced the concept of information resources management and the principle of information as an institutional resource which has both value and associated costs. Information resources management is a tool that managers use to achieve agency objectives. Information resources management is successful if it enables managers to achieve agency objectives efficiently and effectively.

Information resources management planning is an integral part of overall mission

planning. Agencies need to plan from the outset for the steps in the information life cycle. When creating or collecting information, agencies must plan how they will process and transmit the information, how they will use it, how they will protect its integrity, what provisions they will make for access to it, whether and how they will disseminate it, how they will store and retrieve it, and finally, how the information will ultimately be disposed of. They must also plan for the effects their actions and programs will have on the public and State and local governments.

The Role of State and Local Governments. OMB made additions at Sections 7a, 7e, and 7j, Basic Considerations and Assumptions, concerning State and local governments, and also in policy statements at Sections 8a(1)(c), (3)(f), (5)(d)(iii), and (8)(e).

State and local governments, and tribal governments, cooperate as major partners with the Federal Government in the collection, processing, and dissemination of information. For example, State governments are the principal collectors and/or producers of information in the areas of health, welfare, education, labor markets, transportation, the environment, and criminal justice.

The States supply the Federal Government with data on aid to families with dependent children; medicare; school enrollments, staffing, and financing; statistics on births, deaths, and infectious diseases; population related data that form the basis for national estimates; employment and labor market data; and data used for census geography. National information resources are greatly enhanced through these major cooperating efforts.

Federal agencies need to be sensitive to the role of State and local governments, and tribal governments, in managing information and in managing information technology. When planning, designing, and carrying out information collections, agencies should systematically consider what effect their activities will have on cities, counties, and States, and take steps to involve these governments as appropriate. Agencies should ensure that their information collections impose the minimum burden and do not duplicate or conflict with local efforts or other Federal agency requirements or mandates. The goal is that Federal agencies routinely integrate State and local government concerns into Federal information resources management practices. This goal is consistent with standards for State and local government review of Federal policies and programs.

Training. Training is particularly important in view of the changing nature of information resources management. Decentralization of information technology has placed the management of automated information and information technology directly in the hands of nearly all agency personnel rather than in the hands of a few employees at centralized facilities. Agencies must plan for incorporating policies and procedures regarding computer security, records management, protection of privacy, and other safeguards into the training of every employee and contractor.

Section 8a(2). Information Collection. The PRA requires that the creation or collection of information be carried out in an efficient, effective, and economical manner. When Federal agencies create or collect information—just as when they perform any other program functions—they consume scarce resources. Such activities must be continually evaluated for their relevance to agency missions.

Agencies must justify the creation or collection of information based on their statutory functions. Policy statement 8a(2) uses the justification standard—"necessary for the proper performance of the functions of the agency"—established by the PRA (44 U.S.C. 3508). Furthermore, the policy statement includes the requirement that the information have practical utility, as defined in the PRA (44 U.S.C. 3502(11)) and elaborated in 5 CFR Part 1320. Practical utility includes such qualities of information as accuracy, adequacy, and reliability. In the case of general purpose statistics or recordkeeping, practical utility means that actual uses can be demonstrated (5 CFR 1320.3(l)). It should be noted that OMB's intent in placing emphasis on reducing unjustified burden in collecting information, an emphasis consistent with the Act, is not to diminish the importance of collecting information whenever agencies have legitimate program reasons for doing so. Rather, the concern is that the burdens imposed should not exceed the benefits to be derived from the information. Moreover, if the same benefit can be obtained by alternative means that impose a lesser burden, that alternative should be adopted.

Section 8a(3). Electronic Information Collection. Section 7l articulates a basic assumption of the Circular that modern information technology can help the government provide better service to the public through improved management of government programs. One potentially useful application of information technology is in the government's collection of information. While some information collections may not be good candidates for electronic techniques, many are. Agencies with major electronic information collection programs have found that automated information collections allow them to meet program objectives more efficiently and effectively. Electronic data interchange (EDI) and related standards for the electronic exchange of information will ease transmission and processing of routine business transaction information such as invoices, purchase orders, price information, bills of lading, health insurance claims, and other common commercial documents. EDI holds similar promise for the routine filing of regulatory information such as tariffs, customs declarations, license applications, tax information, and environmental reports.

Benefits to the public and agencies from electronic information collection appear substantial. Electronic methods of collection reduce paperwork burden, reduce errors, facilitate validation, and provide increased convenience and more timely receipt of benefits.

The policy in Section 8a(3) encourages agencies to explore the use of automated techniques for collection of information, and sets forth conditions conducive to the use of those techniques.

Section 8a(4). Records Management. Section 8a(4) begins with the fundamental requirement for Federal records management, namely, that agencies create and keep adequate and proper documentation of their activities. Federal agencies cannot carry out their missions in a responsible and responsive manner without adequate recordkeeping. Section 7h articulates the basic considerations concerning records management. Policy statements concerning records management are also interwoven throughout Section 8a, particularly in subsections on planning (8a(1)(j)), information dissemination (8a(5)), and safeguards (8a(9)).

Records support the immediate needs of government—administrative, legal, fiscal—and ensure its continuity. Records are essential for protecting the rights and interests of the public, and for monitoring the work of public servants. The government needs records to ensure accountability to the public which includes making the information available to the public.

Each stage of the information life cycle carries with it records management responsibilities. Agencies need to record their plans, carefully document the content and procedures of information collection, ensure proper documentation as a feature of every information system, keep records of dissemination programs, and, finally, ensure that records of permanent value are preserved.

Preserving records for future generations is the archival mission. Advances in technology affect the amount of information that can be created and saved, and the ways this information can be made available. Technological advances can ease the task of records management; however, the rapid pace of change in modern technology makes decisions about the appropriate application of technology critical to records management. Increasingly the records manager must be concerned with preserving valuable electronic records in the context of a constantly changing technological environment.

Records schedules are essential for the appropriate maintenance and disposition of records. Records schedules must be prepared in a timely fashion, implement the General Records Schedules issued by the National Archives and Records Administration, be approved by the Archivist of the United States, and be kept accurate and current. (See 44 U.S.C. 3301 et seq.) The National Archives and Records Administration and the General Services Administration provide guidance and assistance to agencies in implementing records management responsibilities. They also evaluate agencies' records management programs to determine the extent to which they are appropriately implementing their records management responsibilities.

Sections 8a(5) and 8a(6). Information Dissemination Policy. Section 8a(5). Every agency has a responsibility to inform the public within the context of its mission. This responsibility requires that agencies distribute information at the agency's initiative, rather than merely responding when the public requests information.

The FOIA requires each agency to publish in the **Federal Register** current descriptions

of agency organization, where and how the public may obtain information, the general methods and procedural requirements by which agency functions are determined, rules of procedure, descriptions of forms and how to obtain them, substantive regulations, statements of general policy, and revisions to all the foregoing (5 U.S.C. 552(a)(1)). The Privacy Act also requires publication of information concerning "systems of records" which are records retrieved by individual identifier such as name, Social Security Number, or fingerprint. The Government in the Sunshine Act requires agencies to publish meeting announcements (5 U.S.C. 552b (e)(1)). The PRA (44 U.S.C. 3507(a)(2)) and its implementing regulations (5 CFR Part 1320) require agencies to publish notices when they submit information collection requests for OMB approval. The public's right of access to government information under these statutes is balanced against other concerns, such as an individual's right to privacy and protection of the government's deliberative process.

As agencies satisfy these requirements, they provide the public basic information about government activities. Other statutes direct specific agencies to issue specific information dissemination products or to conduct information dissemination programs. Beyond generic and specific statutory requirements, agencies have responsibilities to disseminate information as a necessary part of performing their functions. For some agencies the responsibility is made explicit and sweeping; for example, the Agriculture Department is directed to ". . . diffuse among people of the United States, useful information on subjects connected with agriculture. . . ." (7 U.S.C. 2201) For other agencies, the responsibility may be much more narrowly drawn.

Information dissemination is also a consequence of other agency activities. Agency programs normally include an organized effort to inform the public about the program. Most agencies carry out programs that create or collect information with the explicit or implicit intent that the information will be made public. Disseminating information is in many cases the logical extension of information creation or collection.

In other cases, agencies may have information that is not meant for public dissemination but which may be the subject of requests from the public. When the agency establishes that there is public demand for the information and that it is in the public interest to disseminate the information, the agency may decide to disseminate it automatically.

The policy in Section 8a(5)(d) sets forth several factors for agencies to take into account in conducting their information dissemination programs. First, agencies must balance two goals: maximizing the usefulness of the information to the government and the public, and minimizing the cost to both. Deriving from the basic purposes of the PRA (44 U.S.C. 3501), the two goals are frequently in tension because increasing usefulness usually costs more. Second, Section 8a(5)(d)(ii) requires agencies to conduct information dissemination programs equitably and in a timely manner. The word "equal" was removed from this Section since there may be instances where, for example, an agency determines that its mission includes disseminating information to certain specific groups or members of the public, and the agency determines that user charges will constitute a significant barrier to carrying out this responsibility.

Section 8a(5)(d)(iii), requiring agencies to take advantage of all dissemination channels, recognizes that information reaches the public in many ways. Few persons may read a **Federal Register** notice describing an agency action, but those few may be major secondary disseminators of the information. They may be affiliated with publishers of newspapers, newsletters, periodicals, or books; affiliated with on-line database providers; or specialists in certain information fields. While millions of information users in the public may be affected by the agency's action, only a handful may have direct contact with the agency's own information dissemination products. As a deliberate strategy, therefore, agencies should cooperate with the information's original creators, as well as with secondary disseminators, in order to further information dissemination goals and foster a diversity of information sources. An adjunct responsibility to this strategy is reflected in Section 8a(5)(d)(iv), which directs agencies to assist the public in finding government information. Agencies may accomplish this, for example, by specifying and disseminating "locator" information, including information about content, format, uses and limitations, location, and means of access.

Section 8a(6). Information Dissemination Management System. This Section requires agencies to maintain an information dissemination management system which can ensure the routine performance of certain functions, including the essential functions previously required by Circular No. A–3. Smaller agencies need not establish elaborate formal systems, so long as the heads of the agencies can ensure that the functions are being performed.

Subsection (6)(a) carries over a requirement from OMB Circular No. A–3 that agencies' information dissemination products are to be, in the words of 44 U.S.C. 1108, "necessary in the transaction of the public business required by law of the agency." (Circular No. A–130 uses the expression "necessary for the proper performance of agency functions," which OMB considers to be equivalent to the expression in 44 U.S.C. 1108.) The point is that agencies should determine systematically the need for each information dissemination product.

Section 8a(6)(b) recognizes that to carry out effective information dissemination programs, agencies need knowledge of the marketplace in which their information dissemination products are placed. They need to know what other information dissemination products users have available in order to design the best agency product. As agencies are constrained by finite budgets, when there are several alternatives from which to choose, they should not expend public resources filling needs which have already been met by others in the public or private sector. Agencies have a responsibility not to undermine the existing diversity of information sources.

At the same time, an agency's responsibility to inform the public may be independent of the availability or potential availability of a similar information dissemination product. That is, even when another governmental or private entity has offered an information dissemination product identical or similar to what the agency would produce, the agency may conclude that it nonetheless has a responsibility to disseminate its own product. Agencies should minimize such instances of duplication but could reach such a conclusion because legal considerations require an official government information dissemination product.

Section 8a(6)(c) makes the Circular consistent with current practice (See OMB Bulletins 88–15, 89–15, 90–09, and 91–16), by requiring agencies to establish and maintain inventories of information dissemination products. (These bulletins eliminated annual reporting to OMB of title-by-title listings of publications and the requirement for agencies to obtain OMB approval for each new periodical. Publications are now reviewed as necessary during the normal budget review process.) Inventories help other agencies and the public identify information which is available. This serves both to increase the efficiency of the dissemination function and to avoid unnecessary burdens of duplicative information collections. A corollary, enunciated in Section 8a(6)(d), is that agencies can better serve public information needs by developing finding aids for locating information produced by the agencies. Finally, Section 8a(6)(f) recognizes that there will be situations where agencies may have to take appropriate steps to ensure that members of the public with disabilities whom the agency has a responsibility to inform have a reasonable ability to access the information dissemination products.

Depository Library Program. Sections 8a(6)(g) and (h) pertain to the Federal Depository Library Program. Agencies are to establish procedures to ensure compliance with 44 U.S.C. 1902, which requires that government publications (defined in 44 U.S.C. 1901 and repeated in Section 6 of the Circular) be made available to depository libraries through the Government Printing Office (GPO).

Depository libraries are major partners with the Federal Government in the dissemination of information and contribute significantly to the diversity of information sources available to the public. They provide a mechanism for wide distribution of government information that guarantees basic availability to the public. Executive branch agencies support the depository library program both as a matter of law and on its merits as a means of informing the public about the government. On the other hand, the law places the administration of depository libraries with GPO. Agency responsibility for the depository libraries is limited to supplying government publications through GPO.

Agencies can improve their performance in providing government publications as well as electronic information dissemination products to the depository library program. For example, the proliferation of "desktop publishing" technology in recent years has afforded the opportunity for many agencies to produce their own printed documents. Many such documents may properly belong in the depository libraries but are not sent because they are not printed at GPO. The policy requires agencies to establish management controls to ensure that the appropriate documents reach the GPO for inclusion in the depository library program.

At present, few agencies provide electronic information dissemination products to the depository libraries. At the same time, a small but growing number of information dissemination products are disseminated only in electronic format.

OMB believes that, as a matter of policy, electronic information dissemination products generally should be provided to the depository libraries. Given that production and supply of information dissemination products to the depository libraries is primarily the responsibility of GPO, agencies should provide appropriate electronic information dissemination products to GPO for inclusion in the depository library program.

While cost may be a consideration, agencies should not conclude without investigation that it would be prohibitively expensive to place their electronic information dissemination products in the depository libraries. For electronic information dissemination products other than on-line services, agencies may have the option of having GPO produce the information dissemination product for them, in which case GPO would pay for depository library costs. Agencies should consider this option if it would be a cost effective alternative to the agency making its own arrangements for production of the information dissemination product. Using GPO's services in this manner is voluntary and at the agency's discretion. Agencies could also consider negotiating other terms, such as inviting GPO to participate in agency procurement orders in order to distribute the necessary copies for the depository libraries. With adequate advance planning, agencies should be able to provide electronic information dissemination products to the depository libraries at nominal cost.

In a particular case, substantial cost may be a legitimate reason for not providing an electronic information dissemination product to the depository library program. For example, for an agency with a substantial number of existing titles of electronic information dissemination products, furnishing copies of each to the depository libraries could be prohibitively expensive. In that situation, the agency should endeavor to make available those titles with the greatest general interest, value, and utility to the public. Substantial cost could also be an impediment in the case of some on-line information services where the costs associated with operating centralized databases would make provision of unlimited direct access to numerous users prohibitively expensive. In both cases, agencies should consult with the GPO, in order to identify those information dissemination products with the greatest public interest and utility for dissemination. In all cases, however, where an agency discontinues publication of an information dissemination product in paper format in favor of electronic formats, the agency should work with the GPO to ensure availability of the information dissemination product to depository libraries.

Notice to the Public. Sections 8a(6)(i) and (j) present new practices for agencies to observe in communicating with the public about information dissemination. Among agencies' responsibilities for dissemination is an active knowledge of, and regular consultation with, the users of their information dissemination products. A primary reason for communication with users is to gain their contribution to improving the quality and relevance of government information—how it is created, collected, and disseminated. Consultations with users might include participation at conferences and workshops, careful attention to correspondence and telephone communications (e.g., logging and analyzing inquiries), or formalized user surveys.

A key part of communicating with the public is providing adequate notice of agency information dissemination plans. Because agencies' information dissemination actions affect other agencies as well as the public, agencies must forewarn other agencies of significant actions. The decision to initiate, terminate, or substantially modify the content, form, frequency, or availability of significant products should also trigger appropriate advance public notice. Where appropriate, the Government Printing Office should be notified directly. Information dissemination products deemed not to be significant require no advance notice.

Examples of significant products (or changes to them) might be those that:

(a) Are required by law; e.g., a statutorily mandated report to Congress;

(b) Involve expenditure of substantial funds;

(c) By reason of the nature of the information, are matters of continuing public interest; e.g., a key economic indicator;

(d) By reason of the time value of the information, command public interest; e.g., monthly crop reports on the day of their release;

(e) Will be disseminated in a new format or medium; e.g., disseminating a printed product in electronic medium, or disseminating a machine-readable data file via on-line access.

Where members of the public might consider a proposed new agency product unnecessary or duplicative, the agency should solicit and evaluate public comments. Where users of an agency information dissemination product may be seriously affected by the introduction of a change in medium or format, the agency should notify users and consider their views before instituting the change. Where members of the public consider an existing agency product important and necessary, the agency should consider these views before deciding to terminate the product. In all cases, however, determination of what is a significant information dissemination product and what constitutes adequate notice are matters of agency judgment.

Achieving Compliance with the Circular's Requirements. Section 8a(6)(k) requires that the agency information dissemination management system ensure that, to the extent existing information dissemination policies or practices are inconsistent with the requirements of this Circular, an orderly transition to compliance with the requirements of this Circular is made. For example, some agency information dissemination products may be priced at a level which exceeds the cost of dissemination, or the agency may be engaged in practices which are otherwise unduly restrictive. In these instances, agencies must plan for an orderly transition to the substantive policy requirements of the Circular. The information dissemination management system must be capable of identifying these situations and planning for a reasonably prompt transition. Instances of existing agency practices which cannot immediately be brought into conformance with the requirements of the Circular are to be addressed through the waiver procedures of Section 10(b).

Section 8a(7). Avoiding Improperly Restrictive Practices. Federal agencies are often the sole suppliers of the information they hold. The agencies have either created or collected the information using public funds, usually in furtherance of unique governmental functions, and no one else has it. Hence agencies need to take care that their behavior does not inappropriately constrain public access to government information.

When agencies use private contractors to accomplish dissemination, they must take care that they do not permit contractors to impose restrictions that undercut the agencies' discharge of their information dissemination responsibilities. The contractual terms should assure that, with respect to dissemination, the contractor behaves as though the contractor were the agency. For example, an agency practice of selling, through a contractor, on-line access to a database but refusing to sell copies of the database itself may be improperly restrictive because it precludes the possibility of another firm making the same service available to the public at a lower price. If an agency is willing to provide public access to a database, the agency should be willing to sell copies of the database itself.

By the same reasoning, agencies should behave in an even-handed manner in handling information dissemination products. If an agency is willing to sell a database or database services to some members of the public, the agency should sell the same products under similar terms to other members of the public, unless prohibited by statute. When an agency decides it has public policy reasons for offering different terms of sale to different groups in the public, the agency should provide a clear statement of the policy and its basis.

Agencies should not attempt to exert control over the secondary uses of their

information dissemination products. In particular, agencies should not establish exclusive, restricted, or other distribution arrangements which interfere with timely and equitable availability of information dissemination products, and should not charge fees or royalties for the resale or redissemination of government information. These principles follow from the fact that the law prohibits the Federal Government from exercising copyright.

Agencies should inform the public as to the limitations inherent in the information dissemination product (e.g., possibility of errors, degree of reliability, and validity) so that users are fully aware of the quality and integrity of the information. If circumstances warrant, an agency may wish to establish a procedure by which disseminators of the agency's information may at their option have the data and/or value-added processing checked for accuracy and certified by the agency. Using this method, redisseminators of the data would be able to respond to the demand for integrity from purchasers and users. This approach could be enhanced by the agency using its authority to trademark its information dissemination product, and requiring that redisseminators who wish to use the trademark agree to appropriate integrity procedures. These methods have the possibility of promoting diversity, user responsiveness, and efficiency as well as integrity. However, an agency's responsibility to protect against misuse of a government information dissemination product does not extend to restricting or regulating how the public actually uses the information.

The Lanham Trademark Act of 1946, 15 U.S.C. 1055, 1125, 1127, provides an efficient method to address legitimate agency concerns regarding public safety. Specifically, the Act permits a trademark owner to license the mark, and to demand that the user maintain appropriate quality controls over products reaching consumers under the mark. See generally, McCarthy on Trademarks, Sec. 18.13. When a trademark owner licenses the trademark to another, it may retain the right to control the quality of goods sold under the trademark by the licensee. Furthermore, if a licensee sells goods under the licensed trademark in breach of the licensor's quality specifications, the licensee may be liable for breach of contract as well as for trademark infringement. This technique is increasingly being used to assure the integrity of digital information dissemination products. For example, the Census Bureau has trademarked its topologically integrated geographic encoding and referencing data product ("TIGER/Line"), which is used as official source data for legislative districting and other sensitive applications.

Whenever a need for special quality control procedures is identified, agencies should adopt the least burdensome methods and ensure that the methods chosen do not establish an exclusive, restricted, or other distribution arrangement that interferes with timely and equitable availability of public information to the public. Agencies should not attempt to condition the resale or redissemination of its information dissemination products by members of the public.

User charges. Title 5 of the Independent Offices Appropriations Act of 1952 (31 U.S.C. 9701) establishes Federal policy regarding fees assessed for government services, and for sale or use of government property or resources. OMB Circular No. A–25, User Charges, implements the statute. It provides for charges for government goods and services that convey special benefits to recipients beyond those accruing to the general public. It also establishes that user charges should be set at a level sufficient to recover the full cost of providing the service, resource, or property. Since Circular No. A–25 is silent as to the extent of its application to government information dissemination products, full cost recovery for information dissemination products might be interpreted to include the cost of collecting and processing information rather than just the cost of dissemination. The policy in Section 8a(7)(c) clarifies the policy of Circular No. A–25 as it applies to information dissemination products. This policy was codified by the Paperwork Reduction Act of 1995 at 35 U.S.C. Section 3506(d)(4)(D).

Statutes such as FOIA and the Government in the Sunshine Act establish a broad and general obligation on the part of Federal agencies to make government information available to the public and to avoid erecting barriers that impede public access. User charges higher than the cost of dissemination may be a barrier to public access. The economic benefit to society is maximized when government information is publicly disseminated at the cost of dissemination. Absent statutory requirements to the contrary, the general standard for user charges for government information dissemination products should be to recover no more than the cost of dissemination. It should be noted in this connection that the government has already incurred the costs of creating and processing the information for governmental purposes in order to carry out its mission.

Underpinning this standard is the FOIA fee structure which establishes limits on what agencies can charge for access to Federal records. That Act permits agencies to charge only the direct reasonable cost of search, reproduction and, in certain cases, review of requested records. In the case of FOIA requests for information dissemination products, charges would be limited to reasonable direct reproduction costs alone. No search would be needed to find the product, thus no search fees would be charged. Neither would the record need to be reviewed to determine if it could be withheld under one of the Act's exemptions since the agency has already decided to release it. Thus, FOIA provides an information "safety net" for the public.

While OMB does not intend to prescribe procedures for pricing government information dissemination products, the cost of dissemination may generally be thought of as the sum of all costs specifically associated with preparing a product for dissemination and actually disseminating it to the public. When an agency prepares an information product for its own internal use, costs associated with such production would not generally be recoverable as user charges on subsequent dissemination. When the agency prepares the product for public dissemination, and disseminates it, costs associated with preparation and actual dissemination would be recoverable as user charges.

In the case of government databases which are made available to the public on-line, the costs associated with initial database development, including the costs of the necessary hardware and software, would not be included in the cost of dissemination. Once a decision is made to disseminate the data, additional costs logically associated with dissemination can be included in the user fee. These may include costs associated with modification of the database to make it suitable for dissemination, any hardware or software enhancements necessary for dissemination, and costs associated with providing customer service or telecommunications capacity.

In the case of information disseminated via cd-rom, the costs associated with initial database development would likewise not be included in the cost of dissemination. However, a portion of the costs associated with formatting the data for cd-rom dissemination and the costs of mastering the cd-rom, could logically be included as part of the dissemination cost, as would the cost associated with licensing appropriate search software.

Determining the appropriate user fee is the responsibility of each agency, and involves the exercise of judgment and reliance on reasonable estimates. Agencies should be able to explain how they arrive at user fees which represent average prices and which, given the likely demand for the product, can be expected to recover the costs associated with dissemination.

When agencies provide custom tailored information services to specific individuals or groups, full cost recovery, including the cost of collection and processing, is appropriate. For example, if an agency prepares special tabulations or similar services from its databases in answer to a specific request from the public, all costs associated with fulfilling the request would be charged, and the requester should be so informed before work is begun.

In a few cases, agencies engaging in information collection activities augment the information collection at the request of, and with funds provided by, private sector groups. Since the 1920's, the Bureau of the Census has carried out, on request, surveys of certain industries at greater frequency or at a greater level of detail than Federal funding would permit, because gathering the additional information is consistent with Federal purposes and industry groups have paid the additional information collection and processing costs. While the results of these surveys are disseminated to the public at the cost of dissemination, the existence and availability of the additional government data are special benefits to certain recipients beyond those accruing to the public. It is appropriate that those recipients should bear the full costs of information collection and processing, in addition to the normal costs of dissemination.

Agencies must balance the requirement to establish user charges and the level of fees

charged against other policies, specifically, the proper performance of agency functions and the need to ensure that information dissemination products reach the public for whom they are intended. If an agency mission includes disseminating information to certain specific groups or members of the public and the agency determines that user charges will constitute a significant barrier to carrying out this responsibility, the agency may have grounds for reducing or eliminating its user charges for the information dissemination product, or for exempting some recipients from the charge. Such reductions or eliminations should be the subject of agency determinations on a case by case basis and justified in terms of agency policies.

Section 8a(8). Electronic Information Dissemination. Advances in information technology have changed government information dissemination. Agencies now have available new media and formats for dissemination, including CD-ROM, electronic bulletin boards, and public networks. The growing public acceptance of electronic data interchange (EDI) and similar standards enhances their attractiveness as methods for government information dissemination. For example, experiments with the use of electronic bulletin boards to advertise Federal contracting opportunities and to receive vendor quotes have achieved wider dissemination of information about business opportunities with the Federal Government than has been the case with traditional notices and advertisements. Improved information dissemination has increased the number of firms expressing interest in participating in the government market and decreased prices to the government due to expanded competition. In addition, the development of public electronic information networks, such as the Internet, provides an additional way for agencies to increase the diversity of information sources available to the public. Emerging applications such as Wide Area Information Servers and the World-wide Web (using the NISO Z39.50 standard) will be used increasingly to facilitate dissemination of government information such as environmental data, international trade information, and economic statistics in a networked environment.

A basic purpose of the PRA is to "provide for the dissemination of public information on a timely basis, on equitable terms, and in a manner that promotes the utility of the information to the public and makes effective use of information technology." (44 U.S.C. 3501(7)) Agencies can frequently enhance the value, practical utility, and timeliness of government information as a national resource by disseminating information in electronic media. Electronic collection and dissemination may substantially increase the usefulness of government information dissemination products for three reasons. First, information disseminated electronically is likely to be more timely and accurate because it does not require data re-entry. Second, electronic records often contain more complete and current information because, unlike paper, it is relatively easy to make frequent changes. Finally, because electronic information is more easily manipulated by the user and can be tailored to a wide variety of needs, electronic information dissemination products are more useful to the recipients.

As stated at Section 8a(1)(h), agencies should use voluntary standards and Federal Information Processing Standards to the extent appropriate in order to ensure the most cost effective and widespread dissemination of information in electronic formats.

Agencies can frequently make government information more accessible to the public and enhance the utility of government information as a national resource by disseminating information in electronic media. Agencies generally do not utilize data in raw form, but edit, refine, and organize the data in order to make it more accessible and useful for their own purposes. Information is made more accessible to users by aggregating data into logical groupings, tagging data with descriptive and other identifiers, and developing indexing and retrieval systems to facilitate access to particular data within a larger file. As a general matter, and subject to budgetary, security or legal constraints, agencies should make available such features developed for internal agency use as part of their information dissemination products.

There will also be situations where the agency determines that its mission will be furthered by providing enhancements beyond those needed for its own use, particularly those that will improve the public availability of government information over the long term. In these instances, the agency should evaluate the expected usefulness of the enhanced information in light of its mission, and where appropriate construct partnerships with the private sector to add these elements of value. This approach may be particularly appropriate as part of a strategy to utilize new technology enhancements, such as graphic images, as part of a particular dissemination program.

Section 8a(9). Information Safeguards. The basic premise of this Section is that agencies should provide an appropriate level of protection to government information, given an assessment of the risks associated with its maintenance and use. Among the factors to be considered include meeting the specific requirements of the Privacy Act of 1974 and the Computer Security Act of 1987.

In particular, agencies are to ensure that they meet the requirements of the Privacy Act regarding information retrievable by individual identifier. Such information is to be collected, maintained, and protected so as to preclude intrusion into the privacy of individuals and the unwarranted disclosure of personal information. Individuals must be accorded access and amendment rights to records, as provided in the Privacy Act. To the extent that agencies share information which they have a continuing obligation to protect, agencies should see that appropriate safeguards are instituted. Appendix I prescribes agency procedures for the maintenance of records about individuals, reporting requirements to OMB and Congress, and other special requirements of specific agencies, in accordance with the Privacy Act.

This Section also incorporates the requirement of the Computer Security Act of 1987 that agencies plan to secure their systems commensurate with the risk and magnitude of loss or harm that could result from the loss, misuse, or unauthorized access to information contained in those systems. It includes assuring the integrity, availability, and appropriate confidentiality of information. It also involves protection against the harm that could occur to individuals or entities outside of the Federal Government as well as the harm to the Federal Government. Appendix III prescribes a minimum set of controls to be included in Federal automated information resources security programs and assigns Federal agency responsibilities for the security of automated information resources. The Section also includes limits on collection and sharing of information and procedures to assure the integrity of information as well as requirements to adequately secure the information.

Incorporation of Circular No. A–114. OMB Circular No. A–114, Management of Federal Audiovisual Activities, last revised on March 20, 1985, prescribed policies and procedures to improve Federal audiovisual management. Although OMB has rescinded Circular No. A–114, its essential policies and procedures continue. This revision provides information resources management policies and principles independent of medium, including paper, electronic, or audiovisual. By including the term "audiovisual" in the definition of "information," audiovisual materials are incorporated into all policies of this Circular.

The requirement in Circular No. A–114 that the head of each agency designate an office with responsibility for the management oversight of an agency's audiovisual productions and that an appropriate program for the management of audiovisual productions in conformance with 36 CFR 1232.4 is incorporated into this Circular at Section 9a(10). The requirement that audiovisual activities be obtained consistent with OMB Circular No. A–76 is covered by Sections 8a(1)(d), 8a(5)(d)(i) and 8a(6)(b).

The National Archives and Records Administration will continue to prescribe the records management and archiving practices of agencies with respect to audiovisual productions at 36 CFR 1232.4, "Audiovisual Records Management."

Section 8b. Information Systems and Information Technology Management.

Section 8b(1). Evaluation and Performance Measurement. OMB encourages agencies to stress several types of evaluation in their oversight of information systems. As a first step, agencies must assess the continuing need for the mission function. If the agency determines there is a continuing need for a function, agencies should reevaluate existing work processes prior to creating new or updating existing information systems. Without this analysis, agencies tend to develop information systems that improve the efficiency of traditional paper-based processes which may be no longer needed. The application of information technology presents an opportunity to reevaluate existing organizational structures, work

processes, and ways of interacting with the public to see whether they still efficiently and effectively support the agency's mission.

Benefit-cost analyses provide vital management information on the most efficient allocation of human, financial, and information resources to support agency missions. Agencies should conduct a benefit-cost analysis for each information system to support management decision making to ensure: (a) alignment of the planned information system with the agency's mission needs; (b) acceptability of information system implementation to users inside the Government; (c) accessibility to clientele outside the Government; and (d) realization of projected benefits. When preparing benefit-cost analyses to support investments in information technology, agencies should seek to quantify the improvements in agency performance results through the measurement of program outputs.

The requirement to conduct a benefit-cost analysis need not become a burdensome activity for agencies. The level of detail necessary for such analyses varies greatly and depends on the nature of the proposed investment. Proposed investments in "major information systems" as defined in this Circular require detailed and rigorous analysis. This analysis should not merely serve as budget justification material, but should be part of the ongoing management oversight process to ensure prudent allocation of scarce resources. Proposed investments for information systems that are not considered "major information systems" should be analyzed and documented more informally.

While it is not necessary to create a new benefit-cost analysis at each stage of the information system life cycle, it is useful to refresh these analyses with up-to-date information to ensure the continued viability of an information system prior to and during implementation. Reasons for updating a benefit-cost analysis may include such factors as significant changes in projected costs and benefits, significant changes in information technology capabilities, major changes in requirements (including legislative or regulatory changes), or empirical data based on performance measurement gained through prototype results or pilot experience.

Agencies should also weigh the relative benefits of proposed investments in information technology across the agency. Given the fiscal constraints facing the Federal government in the upcoming years, agencies should fund a portfolio of investments across the agency that maximizes return on investment for the agency as a whole. Agencies should also emphasize those proposed investments that show the greatest probability (i.e., display the lowest financial and operational risk) of achieving anticipated benefits for the organization. OMB and GAO are creating a publication that will provide agencies with reference materials for setting up such evaluation processes.

Agencies should complete a retrospective evaluation of information systems once operational to validate projected savings, changes in practices, and effectiveness in serving affected publics. These post-implementation reviews may also serve as the basis for agency-wide learning about effective management practices.

Section 8b(2). Strategic Information Resources Management (IRM) Planning. Agencies should link to, and to the extent possible, integrate IRM planning with the agency strategic planning required by the Government Performance and Results Act (P.L. 103–62). Such a linkage ensures that agencies apply information resources to programs that support the achievement of agreed-upon mission goals. Additionally, strategic IRM planning by agencies may help avoid automating out-of-date, ineffective, or inefficient procedures and work processes.

Agencies should also devote management attention to operational information resources management planning. This operational IRM planning should provide a one to five year focus to agency IRM activities and projects. Agency operational IRM plans should also provide a listing of the major information systems covered by the management oversight processes described in Section 8b(3). Agency operational planning for IRM should also communicate to the public how the agency's application of information resources might affect them. For the contractor community, this includes articulating the agency's intent to acquire information technology from the private sector. These data should not be considered acquisition sensitive, so that they can be distributed as widely as possible to the vendor community in order to promote competition. Agencies should make these acquisition plans available to the public through government-wide information dissemination mechanisms, including electronic means.

Operational planning should also include initiatives to reduce the burden, including information collection burden, an agency imposes on the public. Too often, for example, agencies require personal visits to government offices during office hours inconvenient to the public. Instead, agencies should plan to use information technology in ways that make the public's dealing with the Federal government as "user-friendly" as possible.

Each year, OMB issues a bulletin requesting copies of agencies' latest strategic IRM plans and annual updates to operational plans for information and information technology.

Section 8b(3). Information Systems Management Oversight. Agencies should consider what constitutes a "major information system" for purposes of this Circular when determining the appropriate level of management attention for an information system. The anticipated dollar size of an information system or a supporting acquisition is only one determinant of the level of management attention an information system requires. Additional criteria to assess include the maturity and stability of the technology under consideration, how well defined user requirements are, the level of stability of program and user requirements, and security concerns.

For instance, certain risky or "cutting-edge" information systems require closer scrutiny and more points of review and evaluation. This is particularly true when an agency uses an evolutionary life cycle strategy that requires a technical and financial evaluation of the project's viability at prototype and pilot testing phases. Projects relying on commercial off-the-shelf technology and applications will generally require less oversight than those using custom-designed software.

While each phase of an information system life cycle may have unique characteristics, the dividing line between the phases may not always be distinct. For instance, both planning and evaluation should continue throughout the information system life cycle. In fact, during any phase, it may be necessary to revisit the previous stages based on new information or changes in the environment in which the system is being developed.

The policy statements in this Circular describe an information system life cycle. It does not, however, make a definitive statement that there must be four versus five phases of a life cycle because the life cycle varies by the nature of the information system. Only two phases are common to all information systems—a beginning and an end. As a result, life cycle management techniques that agencies can use may vary depending on the complexity and risk inherent in the project.

One element of this management oversight policy is the recognition of imbedded and/or parallel life cycles. Within an information system's life cycle there may be other subsidiary life cycles. For instance, most Federal information systems projects include an acquisition of goods and services that have life cycle characteristics. Some projects include software development components, which also have life cycles. Effective management oversight of major information systems requires a recognition of all these various life cycles and an integrated information systems management oversight with the budget and human resource management cycles that exist in the agency.

Section 8b(2) of the Circular underscores the need for agencies to bring an agency-wide perspective to a number of information resources management issues. These issues include policy formulation, planning, management and technical frameworks for using information resources, and management oversight of major information systems. Agencies should also provide for coordinated decision making (Section 8b(3)(f)) in order to bring together the perspectives from across an agency, and outside if appropriate. Such coordination may take place in an agency-wide management or IRM committee. Interested groups typically include functional users, managers of financial and human resources, information resources management specialists, and, as appropriate, the affected public.

Section 8b(4). Use of Information Resources. Agency management of information resources should be guided by management and technical frameworks for agency-wide information and information technology needs. The technical framework should serve as a reference for updates to existing and new information systems. The

management framework should assure the integration of proposed information systems projects into the technical framework in a manner that will ensure progress toward achieving an open systems environment. Agency strategic IRM planning should describe the parameters (e.g., technical standards) of such a technical framework. The management framework should drive operational planning and should describe how the agency intends to use information and information technology consistent with the technical framework.

Agency management and technical frameworks for information resources should address agency strategies to move toward an open systems environment. These strategies should consist of one or multiple profiles (an internally consistent set of standards), based on the current version of the NIST's Application Portability Profile. These profiles should satisfy user requirements, accommodate officially recognized or de facto standards, and promote interoperability, application portability, and scalability by defining interfaces, services, protocols, and data formats favoring the use of nonproprietary specifications.

Agencies should focus on how to better utilize the data they currently collect from the public. Because agencies generally do not share information, the public often must respond to duplicative information collections from various agencies or their components. Sharing of information about individuals should be consistent with the Privacy Act of 1974, as amended, and Appendix I of this Circular.

Services provided by IPSOs to components of their own agency are often perceived to be "free" by the service recipients because their costs are budgeted as an "overhead" charge. Service recipients typically do not pay for IPSO services based on actual usage. Since the services are perceived to be free, there is very little incentive for either the service recipients or the IPSO managers to be watchful for opportunities to improve productivity or to reduce costs. Agencies are encouraged to institute chargeback mechanisms for IPSOs that provide common information processing services across a number of agency components when the resulting economies are expected to exceed the cost of administration.

Section 8b(5). Acquisition of Information Technology. Consistent with the requirements of the Brooks Act and the Paperwork Reduction Act, agencies should acquire information technology to improve service delivery, reduce the cost of Federal program administration, and minimize burden of dealing with the Federal government. Agencies may wish to ask potential offerors to propose different technical solutions and approaches to fulfilling agency mission requirements. Evaluating acquisitions of information technology must assess both the benefits and costs of applying technology to meet such requirements.

The distinction between information system life cycles and acquisition life cycles is important when considering the implications of OMB Circular A–109, Acquisition of Major Systems, to the acquisition of information resources. Circular A–109 presents one strategy for acquiring information technology when:

(i) The agency intends to fund operational tests and demonstrations of system design;

(ii) The risk is high due to the unproven integration of custom designed software and/or hardware components;

(iii) The estimated cost savings or operational improvements from such a demonstration will further improve the return on investment; or

(iv) The agency wants to acquire a solution based on state-of-the-art, unproven technology.

Agencies should comply with OMB Circular A–76, Performance of Commercial Activities, when considering conversion to or from in-house or contract performance.

Agencies should ensure that acquisitions for new information technology comply with GSA regulations concerning information technology accessibility for individuals with disabilities [41 C.F.R. 201–20.103–7].

Section 9a(11). Ombudsman. The senior agency official designated by the head of each agency under 44 U.S.C 3506(a) is charged with carrying out the responsibilities of the agency under the PRA. Agency senior information resources management officials are responsible for ensuring that their agency practices are in compliance with OMB policies. It is envisioned that the agency senior information resources management official will work as an ombudsman to investigate alleged instances of agency failure to adhere to the policies set forth in the Circular and to recommend or take corrective action as appropriate. Agency heads should continue to use existing mechanisms to ensure compliance with laws and policies.

Section 9b. International Relationships. The information policies contained in the PRA and Circular A–130 are based on the premise that government information is a valuable national resource, and that the economic benefits to society are maximized when government information is available in a timely and equitable manner to all. Maximizing the benefits of government information to society depends, in turn, on fostering diversity among the entities involved in disseminating it. These include for-profit and not-for-profit entities, such as information vendors and libraries, as well as State, local and tribal governments. The policies on charging the cost of dissemination and against restrictive practices contained in the PRA and Circular A–130 are aimed at achieving this goal.

Other nations do not necessarily share these values. Although an increasing number are embracing the concept of equitable and unrestricted access to public information—particularly scientific, environmental, and geographic information of great public benefit—other nations are treating their information as a commodity to be "commercialized". Whereas the Copyright Act, 17 U.S.C. 105, has long provided that "[c]opyright protection under this title is not available for any work of the United States Government," some other nations take advantage of their domestic copyright laws that do permit government copyright and assert a monopoly on certain categories of information in order to maximize revenues. Such arrangements tend to preclude other entities from developing markets for the information or otherwise disseminating the information in the public interest.

Thus, Federal agencies involved in international data exchanges are sometimes faced with problems in disseminating data stemming from differing national treatment of government copyright. For example, one country may attempt to condition the sharing of data with a Federal agency on an agreement that the agency will withhold release of the information or otherwise restrict its availability to the public. Since the Freedom of Information Act does not provide a categorical exemption for copyrighted information, and Federal agencies have neither the authority nor capability to enforce restrictions on behalf of other nations, agencies faced with such restrictive conditions lack clear guidance as to how to respond.

The results of the July 1995 Congress of the World Meteorological Organization, which sought to strike a balance of interests in this area, are instructive. Faced with a resolution which would have essentially required member nations to enforce restrictions on certain categories of information for the commercial benefit of other nations, the United States proposed a compromise which was ultimately accepted. The compromise explicitly affirmed the general principle that government meteorological information—like all other scientific, technical and environmental information—should be shared globally without restriction; but recognized that individual nations may in particular cases apply their own domestic copyright and similar laws to prevent what they deem to be unfair or inappropriate competition within their own territories. This compromise leaves open the door for further consultation as to whether the future of government information policy in a global information infrastructure should follow the "open and unrestricted access" model embraced by the United States and a number of other nations, or if it should follow the "government commercialization" model of others.

Accordingly, since the PRA and Circular A–130 are silent as to how agencies should respond to similar situations, we are providing the following suggestions. They are intended to foster globally the open and unrestricted information policy embraced by the United States and like minded nations, while permitting agencies to have access to data provided by foreign governments with restrictive conditions.

Release by a Federal agency of copyrighted information, whether under a FOIA request or otherwise, does not affect any rights the copyright holder might otherwise possess. Accordingly, agencies should inform any concerned foreign governments that their copyright claims may be enforceable under United States law, but that the agency is not authorized to prosecute any such claim on behalf of the foreign government.

Whenever an agency seeks to negotiate an international agreement in which a foreign party seeks to impose restrictive practices on information to be exchanged, the agency

should first coordinate with the State Department. The State Department will work with the agency to develop the least restrictive terms consistent with United States policy, and ensure that those terms receive full interagency clearance through the established process for granting agencies authority to negotiate and conclude international agreements.

Finally, whenever an agency is attending meetings of international or multilateral organizations where restrictive practices are being proposed as binding on member states, the agency should coordinate with the State Department, the Office of Management and Budget, the Office of Science and Technology Policy, or the U.S. Trade Representative, as appropriate, before expressing a position on behalf of the United States.

[FR Doc. 96–3645 Filed 2–16–96; 8:45 am]

BILLING CODE 3110–01–P

Mr. HORN. So we will now move to have the oath since I didn't begin it that way. If you will all stand.

[Witnesses sworn.]

Mr. HORN. The clerk will note all the witnesses affirmed.

And we now go to the agent of the Comptroller General of the United States, which is Joel Willemssen, Director, Accounting and Information Management Division, U.S. General Accounting Office.

Mr. Willemssen.

STATEMENT OF JOEL WILLEMSSEN, DIRECTOR, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY ROBERT DAYCE, DIRECTOR FOR COMPUTER SECURITY ISSUES, GENERAL ACCOUNTING OFFICE

Mr. WILLEMSSEN. Thank you, Mr. Chairman, Ranking Member Turner. Thank you for inviting us to testify today. Accompanying me is Robert Dayce, GAO's Director for Computer Security Issues, and as requested I'll briefly summarize our statement.

Overall GAO and inspector general reviews done over the past year continue to show that Federal agencies have serious and widespread computer security weaknesses. Our analysis of recently issued GAO and inspector general reports revealed significant weaknesses at each of the 24 major Federal agencies. As displayed on the board, these weaknesses were reported in all six major areas of general computer security controls.

For example, in the area of security program management, weaknesses were identified at 21 agencies. Security program management is fundamental to the appropriate selection and effectiveness of the other categories of controls shown on the board. This area covers a range of activities related to understanding risks, selecting and implementing controls appropriate with risk levels, and ensuring the controls, once implemented, continue to operate effectively.

Another critical area where weaknesses have been found at each of the 24 agencies is access controls. Weak controls over access to sensitive data and systems make it possible for a person to inappropriately modify, destroy or disclose data or computer programs. For the other highlighted areas of security controls, we've also found significant weaknesses at most of the agencies in which audit work has been done.

I think it's noteworthy to point out that since our last analysis of issued reports in 1998, the scope of audit work performed has expanded to more fully cover all six major control areas at each agency. Not surprisingly, this has led to the identification of additional areas of weakness. However, this does not necessarily mean that security is getting worse, although it is clear that serious pervasive weaknesses persist. These serious weaknesses present substantial risk to Federal operations, assets and confidentiality.

Because virtually all Federal operations are supported by automated systems and electronic data, the risks are very high, and the breadth of the potential impact is very wide. The risks cover areas as diverse as taxpayer records, law enforcement, national defense, and a wide range of benefit programs.

While a number of factors have distributed to weak Federal information security, I want to emphasize that we believe the key un-

derlying problem is ineffective security program management. With that in mind, we have issued two executive guides that discuss practices that leading organizations have employed to strengthen the effectiveness of their security programs.

In conclusion, the expanded body of audit evidence that has become available shows that important operations at every major Federal agency continue to be at risk as a result of weak controls. Reducing these risks will require agencies to implement fundamental improvements in managing computer security.

Thank you, Mr. Chairman, and I would be pleased to address any questions that you may have.

Mr. HORN. Well, thank you very much. We will have the questions after all the witnesses have made their presentation.

[The prepared statement of Mr. Willemssen follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m. EDT
Monday,
September 11, 2000

COMPUTER SECURITY

Critical Federal Operations and Assets Remain at Risk

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

GAO/T-AIMD-00-314

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our analysis of recent information security audits at federal agencies. As with other large organizations, federal agencies rely extensively on computerized systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, data tampering, fraud, and inappropriate disclosure of confidential information.

The report being released at today's hearing responds to your July 28, 2000, request that we summarize the results of recent information security audits performed by us and by agency inspectors general at 24 major federal departments and agencies.[1] In summarizing these results, I will discuss the pervasive weaknesses that continue since we reported on the results of a similar analysis 2 years ago this month.[2] I will then illustrate the serious risks that these weaknesses pose at selected individual agencies. Finally, I will describe the major common weaknesses that agencies need to address in order to improve their information security programs.

Background

Dramatic increases in computer interconnectivity, especially in use of the Internet, are revolutionizing the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often on a 24-hour-a-day basis; and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of other individuals and groups.

In addition to such benefits, however, this widespread interconnectivity poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support. Telecommunications, power distribution, national defense—including the military's warfighting capability, law enforcement, government services, and emergency services all depend on the security of their computer

[1] *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 6, 2000).

[2] *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998).

operations. The speed and accessibility that create the enormous benefits of the computer age likewise, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. Disruptions caused by recent virus attacks, such as the ILOVEYOU virus this past May and 1999's Melissa virus, have illustrated the potential for damage that such attacks hold.[3] In addition, natural disasters and inadvertent errors by authorized computer users can have devastating consequences if information resources are poorly protected.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the Federal Bureau of Investigation (FBI), terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, or degrade the integrity of and deny access to data. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood that information attacks will threaten vital national interests increases.

Our previous analyses have shown that federal agency systems were not being adequately protected from these threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In September 1996, we reported that serious weaknesses had been found at 10 of the largest 15 federal agencies.[4] In that report we concluded that poor information security was a widespread federal problem with potentially devastating consequences; accordingly, in 1997 and 1999 reports to the Congress, we identified information security as a high-risk issue.[5] In 1998, we analyzed

[3] *Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities* (GAO/T-AIMD-00-181, May 18, 2000). *Information Security: "ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements* (GAO/T-AIMD-00-171, May 10, 2000). *Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data* (GAO/T-AIMD-99-146, April 15, 1999).

[4] *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110, September 24, 1996).

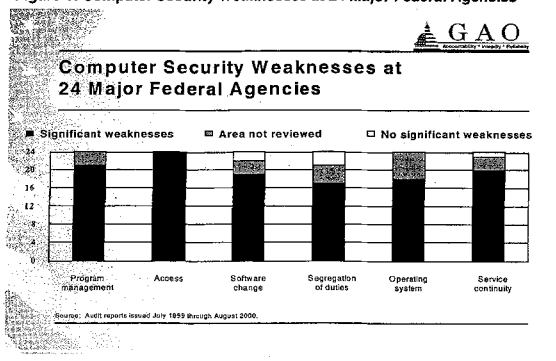
[5] *High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1, 1997). *High-Risk Series: An Update* (GAO/HR-99-1, January 1999).

audit results for 24 of the largest federal agencies: all of them had significant information security weaknesses.[6]

Weaknesses Remain Pervasive

Evaluations published since July 1999 continue to show that federal computer systems are riddled with weaknesses that continue to put critical operations and assets at risk. As in 1998, our current analysis identified significant weaknesses in each of the 24 agencies covered by our review. More areas have been reviewed at more agencies and, as in 1998, weaknesses were reported in all six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These weaknesses placed a broad range of critical operations and assets at risk for fraud, misuse, and disruption. In addition, they placed an enormous amount of highly sensitive data—much of it pertaining to individual taxpayers and beneficiaries—at risk of inappropriate disclosure.

Figure 1: Computer Security Weaknesses at 24 Major Federal Agencies



[6]GAO/AIMD-98-92, September 23, 1998.

Figure 1 illustrates the distribution of weaknesses across the 24 agencies. As in 1998, the most widely audited area, and the area where weaknesses were most often identified, was access controls. Weak controls over access to sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise.

At 21 of the 24 agencies, problems were also identified in the area of security program management—an area that is fundamental to the appropriate selection and effectiveness of the other categories of controls. Security program management covers a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively.

One notable change since September 1998 is that the scope of audit work performed has expanded to more fully cover all six major areas of general controls at each agency. Not surprisingly, this has led to the identification of additional areas of weakness at some agencies. While these increases in reported weaknesses are disturbing, they do not necessarily mean that information security at federal agencies is getting worse. They more likely indicate that information security weaknesses are becoming more fully understood—an important step toward addressing the overall problem. Nevertheless, the numbers leave no doubt that serious, pervasive weaknesses persist. As auditors increase their proficiency and the body of audit evidence expands, it is probable that additional significant deficiencies will be identified.

Most of the audits represented in figure 1 were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at other agencies whose missions are primarily nonfinancial, such as the Departments of Defense and Justice, the audits used to develop the figure may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluating systems supporting nonfinancial operations. In response to congressional interest, during fiscal years 1999 and 2000, we expanded our audit focus to cover a wider range of nonfinancial operations, a trend that is likely to continue.

Risks to Federal Operations, Assets, and Confidentiality Are Substantial

To fully understand the significance of the weaknesses summarized in figure 1, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is extremely high. Examples of the significant risks posed to critical federal operations are described below.

- The Department of the Treasury (which includes the Internal Revenue Service; U.S. Customs Service; Bureau of the Public Debt; Financial Management Service; and Bureau of Alcohol, Tobacco, and Firearms) relies on computer systems to process, collect or disburse, and account for over $1.8 trillion in federal receipts and payments annually. Its computers handle enormous amounts of highly sensitive data associated with taxpayer records, law enforcement operations, and support operations critical to financing the federal government, maintaining the flow of benefits to individuals and organizations, and controlling imports and exports. Although protecting these operations and assets is essential, Treasury's Inspector General (IG) reported in February the absence of effective general controls over computer-based financial systems at certain Treasury components, and that this absence of controls made the department vulnerable to losses, fraud, delays, and interruptions in service.[7]

- The Department of Defense (DOD) relies on a complex computerized information infrastructure to support virtually all aspects of its operations, including strategic and tactical operations, weaponry, intelligence, and security. Evaluations of the security of DOD systems since July 1999 have continued to identify weaknesses that could seriously jeopardize operations and compromise the confidentiality, integrity, or availability of sensitive information. In August 1999, we reported that serious weaknesses in DOD information security continued to provide both hackers as well as hundreds of thousands of authorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DOD data.[8] As a result, numerous DOD functions—including weapons and supercomputer research, logistics, finance, procurement,

[7] *Report on the Department of the Treasury's Fiscal Year 1999 Financial Statements* (OIG-00-056, February 29, 2000).

[8] *DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk* (GAO/AIMD-99-107, August 26, 1999)

personnel management, military health, and payroll—had already been adversely affected by system attacks or fraud. This past May, we testified that the preliminary results of a recent review of the department's financial management systems showed that serious weaknesses in access controls and systems software continued to exist.[9]

- Information technology is essential to the Department of Energy's (DOE) scientific research mission, which is supported by a large and diverse set of computing systems, including very powerful supercomputers located at DOE laboratories across the nation. In June, we reported that computer systems at DOE laboratories supporting civilian research had become a popular target of the hacker community, with the result that the threat of attacks had grown dramatically in recent years.[10] Further, because of security breaches, several laboratories had been forced to temporarily disconnect their networks from the Internet, disrupting the laboratories' ability to do scientific research for up to a full week on at least two occasions.

- In February, the Department of Health and Human Services' (HHS) IG again reported serious control weaknesses affecting the integrity, confidentiality, and availability of data maintained by the department.[11] Most significant were weaknesses associated with the department's Health Care Financing Administration, which was responsible, during fiscal year 1999, for processing health care claims for over 39.5 million beneficiaries and outlays of $299 billion—17.5 percent of total federal outlays.

- The Social Security Administration (SSA) relies on extensive information processing resources to carry out its operations, which for 1999 included payments that totaled $410 billion to more than 50 million beneficiaries, many of whom rely on the uninterrupted flow of monthly payments to meet their basic needs. This represents about 25 percent of the $1.7 trillion in federal expenditures. The agency also issues social security numbers and maintains earnings records and other personal information on virtually all U.S. citizens. The public depends on SSA to protect trust fund revenues and assets from fraud and to protect sensitive information on individuals from inappropriate disclosure. According to SSA, no other

[9] *Department of Defense: Progress in Financial Management Reform* (GAO/T-AIMD/NSIAD-00-163, May 9, 2000)

[10] *Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research* (GAO/AIMD-00-140, June 9, 2000).

[11] *Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 1999*, A-17-99-00002, February 2000.

public program or public-service entity directly touches the lives of so many people.

In November 1999, the IG reported that SSA's systems environment remained threatened by weaknesses in several components of its information protection control structure.[12] According to the IG, until corrected, these weaknesses will continue to increase the risks of unauthorized access to, modification, or disclosure of sensitive SSA information. These, in turn, increase the risks that data or SSA Trust Fund resources could be lost and that the privacy of information associated with SSA's enumeration, earnings, retirement, and disability processes and programs could be compromised. For example, such weaknesses might allow an individual or group to fraudulently obtain payments by creating fictitious beneficiaries or increasing payment amounts. Similarly, an individual or group might secretly obtain sensitive information and sell or otherwise use it for personal gain.

[12] *Social Security Accountability Report for Fiscal Year 1999*, November 18, 1999.

- The Environmental Protection Agency (EPA) relies on its computer systems to collect and maintain a wealth of environmental data under various statutory and regulatory requirements. EPA makes much of its information available to the public through Internet access in order to encourage public awareness and participation in managing human health and environmental risks and to meet statutory requirements. EPA also maintains confidential data from private businesses, data of varying sensitivity on human health and environmental risks, financial and contract data, and personal information on its employees. Consequently, EPA's information security program must accommodate the often competing goals of making much of its environmental information widely accessible while maintaining data integrity, availability, and appropriate confidentiality. In July, we reported serious and pervasive problems that essentially rendered EPA's agencywide information security program ineffective.[13] Our tests of computer-based controls concluded that the computer operating systems and the agencywide computer network that support most of EPA's mission-related and financial operations were riddled with security weaknesses.

  Of particular concern was that many of the most serious weaknesses we identified—those related to inadequate protection from intrusions through the Internet and poor security planning—had been previously reported to EPA management in 1997 by EPA's IG.[14] The negative effects of such weaknesses are illustrated by EPA's own records, which show several serious computer security incidents since early 1998 that have resulted in damage and disruption to agency operations. As a result of these weaknesses, EPA's computer systems and the operations that rely on these systems were highly vulnerable to tampering, disruption, and misuse from both internal and external sources.

- In July the Department of Transportation's (DOT) IG reported that reviews of a financial system and 13 network systems identified a general lack of background checks on contractor personnel and a lack of appropriate background checks on employees throughout DOT.[15] The IG also found that the department's systems were vulnerable to unauthorized access by Internet users. Further, in December 1999, we had reported that DOT's

[13] *Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk* (GAO/AIMD-00-215, July 6, 2000).

[14] *EPA's Internet Connectivity Controls*, Office of Inspector General Report of Audit (Redacted Version), September 5, 1997.

[15] *Interim Report on Computer Security* (FI-2000-108, July 13, 2000).

Federal Aviation Administration was not following sound personnel security practices and, as such, had increased the risk that inappropriate individuals may have gained access to its facilities, information, or resources.[16] For example, no background searches were performed on 36 mainland Chinese nationals who reviewed the source code of eight mission-critical systems.

- The Department of Veterans Affairs (VA) relies on a vast array of computer and telecommunications systems to support its operations and to store sensitive information the department collects in carrying out its mission. Such operations include financial management, health care delivery, and benefits payments. In September 1998, we reported weaknesses that placed the systems that support these operations at risk of misuse and disruption.[17] In October 1999, we reported that VA systems continued to be vulnerable to unauthorized access.[18] These weaknesses placed sensitive information, including financial data and sensitive veteran medical data and benefit information, at increased risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction—possibly occurring without detection.

- In July 1999, we reported that the Department of Agriculture's National Finance Center (NFC) had serious access control weaknesses that affected its ability to prevent or detect unauthorized changes to payroll and other payment data or computer software.[19] NFC is responsible for processing billions of dollars in payroll payments for hundreds of thousands of federal employees and maintaining records for the world's largest 401(k)-type program.

We have made numerous recommendations to the agencies, and in many cases, corrective actions are underway.

[16] *Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software* (GAO/AIMD-00-55, December 23, 1999).

[17] *Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure* (GAO/AIMD-98-175, September 23,1998).

[18] *Information Systems: The Status of Computer Security at the Department of Veterans Affairs* (GAO/AIMD-00-5, October 4,1999).

[19] *USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misus. and Improper Disclosure* (GAO/AIMD-99-227, July 30, 1999).

While Nature of Risk Varies, Control Weaknesses Across Agencies Are Strikingly Similar

The nature of agency operations and the related risks vary. However, striking similarities remain in the specific types of general control weaknesses reported and in their serious negative impact on an agency's ability to ensure the integrity, availability, and appropriate confidentiality of its computerized operations—and therefore on what corrective actions they must take. The sections that follow describe the six areas of general controls that are represented in figure 1—and the specific weaknesses that were most widespread at the agencies covered by our analysis.

Security Program Management

Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks costeffectively, rather than react to individual problems in an ad-hoc manner only after a violation has been detected or an audit finding reported.

Despite the importance of this aspect of an information security program, poor security program management continues to be a widespread problem. Of the 21 agencies for which this aspect of security was reviewed, all had deficiencies. Specifically, many had not developed security plans for major systems based on risk, had not documented security policies, and had not implemented a program for testing and evaluating the effectiveness of the controls they relied on. As a result, agencies

- were not fully aware of the information security risks to their operations,
- had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable,
- had a false sense of security because they were relying on controls that were not effective, and
- could not make informed judgments as to whether they were spending too little or too much of their resources on security.

Access Controls

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure. Access controls include physical protections—such as gates and guards—as well as logical controls, which are controls built into software that require

users to authenticate themselves through the use of secret passwords or other identifiers and limit the files and other resources that an authenticated user can access and the actions that he or she can execute. Without adequate access controls, unauthorized individuals, including outside intruders and terminated employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. Even authorized users can unintentionally modify or delete data or execute changes that are outside their span of authority.

For access controls to be effective, they must be properly implemented and maintained. First, an organization must analyze the responsibilities of individual computer users to determine what type of access (e.g., read, modify, delete) they need to fulfill their responsibilities. Then, specific control techniques, such as specialized access control software, must be implemented to restrict access to these authorized functions. Such software can be used to limit a user's activities associated with specific systems or files and to keep records of individual users' actions on the computer. Finally, access authorizations and related controls must be maintained and adjusted on an ongoing basis to accommodate new and terminated employees, and changes in users' responsibilities and related access needs.

Access controls were evaluated at all 24 of the agencies covered by our analysis, and significant weaknesses were reported for each of the 24, as evidenced by the following examples:

- Accounts and passwords for individuals no longer associated with the agency were not deleted or disabled; neither were they adjusted for those whose responsibilities, and thus need to access certain files, changed. At one agency, as a result, former employees and contractors could and in many cases did still read, modify, copy, or delete data. At this same agency, even after 160 days of inactivity, 7,500 out of 30,000 users' accounts had not been deactivated.
- Users were not required to periodically change their passwords.
- Managers did not precisely identify and document access needs for individual users or groups of users. Instead, they provided overly broad access privileges to very large groups of users. As a result, far more individuals than necessary had the ability to browse and, sometimes, modify or delete sensitive or critical information. At one agency, all 1,100 users were granted access to sensitive system directories and settings. At

another agency, 20,000 users had been provided access to one system without written authorization.

- Use of default, easily guessed, and unencrypted passwords significantly increased the risk of unauthorized access. During testing at one agency, we were able to guess many passwords based on our knowledge of commonly used passwords and were able to observe computer users' keying in passwords and then use those passwords to obtain "high level" system administration privileges.

- Software access controls were improperly implemented, resulting in unintended access or gaps in access-control coverage. At one agency data center, all users, including programmers and computer operators, had the capability to read sensitive production data, increasing the risk that such sensitive information could be disclosed to unauthorized individuals. Also at this agency, certain users had the unrestricted ability to transfer system files across the network, increasing the risk that unauthorized individuals could gain access to the sensitive data or programs.

To illustrate the risks associated with poor authentication and access controls, in recent years we have begun to incorporate penetration testing into our audits of information security. Such tests involve attempting—with agency cooperation—to gain unauthorized access to sensitive files and data by searching for ways to circumvent existing controls, often from remote locations. As we reported in 1998, our auditors have been successful, in almost every test, in readily gaining unauthorized access that would allow intruders to read, modify, or delete data for whatever purpose they had in mind. Further, user activity was inadequately monitored. At one agency, much of the activity associated with our intrusion testing was not recognized and recorded, and the problem reports that were recorded did not recognize the magnitude of our activity or the severity of the security breaches we initiated.

Application Software Development and Change Controls

Application software development and change controls prevent unauthorized software programs or modifications to programs from being implemented. Key aspects of such controls are ensuring that (1) software changes are properly authorized by the managers responsible for the agency program or operations that the application supports, (2) new and modified software programs are tested and approved prior to their implementation, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes and to ensure that different versions are not misidentified.

Such controls can prevent both errors in software programming as well as malicious efforts to insert unauthorized computer program code. Without adequate controls, incompletely tested or unapproved software can result in erroneous data processing that depending on the application, could lead to losses or faulty outcomes. In addition, individuals could surreptitiously modify software programs to include processing steps or features that could later be exploited for personal gain or sabotage.

Weaknesses in software program change controls were identified for 19 of the 21 agencies where such controls were evaluated. Examples of weaknesses in this area included the following:

- Testing procedures were undisciplined and did not ensure that implemented software operated as intended. For example, at one agency, senior officials authorized some systems for processing without testing access controls to ensure that they had been implemented and were operating effectively. At another, documentation was not retained to demonstrate user testing and acceptance.
- Implementation procedures did not ensure that only authorized software was used. In particular, procedures did not ensure that emergency changes were subsequently tested and formally approved for continued use and that implementation of "locally developed" (unauthorized) software programs was prevented or detected.
- Agencies' policies and procedures frequently did not address the maintenance and protection of program libraries.

Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records without detection. For example, one computer programmer should not be allowed to independently write, test, and approve program changes.

Although segregation of duties alone will not ensure that only authorized activities occur, inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes could be implemented, and computer resources could be damaged or destroyed. For example,

- an individual who was independently responsible for authorizing, processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection or

- a computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.

Controls to ensure appropriate segregation of duties consist mainly of documenting, communicating, and enforcing policies on group and individual responsibilities. Enforcement can be accomplished by a combination of physical and logical access controls and by effective supervisory review.

Segregation of duties was evaluated at 20 of the 24 agencies covered by our analysis, and weaknesses were identified at 17 of these agencies. Common problems involved computer programmers and operators who were authorized to perform a variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security features. For example, at one data center, a single individual could independently develop, test, review, and approve software changes for implementation.

Segregation of duties problems were also identified related to transaction processing. For example, at one agency, 11 staff involved with procurement had system access privileges that allowed them to individually request, approve, and record the receipt of purchased items. In addition, 9 of the 11 had system access privileges that allowed them to edit the vendor file, which could result in fictitious vendors being added to the file for fraudulent purposes. For fiscal year 1999, we identified 60 purchases, totaling about $300,000, that were requested, approved, and receipt recorded by the same individual.

Operating System Controls

Operating system software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation. Generally, one set of system software is used to support and control a variety of applications that may run on the same computer hardware. System software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on the system. Some system software can change data and program code on files without leaving an audit trail or can be

used to modify or delete audit trails. Examples of system software include the operating system, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems.

Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs. Also, authorized users of the system may gain unauthorized privileges to conduct unauthorized actions or to circumvent edits and other controls built into application programs. Such weaknesses seriously diminish the reliability of information produced by all of the applications supported by the computer system and increase the risk of fraud, sabotage, and inappropriate disclosures. Further, system software programmers are often more technically proficient than other data processing personnel and, thus, have a greater ability to perform unauthorized actions if controls in this area a weak.

The control concerns for system software are similar to the access control issues and software program change control issues discussed earlier. However, because of the high level of risk associated with system software activities, most entities have a separate set of control procedures that apply to them.

Operating system software controls were covered in audits for 18 of the 24 agencies included in our review. This was double that of 1998, when this important control area had been reviewed for only nine agencies.

Weaknesses were identified at each of the 18 agencies for which operating system controls were reviewed. A common type of problem reported was insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a variety of ways. For example, at one agency, system support personnel had the ability to change data in the system audit log. As a result, they could have engaged in a wide array of inappropriate and unauthorized activity and could have subsequently deleted related segments of the audit log, thus diminishing the likelihood that their actions would be detected.

Service Continuity

Finally, service continuity controls ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. For this reason, an agency should

have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers, as well as the activities performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. If controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information. Controls to ensure service continuity should address the entire range of potential disruptions. These may include relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters that would require reestablishing operations at a remote location.

Service continuity controls include (1) taking steps, such as routinely making backup copies of files, to prevent and minimize potential damage and interruption, (2) developing and documenting a comprehensive contingency plan, and (3) periodically testing the contingency plan and adjusting it as appropriate.

Service continuity controls were evaluated for 21 of the 24 agencies included in our analysis. Of these 21, weaknesses were reported for 20 agencies. Examples of weaknesses included the following:

Plans were incomplete because operations and supporting resources had not been fully analyzed to determine which were the most critical and would need to be resumed as soon as possible should a disruption occur.

Disaster recovery plans were not fully tested to identify their weaknesses. At one agency, periodic walkthroughs or unannounced tests of the disaster recovery plan had not been performed. Conducting these types of tests provides a scenario more likely to be encountered in the event of an actual disaster.

In conclusion, the expanded body of audit evidence that has become available in the past 2 years on the status of federal information security shows that important operations at every major federal agency continue to be at risk as a result of weak information security controls. There are many specific causes of these weaknesses, but an underlying problem is

poor security program management and poor administration of available control techniques. While agencies have taken steps to address problems and many have good remedial efforts underway, audits completed over the past year show that agencies by and large have not implemented the fundamental management practices needed to ensure that their computer-based controls remain effective on an ongoing basis.

The audit reports cited in the report being released today include many recommendations to individual agencies that address the specific weaknesses reported. For this reason, we are making no additional recommendations at this time. However, we have issued two executive guides that discuss practices that leading organizations have employed to strengthen the effectiveness of their security programs. These guides are *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998) and *Information Security Risk Assessment: Practices of Leading Organizations* (GAO/AIMD-00-33, November 1999).

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Subcommittee may have this time.

Contact and Acknowledgments

If you should have any questions about this testimony, please contact me at (202) 512-6253 or Robert Dacey at (202) 512-3317. We can also be reached by e-mail at *willemssenj.aimd@gao.gov* and *daceyr.aimd@gao.gov*, respectively.

(512027)

Ordering Information

Orders by Internet

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

1-800-424-5454 (automated answering system)

Mr. HORN. The next witness is John Gilligan, the Chief Information Officer for the Department of Energy, the cochair for Security, Privacy and Critical Infrastructure Committee of the Chief Information Officers Council. I will give you another minute besides the 5 because you're speaking for the Chief Information Officers Council. Mr. Gilligan, you've prepared a very thorough statement, but we can't obviously get over 25 pages into the record at this point, but it is in the record, but not having been spoken.

So if Mr. Gilligan will proceed.

STATEMENT OF JOHN GILLIGAN, CHIEF INFORMATION OFFICER, DEPARTMENT OF ENERGY, COCHAIR, SECURITY, PRIVACY AND CRITICAL INFRASTRUCTURE COMMITTEE, CHIEF INFORMATION OFFICERS COUNCIL

Mr. GILLIGAN. Thank you, Chairman Horn and Ranking Member Turner. I want to thank you for the opportunity to appear before this subcommittee to address the very important issue of improving security of our Federal information systems. My remarks today will focus on my perspectives as cochair of the CIO Council's Security, Privacy and Critical Infrastructure Committee.

Federal CIOs share the concerns that have been expressed by Members of Congress, senior members in the administration, and the public, that we need to improve the security of our government information systems. Federal CIOs take their responsibility to oversee agency efforts in cybersecurity very seriously. We share the frustration of members of this committee that progress in securing government systems has not been more rapid. Let me assure you that Federal CIOs are not asleep at the wheel. Rather, they are laboring hard to get a handle on one of the Nation's most complex technological and management problems.

Perhaps it is useful to put the difficulty of cybersecurity into perspective. I recall an exchange I had with a military four-star general a few years ago. We were discussing his frustration with the slow progress on an information technology project. This very successful commander with hundreds of thousands of troops under his command was clearly exasperated. He commented to me after we had discussed the project status, "John, after all, this is not rocket science." As I later examined his comment, it became clear that he was right. The problem could not correctly be compared to rocket science where we have literally hundreds of years of experience, including a well-defined set of engineering principles.

Due to the rapid pace of evolution of information technology, we are typically faced with applying information technology solutions that have been in existence for months or, at best, a few years. I submit that the situation is acute for cybersecurity. It is not rocket science. No, many aspects of cybersecurity are indeed much more difficult than rocket science.

When I addressed this committee in March of this year, I stated that the single biggest challenge that I saw for CIOs in cybersecurity was making line management aware that cybersecurity is not just a complex technological issue. At the core cybersecurity is also a complex risk management issue.

Another challenge that I see facing CIOs is helping line management answer the question, "what is adequate security?" Security

experts tell us that no system is impenetrable if network access is provided. However, the collective inexperience of government and industry in applying security to a range of functions including public Web sites, financial data bases, procurement-sensitive data, citizen benefits and corporate-sensitive or government-sensitive research, makes this a hard problem.

The primary focus of the CIO Council efforts in this area has been to help Federal organizations address the question of what is adequate security. The CIO Council has sponsored a Web-based repository for sharing best practices. This repository can be found at http://bsp.cio.gov.

We have developed sample security policies for use by agencies in intrusion reporting and procuring security projects. We have worked to improve governmentwide processes for reporting security incidents and distributing warnings in a rapid fashion. An ongoing effort is to develop a set of benchmark security practices for electronic services.

The Council has also sponsored a number of training and education forums addressing privacy and critical infrastructure protection.

The CIO Council is also leading efforts to establish a governmentwide encryption infrastructure using public key technology called a public key infrastructure [PKI].

An additional CIO Council effort that is particularly relevant to today's hearing is the development of an Information Technology Security Assessment Framework. This effort was initiated about 10 months ago to provide a tool to help guide security efforts within Federal agencies. This framework has been developed largely with the leadership of the National Institute of Standards and Technology and built upon existing policy and guidance from the Office of Management and Budget, the General Accounting Office, and the National Institutes of Standards and Technology.

The framework provides a road map for Federal organizations to guide them in focusing and prioritizing their efforts to improve security. For each of five levels in the framework, a set of activities is defined that should be undertaken to assure a sound and effective security program. The framework reinforces the importance of a solid foundation for an organization security program and is based on sound policy, clearly defined management responsibility, and organizationwide coverage.

The CIO Council has completed a final draft of version one of the Information Technology Security Assessment Framework and hopes to publish this version in October. Following the example of similar efforts by Carnegie Mellon University to develop security frameworks for software and other disciplines, we plan to continue to refine the framework over the upcoming months. With advice and input from GAO, we have started working on enhancements to the framework that would permit organizations to better assess the effectiveness of the security programs that have been documented and implemented.

The final area that I would like to address is the need for stronger funding support from Congress for a small set of cross-government security initiatives that serve as the foundation for governmentwide improvements in cybersecurity. The cochairs of the Secu-

rity, Privacy and Critical Committee of the CIO Council recently sent a letter to all Members of Congress that highlighted our concern in this area. The letter points out that while there is almost $2 billion identified in the administration's fiscal year 2001 budget request for cybersecurity-related items, only a very small portion of this request totaling less than $50 million is requested for these essential governmentwide foundation programs. The efforts of this group include the Federal Computer Incident Response Capability [FEDCIRC], which is managed by GSA and provides alerts and warnings of virus attacks to all Federal agencies.

It has become clear to the CIO Council that these necessary foundation efforts to improve cybersecurity governmentwide are being hampered by a patchwork of funding and oversight structures in both the executive and legislative branches. We cannot hope to achieve robust governmentwide security without these programs. We urge the respective congressional committees who have jurisdiction over these efforts not to view them as politically driven projects, but as essential elements of a governmentwide foundation for cybersecurity. Moreover, we believe that a $50 million investment for these efforts is a very small investment in view of the great leverage that these efforts will provide.

I would like to enter into the record a copy of the letter entitled "Essential Programs for Ensuring Security of the Federal Cyber Infrastructure."

Mr. HORN. Without objection, it will be in the record at this point in your testimony.

Mr. GILLIGAN. It is clear to Federal CIOs that the lack of a single integrated budget for cybersecurity items—these foundation cybersecurity items—keeps these efforts from getting the proper attention that they deserve and makes progress and governmentwide efforts more difficult.

In similar fashion, the efforts of the CIO Council Security Committee and other CIO Council committees continue to be hampered by lack of effective methods to fund these cross-government initiatives that we undertake. The synergistic benefit and opportunity for savings across the government are enormous. However, due to the use of pass-the-hat funding approaches for the CIO Council, for example, funding for the best security practices efforts that was mentioned earlier had to be limited to $200,000 and was received 9 months into the fiscal year. We will not be able to continue to operate and expand this site or undertake other projects with operational demands without an adequate level of funding.

I would suggest that this committee, working with the administration, should examine ways to provide better methods to fund and manage cross-government initiatives in the information technology area. As a taxpayer, I am dismayed by the difficulty of funding these efforts which have the ability to yield tremendous efficiencies. It is an area where our executive and legislative branches are truly failing, unable to leverage the potential of information technology.

In my written testimony, I've included descriptions of efforts within the Department of Energy to improve the security of our many security systems.

In summary, let me again express my appreciation for the opportunity to share my views on the important subject and encourage the committee to continue to support the CIO Council-sponsored efforts, especially the Information Technology Security Assessment Framework.

While our joint challenge to improve cybersecurity may be more difficult than building rockets, chief information officers are committed to rapidly improving the protection afforded to information systems managed by the Federal Government.

This concludes my remarks. Thank you.

[The prepared statement of Mr. Gilligan follows:]

Statement of John M. Gilligan
Chief Information Officer
U.S. Department of Energy
and
Co-Chair
Security, Privacy, and
Critical Infrastructure

Presented to

U.S. House of Representatives
Subcommittee on Government Management,
Information, and Technology

September 11, 2000

INTRODUCTION

Chairman Horn and distinguished members of this committee, I want to thank you for this opportunity to address this committee on the very important issue of improving security of our federal information systems. My remarks today will focus on my perspectives as Co-chair of the Chief Information Officer's (CIO) Council Committee on Security, Privacy and Critical Infrastructure Protection, and as Chief Information Officer of the Department of Energy.

Federal CIOs share the concerns of this Committee, senior members of the Administration, and the public that we need to continue improving the security of our government information systems. Over the past five years, the technological advances in the Internet and commercially available software have produced enormous consumer and organizational benefits have also moved cyber security from the back room to the front lines. When I addressed this Committee in March of this year, I noted that the single biggest challenge for CIOs in cyber security was increasing line management awareness of this issue. The second biggest challenge I see facing CIOs is helping line management answer the question: What is adequate? Security experts tell us that no system is impenetrable if network access is provided. Additionally, the collective inexperience of government and industry in applying security to a range of functions including public web sites, financial databases, procurement-sensitive data, citizen benefits, corporate-sensitive or government-sensitive research makes this a hard problem.

As co-chair of the Security, Privacy, and Critical Infrastructure Committee of the CIO Council, I have primarily focused my efforts in the area on "what is adequate security". We have made great strides in this area by focusing efforts on programs that provide a broad range of security

enhancements to existing policy and guidance. The Council has sponsored a web-based repository for sharing security best practices. We have developed sample security policies for use by agencies for intrusion reporting and procuring security products. An ongoing effort is to develop a set of benchmark security practices for common electronic services. The Council is also leading efforts to establish a government-wide encryption infrastructure using public key technology that will ensure confidentiality of government information as well as support digital signatures and strong authentication.

An additional CIO Council effort that is particularly relevant to today's hearing is the development of an Information Technology Security Assessment Framework. This effort was initiated about ten months ago to provide a tool to help guide security efforts within Federal agencies. The framework has been developed largely with the leadership of the National Institute of Standards and Technology (NIST) building upon existing policy and guidance from the Office of Management and Budget (OMB) and the General Accounting Office (GAO). We have completed a final draft of Version I of the Information Technology Framework, and we anticipate final release by October 31, 2000. The CIO Council recommends that the Committee adopt this version of the Framework as a common tool for use by the Executive and Legislative branches.

Another area I would like to address is the need for strong support for funding a set of cross-government security initiatives that serve as the foundation for agency cyber security efforts. The co-chairs of the Security Privacy and Critical Infrastructure Committee of the CIO Council recently sent a letter to all Members of Congress that highlighted this concern. The letter highlights that of the almost $2 billion identified in the Administration's Fiscal Year 2001 budget

request for cyber security related items, only about $50 million is requested for government-wide foundation programs. It is clear to Federal CIOs that the lack of a single integrated budget for these foundation cyber security items has made it difficult to give these efforts the proper attention they deserve. Likewise, the efforts of the CIO Council continued to be hampered by the lack of an effective method to fund the cross-government initiatives that we undertake. I have enclosed a copy of the letter (Attachment I) at the end of this testimony.

ACTIVITIES OF THE CIO COUNCIL

The Federal Chief Information Officer's Council has undertaken a number of activities over the past eighteen months that have government-wide implications in improving cyber security of Federal agencies. Key among these efforts are projects to provide federal agencies with the mechanisms to better manage their cyber security programs by developing a web-based repository to share security best practices and a framework to assess the current state of their cyber security program.

Best Security Practices Web Repository

The need for widespread use of best security practices is acknowledged among government departments and agencies. A series of GAO audits and widely reported penetrations of government networks has highlighted the need for a focused effort to collect, document, and disseminate solution sets.

Since this effort has been consistently lacking in the past, the CIO Council, in conjunction with the U.S. Agency for International Development and the Computer Sciences Corporation, has sponsored an initiative to fill the security knowledge gap between professional classroom training and ad hoc electronic bulletin board discussion threads. Providing a structured capability for all Federal IT professionals to share first-hand information regarding their security implementation experiences will do this. The initiative CIO Council's Best Security Practices initiative includes the development of a website (http://bsp.cio.gov) that will collect, document and disseminate solutions sets for IT security professionals. The site allows users to obtain information relevant to their needs. The types of information received from the repository are widespread and include artifacts such as checklists, briefings, and policies. By using these Best Security Practices (BSPs), an agency can reduce the cost of developing their own program, improve the speed of implementation, and increase the quality of security solutions across their agency.

The CIO Council is currently populating the site with Best Security Practices from each agency. I personally drafted a memorandum to my colleagues on the Council encouraging their support by submitting BSPs to the repository. The goal of the Committee is to populate the repository with 100 plus BSPs by mid 2001.

Securing Electronic Government Services to the Public

Over the past year, the government has continued to create electronic government services, changing the way citizens and companies interact with government. A major issue that has been

identified with the implementation of electronic government services is information security, including the validity, reliability and privacy of both stored and transmitted information.

In light of this issue, my colleagues and I on the Committee have partnered with the Chief Financial Officers Council and the Information Technology Association of America to develop a guideline that identifies security solutions that enable delivery of services while ensuring adequate security in a risk balanced implementation.

On May 31, 2000, we invited representatives from government and industry to discuss security benchmarks that Federal agencies can use when implementing electronic government services. More specifically, we discussed cyber security in the context of three electronic government services—web-based information services, government and industry procurement, and financial transactions to the public. This meeting is the first in what will likely become a series of discussions between government and industry to develop a resource guide for Chief Information Officers (CIOs) as they champion electronic government initiatives within their departments and agencies. We expect to release Version 1 of the guideline by December 31, 2000.

Sample Policies and Guidelines for Information Security and Privacy

In my role as CIO of the Department of Energy, I have found it extremely helpful to use guidelines and policies that have been endorsed or used by other agencies. At the same time, I noticed there was a deficiency in the process to disseminate these policies and guidelines and no widely accepted process for distributing good sound policies and guidance from other agencies. The Security, Privacy and Critical Infrastructure Committee has formed a Sample Policy

Working Group to identify policies and guidance that would provide assistance to federal agencies in their efforts to secure their government systems.

The working group reviews policies and recommends some as best practices to be used by other agencies. The best practice is then distributed to the rest of the council members to ensure awareness of the practice, which in turn largely eliminates duplication among agencies in certain areas of cyber security. Over the last several months, the group has identified two policies listed below and has recommended that they be used by the rest of the Federal government:

- *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products.* This document provides guidelines for Federal organizations' acquisition and use of security-related Information Technology products.

- *Model Information Technology Privacy Impact Assessment.* The Internal Revenue Service's (IRS) "Privacy Impact Assessment" has been deemed by the Council as a best practice for evaluating privacy needs and risks on information systems, especially new or upgraded systems. The IRS model is particularly relevant since it is designed to evaluate privacy needs on information systems that contain personal and financial data on virtually every taxpaying resident with extremely rigorous privacy requirements. This is also helpful to agencies because it is now required prior to the development of a new system.

Information Technology Security Assessment Framework

In partnership with NIST, the CIO Council has also developed the Information Technology (IT) Security Assessment Framework to assist managers in their quest for achieving effective cyber security management. The Framework provides the means for Federal organizations to evaluate the state of their security program and to establish a target for improvement where necessary. The Committee has completed version 1 of the Framework. Continuing efforts on the IT Security Assessment Framework will be to develop a companion document that will more explicitly define methods for measuring the effectiveness of the controls for each of the five levels in the Framework. Toward this objective, measures are being developed leveraging parallel work done by Citigroup, a leader in corporate information security. The Council anticipates release of Version 1 by October 31, 2000. The CIO Council recommends that all Federal organizations target achievement of Level 2 of the Framework within the near future.

Funding

Historically, individual agencies developed their own respective cyber security programs to protect their critical information assets. However, there are also several multi-agency initiatives that have been funded to improve cyber security efforts across government. These cross-government efforts have become even more important in today's environment of increased system interconnectivity. Without such efforts, agencies may not have the mechanisms in place to effectively coordinate their cyber security efforts. In the Administration's Fiscal Year 2001 request, federal agencies have requested approximately $2 billion to fund cyber security efforts. Most of this funding has been requested to provide necessary security for individual agencies. Only a small portion of this funding request is intended to provide for cross-government initiatives. These government-wide initiatives provide the necessary foundation for coordinating

government-wide security efforts as well as providing common solutions that will improve efficiency and effectiveness of individual agency security programs.

While there has been significant progress in improving government cyber security, it has become clear that the set of foundation government-wide efforts to improve cyber security are being hampered by a patchwork of funding and oversight structures in both the Executive and Legislative branches. In particular, these cross-government efforts are budgeted for by several agencies, and funding and oversight is likewise provided by a number of congressional committees. Federal CIOs view these programs as critical to our ability to create effective information security programs within individual agencies. Moreover, we are increasingly concerned that the collective visibility of these efforts is being lost. As a result, we are increasing our efforts to ensure oversight of these essential programs and to encourage budget support from Congress.

In a letter delivered to each congressional office last week, the co-chairs of the Security, Privacy and Critical Infrastructure Committee summarized the foundation security programs we believe comprise the essential foundation supporting government wide efforts to provide secure operation of cyber systems. These programs total $48.3 million in the Administration's FY 2001 budget request. I encourage your support for these programs and will continue to ensure oversight from the Council.

Outreach

Over the last year, the Security, Privacy and Critical Infrastructure Committee has responded to the need for government outreach and awareness. The Committee has sponsored a number of activities including conferences, newsletters, and speaking engagements almost on a weekly basis. In addition, the Committee created a website to promote the activities of the Committee and intend to continue with this effort. Specifically, we have sponsored Critical Infrastructure Awareness Day, Hacker Awareness Day, and co-sponsored Defending Cyberspace '99 and the National Information Systems Security Conference.

In conjunction with NIST, the Committee is publishing a bi-monthly newsletter targeted at senior executives in the Federal Government. The newsletter is intended to increase awareness of cyber security trends and issues among the U.S. Government's senior level CIOs and executives. The newsletter highlights cyber security issues and covers articles outlining current trends, issues, and topics of interest.

Public Key Infrastructure

The Council is also leading efforts to establish a government-wide encryption infrastructure using public key technology that will ensure confidentiality of government information as well as support digital signatures and strong authentication. In the spring of this year, the CIO Council adopted the efforts of the Federal Public Key Infrastructure (PKI) Steering Committee. The Steering Committee is working closely with the CIO Council Committees on Architecture and Security, Privacy, and Critical Infrastructure.

The PKI Steering Committee has requested FY 2001 funding to support the implementation of a capability called the Federal Bridge Certification Authority, which supports peer-to-peer agency PKI interoperability. A prototype bridge has been successfully demonstrated to work in a test environment. The requested funding will not only implement this capability on a production level, but will also assist agencies that use it to interoperate, thus helping agencies electronically enable their transactions in an efficient fashion and facilitating compliance with the mandates of the Government Paperwork Elimination Act.

DOE CYBER SECURITY INITIATIVES

During the past eighteen months, the Department of Energy (DOE) has completely restructured its cyber security program. DOE has focused on improving awareness of cyber security threats and installing improved security controls across the DOE complex. I have seen enormous progress in how information is protected and a significant increase in awareness of cyber security issues at all levels within the Department. While we have worked this issue aggressively, cyber security is not a quick fix and more needs to be done. However, the security protection in the Department is improving rapidly, and I appreciate the opportunity to discuss our progress.

In spring 1999, Secretary Bill Richardson announced a comprehensive plan for sweeping security reform, including a restructuring and increased focus on cyber security Department-wide. DOE developed and documented a multilevel management and oversight process for cyber security. The Office of the Chief Information Officer (CIO) is responsible for cyber security policy development and overall supervision of the Department's cyber security program. Line management organizations, including Headquarters Program Secretarial Offices and

Intermediate Offices (Operations and Field), are responsible for monitoring organization implementation of policy, ensuring adequate resources are applied to cyber security, and accepting residual risks through organizational Cyber Security Program Plans.

The Secretary of Energy also established a direct reporting relationship with the Office of Independent Oversight and Performance Assurance (Independent Oversight) to evaluate the effectiveness of line management implementation of Departmental security policy. Independent Oversight maintains a robust vulnerability and penetration testing capability and conducts comprehensive cyber security assessments that include performance testing and programmatic evaluations.

Assuming responsibility for cyber security initiatives that reach all Departmental employees, the Office of the CIO initiated an aggressive plan for restructuring the classified and unclassified computer security programs and implementing a corporate approach to cyber security as part of Departmental organizational management. Continued substantial improvements in the Department commitment to cyber security can occur only when all Federal and contractor employees consistently interact with and are accountable to the cyber security program.

Specific actions taken by DOE since the spring of 1999 to improve the level of cyber security include the following:

- Creating a single, Department-wide Cyber Security Office under me as the Department's Chief Information Officer.
- Requiring work "stand downs" at all sites to conduct security awareness training.

- Developing and issuing four new cyber security policies and three new cyber security guidelines.
- Instituting a set of cyber security metrics, which permit us to evaluate progress at each site.
- Doubling the size and increasing the role of the DOE's security incident and early warning capability located at our Computer Incident Advisory Capability (CIAC) at Lawrence Livermore National Laboratory in California.
- Having each DOE site develop a detailed, site-specific cyber security program plan (CSPP) describing the implementation of cyber security protection at the site.
- Deploying a department-wide cyber security training program to improve the security skills of our Systems Administrators and a separate training course provided to line managers.
- Significantly upgrading DOE site cyber security protection through the expanded use of firewalls and intrusion detection software, stronger passwords, improved system configuration controls, and reconfiguration of system and network connectivity to reduce vulnerabilities.
- Creating a proactive independent security assessment organization, the Office of Independent Oversight and Performance Assurance, that reports directly to the Secretary to conduct independent reviews of security throughout the complex.
- Establishing cyber security Policy and Technical Working Groups to assist in the formulation of policy and guidance as well as to provide technical advice to my office.

Cyber security policies and guidelines

Since July 1999, the Department of Energy has developed and implemented four policies and three guidelines, completely revising previous guidance on unclassified cyber security. Those policies include:

- Use of Warning Banners on Departmental Computer Systems (June 17, 1999)
- Unclassified Cyber Security Program (DOE Notice 205.1, July 26, 1999)
- Foreign National Access To DOE Cyber Systems (DOE Notice 205.2, November 1, 1999)
- Password Generation, Protection, and Use (DOE Notice 205.3, November 23, 1999)

These guidelines include:

- Guidelines on Developing Cyber Security Program Plans
- Password Guide (DOE Guide 205.3-1, November 23, 1999)
- Cyber Security Architecture Guide (July 27, 2000)

We have also posted these policies and guidelines at http://cio.doe.gov/ for easy reference.

Cyber security metrics

A cyber security metrics program was initiated earlier this year to measure progress at each DOE site and to focus management attention on problem areas. Two sets of metrics data have been collected: site reporting of security incidents and site compliance with DOE policy. The Department is in the process of reevaluating its current metrics program to enhance data collection efforts and to better report on the effectiveness of its cyber security program.

Department-wide security incident and early warning capability

DOE N 205.1, Unclassified Cyber Security Program, issued July 26, 1999, requires DOE sites to report significant cyber security incidents to the Department of Energy's Computer Incident Advisory Capability (CIAC). As the DOE's central reporting capability, CIAC is responsible for tracking and analyzing the reports it receives, looking for trends, patterns, and any other events of concern. Each DOE organization is required to provide 24-hour-a-day, 7-day-a-week coverage for incident reporting. DOE policy also requires that DOE organizations specify in their site security plans (i.e., CSPP) the type of events that require monitoring, the "enclaves" and systems subject to monitoring, how the 24x7 monitoring is handled, and the composition of the organization incident response team. In addition, CIAC will provide security incident information to the National Infrastructure Protection Center, the DOE Office of Counterintelligence, and the Federal Computer Incident Reporting Capability/Federal Intrusion Detection Network (FedCIRC/FIDNET), as necessary..

Site-specific cyber security plan

DOE Notice 205.1 requires departmental elements to prepare site cyber security program plans (CSPP) and update these plans at least every two years. Each site has developed a detailed CSPP to describe the implementation of these new policies and guidelines. As of September 11, 2000, 81 site plans have been prepared and reviewed by the CIO, as required by DOE policy. In addition, DOE Notice 205.1 recommends that sites prepare individual plans for major applications. However, these plans for major applications are not centrally reviewed at present.

The Department also has a department-wide plan, entitled Cyber Security Action Plan, dated August 1999, that describes major elements of the cyber security program and timelines. This Action Plan is currently under revision, and its expected publication date is September 30, 2000.

Department-wide cyber security training program

The Department completed a rapid training program to improve the security skills of its System Administrators, with over 2,000 System Administrators trained as of May 15, 2000. A separate cyber security training course was provided to line managers.

Additional cyber security training is being extended to cover all DOE personnel, including users, line managers, senior managers, and technical personnel over the next several months.

Site specific cyber security protection upgrades

Firewalls have been implemented or enhanced at all DOE sites. DOE's Security Architecture Guideline requires application-level protection, including firewalls.

On July 27, 2000, the Department issued draft guidance on cyber security architecture, which further emphasizes risk-based management. This guide supplements DOE Notice 205.1 and provides a common framework for DOE sites to tailor their cyber security program to the unique mission and technology environments at each site. The architecture requires each organization to manage risk by assessing impacts to business operations and implementing effective controls

consistent with the cyber security architecture guidelines and commensurate with the assessed level of risk.

Establishment of the Office of Independent Oversight and Performance Assurance

In May 1999, a proactive independent security assessment organization was established—the Office of Independent Oversight and Performance Assurance—reporting directly to the Secretary. For the past year, this Office has been conducting thorough reviews of cyber security effectiveness at DOE sites with emphasis on major applications with the greatest risk. This Office assesses each site at least every 18 months.

Cyber Security Policy and Technical Working Groups

Since the spring of 1999, all DOE cyber security policies have been developed through extensive Department-wide coordination and consultation. DOE Notice 205.1, dated July 26,1999, formalized this coordination and consultation process by chartering the (cyber security) Policy Working Group (PWG) and the Technical Working Group (TWG). These groups include representation from DOE Laboratories and Program Offices and have been specifically formed to assist in the formulation of policy and guidance as well as to provide technical advice to the CIO. The groups were formed in January 2000. To date, the PWG has met three times, and the TWG has met twice. The Department believes that the two groups are providing an effective collaborative means to develop official policy and guidance leveraging the extensive expertise in the DOE Laboratories.

DOE Actions to Improve Classified Cyber Security

In addition to the items discussed above, the Department of Energy has taken specific steps to improve the level of classified cyber security across the Department. On May 7, 1999, the Secretary of Energy issued a nine Action Item plan for the three weapons laboratories (Lawrence Livermore National Laboratory, Los Alamos National Laboratory, and Sandia National Laboratory). The nine items are as follows:

1. Within seven days of issuance of the Action Item plan, each weapon laboratory scheduled a suspension of all classified personal computers to allow professional and administrative staff who normally uses those computers to attend training and review sessions in computer and information security policies and procedures.

2. On a continuing basis, each laboratory instituted an aggressive computer security training and threat awareness education process for all personnel who use classified computers.

3. Each laboratory implemented processes that made it physically impossible for classified information to be moved within a single work area from a classified computer to an unclassified computer by the transfer of removable media.

4. Each laboratory put into place rigorous new procedures governing the authorized transfer of unclassified files from classified computers.

5. Each laboratory established a process to audit unclassified computer systems to insure compliance with procedures for control of sensitive information and put in place automated sniffing and monitoring programs that continuously scan for classified content in unclassified storage archives and outgoing e-mail.
6. Each Lab developed processes to more stringently apply need-to-know criteria to classified data archives, to institute automated means to monitor and enforce access policies, and to deter and detect any violations.
7. On a continuing basis, each Lab began technical measures to increase the security of its classified networks against insider threats.
8. Each Lab rapidly implemented a three-level network protection program ("green, blue, classified").
9. Each Lab instituted continuing vulnerability analyses, including the use of red teams and senior security policy boards.

The Department is continuing to improve security for our sensitive, classified systems. Preliminary plans have been developed to dramatically improve the technology used to provide protection within our classified systems. A detailed plan will be provided to Congress in January 2001 that will outlines the Department's specific recommendations in this area. In the interim, the Department of Energy is in the process of implementing the following policies:

- The standard workstation configuration for classified data processing will be media-less or physically housed in a protective enclosure;
- Classified data processing on laptops is not allowed, and

- All exceptions to the policy must be documented and approved by a site Designated Approving Authority.

Measurable results from DOE initiatives

The Department of Energy has come a long way over the past 18 months. Recent GAO[1] and Department of Energy Office of Independent Oversight and Performance Assurance[2] reviews have highlighted the positive changes that have taken place Department-wide. While I am not yet satisfied with the level of protection the Department has achieved to date, I believe the initiatives we have taken over the past year have dramatically improved security within the Department. Furthermore, I believe the Department is on track to demonstrating effective security program implementation at all sites in the near future.

Next Steps for DOE

The challenge for the Department of Energy is to maintain the current cyber security program and be sufficiently proactive to meet tomorrow's challenges. I am the first to admit that the Department of Energy has more work ahead. Currently, our near term plan is to better integrate security implementation with line management responsibility, continue implementation of site cyber architectures (boundary protection, host and application based controls), and improve our risk management processes.

---

[1] Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research (GAO/AIMD-00-140, June 9, 2000)

[2] Cyber Security Review of Unclassified Systems at Department of Energy Headquarters (May 2000)

The Department is intent on integrating cyber security into management and work practices at all levels so missions are accomplished while protecting DOE's critical cyber information assets. To accomplish this goal, cyber security management must be integrated into all facets of work planning and execution.

DOE is currently developing a formal, comprehensive department-wide cyber security management program that integrates risk management processes, and physical, technical, and administrative controls for ensuring confidentiality, integrity, and availability of DOE's information assets. Under this program, a framework of objectives, guiding principles, and security activities and functions, applicable to classified and unclassified environments, will be established to govern consistent implementation of cyber security management throughout the Department.

Conclusion

In summary, DOE's cyber security program as of September 11, 2000 bears little resemblance to the program in place just a year ago. We have promulgated updated cyber security policies; our security training has improved the effectiveness of our system administrators and informed our management of upgraded cyber security threats; each site has upgraded its security controls and has improvement plans to be executed as resources are available; and a review and follow-up process using the Secretary's Independent Oversight function permits the Department to objectively assess our status. Although we have made great progress, there is room for improvements. Clearly, the review of Headquarters shows that we have significant weaknesses

that require immediate attention. Moreover, the Department believes that Headquarters must set the standard for the rest of the Department on how it implements security of cyber systems. The Secretary and I are fully committed to ensuring that Headquarters is a model for the rest of the Department.

Beyond fixing the clear weaknesses, the Department is moving to strengthen security in a number of areas. Current focus areas for improvement are eliminating the use of clear-text reusable passwords, implementing consistent security architectures at each site, using automated tools to review firewall and intrusion detection logs to identify and then automatically block access from Internet sites that are attacking DOE sites, and automated distribution of software patches to make the process of patching vulnerabilities more rapid and reliable.

We know that there is no silver bullet fix for cyber security. Success in this area will take continued and focused effort to deal with the increasing complexity of the threats and the rapid evolution of technology.

Thank you. This completes my testimony. I would be happy to answer any questions from Committee members.

Mr. HORN. Well, thank you very much. And I would hope that when there is some budget negotiations going on toward the end, that the President's list will include this, and we hope that the Speaker will include it.

The next witness is John R. Dyer, the Chief Information Officer for the Social Security Administration.

Mr. Dyer.

STATEMENT OF JOHN R. DYER, CHIEF INFORMATION OFFICER, SOCIAL SECURITY ADMINISTRATION

Mr. DYER. Good morning, Mr. Chair, Mr. Turner. Thank you very much for inviting us to testify.

We, too, as this committee, consider security to be an actual vital concern, particularly in this day as we move more into the systems world.

At the onset let me emphasize that the Social Security Administration has always taken the responsibility to protect the privacy of personal information in agency files very seriously. The Social Security Board's first regulation published in 1937 dealt with the confidentiality of SSA records. For 65 years SSA has honored its commitment to the American people to maintain the confidentiality of the records in our possession. We understand in order to address privacy concerns, we need a strong computer security program in place. Today I would like to discuss where we are with computer security, what improvements we're making.

SSA approaches computer security on an entitywide basis. By doing so we address all aspects of the SSA enterprise. Overall the Chief Information Officer, who reports directly to the Commissioner and Deputy Commissioner, is responsible for information system security. In my role as CIO, I assure that our security initiatives are enterprisewide in scope. At the Deputy Commissioner level, Social Security's Chief Financial Officer assures that all new systems have the required financial controls to maintain sound stewardship over the moneys entrusted to our care. We have also placed our system security policy function with this Deputy Commissioner.

In order to meet the challenges of data security in today's highly technological environment, this agency has adopted an enterprisewide approach to system security, financial information, data integrity and prevention of fraud, waste and abuse. We have full-time staff devoted to system security stationed throughout the agency, in all regions and in the central office. We have established centers for security and integrity in each Social Security region. They provide day-to-day oversight control over our computer software. In addition, we have a Deputy Commissioner-level Office of Systems which supports the operating system, develops new software and the related controls, and, in general, assures that Social Security is taking advantage of the latest in effective systems technology.

SSA has been certifying its sensitive systems since the original OMB requirement was published in 1991. Our process requires Deputy Commissioners responsible for those systems to accredit them. SSA's planning and certification activity is now in full compliance with NIST 800–18 guidance.

SSA sensitive systems include all programmatic systems needed to support programs administered by the agency as well as critical personnel functions. They also include the network and the system used to monitor Social Security's data center operations.

As an independent agency we have our own inspector general who can focus his efforts on the agency needs and concerns. The IG is also very active working with other Federal, State and local law enforcement agencies to assure all avenues for investigation and prosecution are being pursued, especially for systems security-related issues.

In summary, we have in place the right authorities, the right personnel, the right software controls to prevent penetration of our systems and to address systems security issues as they surface.

As I mentioned, SSA has maintained an information security program for many years. Key components, such as deploying new security technology, integrating security into the business process, and performing self-assessment of our security infrastructure, to name a few, describe the goals and objectives that will touch every SSA employee.

Of particular importance this year are the activities related to the Presidential Decision Directive PDD–63 on cyberterrorism and infrastructure protection and continuity of operations. We have recently completed an evaluation of all critical SSA assets. I am pleased to note that SSA was one of the first agencies to do so.

Originally, SSA was not a tier I agency, but given the importance of our ongoing monthly payments, we were elevated to this level by the Critical Infrastructure Assurance Office. As part of this effort we have completed an inventory of all critical assets and implemented an incidence response process for computer incidents. We have also revised our physical security plans to assure our facilities are properly secured.

An independent auditor, Pricewaterhouse Coopers, has evaluated our security program over the last 4 years working with the IG. They have given us many recommendations to strengthen our security program, and we have implemented 77 percent of their recommendations. We are addressing the remainder at this time. Most of the ones that will take us to finish up over the next fiscal year are facility-related, and that's what takes a little bit of time.

In addition, we have ongoing site reviews, corrective actions, and we also have another independent contractor, Deloitte and Touche, reviewing our systems and overall management.

In the contingency area this year, we actually tested all of our sites at one time, which was an area of recommendation that Pricewaterhouse Coopers had recommended for us. And so we believe that when we get the next report from PwC, it will indicate that we have made substantial progress.

In terms of the new increasing technology, and as we're moving toward Internet, we are putting in place all the latest security features from firewalls to filters to head off specific attacks.

So I would like to say in conclusion, Mr. Chairman, the Social Security Administration has a longstanding tradition of assuring the public that their personal records are secure. Both the Commissioner and the Deputy Commissioner give system security their highest priority. We all recognize this is not a one-time task to be

accomplished, but rather it's an ongoing mission that we can never lose sight of. We know we cannot rest on past practice. We must be vigilant every way we can to assure that these records remain secure and that the public confidence in Social Security is maintained.

I want to thank the committee for the opportunity to testify at this hearing, and I will be glad to answer any questions you might have.

Mr. HORN. Thank you very much, Mr. Dyer.

[The prepared statement of Mr. Dyer follows:]

FOR RELEASE UPON DELIVERY

STATUS OF COMPUTER SECURITY AT THE SOCIAL SECURITY ADMINISTRATION

STATEMENT BY

JOHN R. DYER
EXECUTIVE DIRECTOR TO THE
DEPUTY COMMISSIONER &
CHIEF INFORMATION OFFICER

BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION AND TECHNOLOGY

HOUSE COMMITTEE ON GOVERNMENT REFORM

SEPTEMBER 11, 2000

SOCIAL SECURITY
USA
ADMINISTRATION

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me here today to discuss computer security at the Social Security Administration (SSA). We appreciate this subcommittee's interest in systems security and agree that system security is critical in today's environment.

At the outset, let me emphasize that SSA has always taken its responsibility to protect the privacy of personal information in Agency files very seriously. The Social Security Board's first regulation, published in 1937, dealt with the confidentiality of SSA records. For 65 years, SSA has honored its commitment to the American people to maintain the confidentiality of the records in our possession. We understand in order to address privacy concerns we need a strong computer security program in place.

Modern computer security requires the implementation of sophisticated software and control of access to the system. SSA uses state of the art software that carefully restricts any user access to data except for its intended use. Using this software, only persons with a "need to know" to perform a particular job function are approved and granted access. Our systems controls not only register and record access, but also determine what functions a person can do once access is authorized. SSA security personnel assign a computer-generated personal identification number and an initial password to persons who are approved for access (the person must change the password every 30 days). This allows SSA to audit and monitor the actions individual employees take when using the system. These same systems provide a means to investigate allegations of misuse and have been crucial in prosecuting employees who misuse their authority.

Today, I would like to discuss where we are with computer security and what improvements we are making. SSA approaches computer security on an entity wide basis. By doing so, we address all aspects of the SSA enterprise.

Enterprise-wide Security

Overall, the Chief Information Officer (CIO) who reports directly to the Commissioner and the Deputy Commissioner is responsible for information system security. In my role as CIO, I assure that our initiatives are enterprise wide in scope. At the Deputy Commissioner level, SSA's Chief Financial Officer, assures that all new systems have the required financial controls to maintain sound stewardship over the monies entrusted to our care. We also have placed our systems security policy function with this Deputy Commissioner.

In order to meet the challenges of data security in today's highly technological environment, the Agency has adopted an enterprise-wide approach to systems security, financial information, data integrity, and prevention of fraud, waste, and abuse. We have full-time staff devoted to systems security stationed throughout the Agency, in all regions and in central office. We have established centers for security and integrity in each SSA region. They provide day to day oversight and control over our computer software. In addition, we have a Deputy Commissioner-level Office of Systems which supports the operating system, develops new software and the related controls and, in general, assures that SSA is taking advantage of the latest in effective systems technology.

SSA has been certifying its sensitive systems since the original OMB requirement was published in 1991. Our process requires Deputy Commissioners responsible for those systems to accredit them. SSA's planning and certification activity is now in full compliance with NIST 800–18 guidance.

SSA's sensitive systems include all programmatic system needed to support programs administered by the Agency as well as critical personnel functions. They also include the network and the system used to monitor SSA's data center operations.

As an independent agency, we have our own Inspector General (IG) who can focus his efforts on the agency's needs and concerns. The IG is also very active in working with other Federal, State and local law enforcement agencies to assure all avenues for investigation and prosecution are being pursued--especially for systems security-related issues.

In summary, we have in place the right authorities, the right personnel, and the right software controls to prevent penetration of our systems and to address systems security issues as they surface.

Information Systems Security Plan

As I mentioned, SSA has maintained an information system security program for many years. Its key components, such as deploying new security technology, integrating security into the business process, and performing self assessments of our security infrastructure, to name a few, describe goals and objectives that will

touch every SSA employee.

Of particular importance this year are the activities related to the Presidential Decision Directives (PDD-63) on infrastructure protection and continuity of operations. We have recently completed an evaluation of all critical SSA assets. I'm pleased to note that SSA was one of the first Agencies to do so.

Originally, SSA was not one of the Tier I agencies. But given the importance of ongoing monthly payments we have been elevated to that level by the critical infrastructure assurance office.

As part of this effort we have completed an inventory of all critical assets and implemented an incidence response process for computer incidents. We have also revised our physical security plans to assure our facilities are properly secured. Recently, we were one of the key agencies that evaluated the CIO Council's "maturity" model. This will help us compare where we are with industry standards overall.

Ongoing Monitoring and Assessment

Our independent auditor, Pricewaterhouse Coopers, has evaluated our security program each of the last 4 years. They have given us many recommendations to strengthen our security program and we have implemented 77 percent of their recommendations. We are addressing the remainder at this time. The remaining recommendations involve longer timeframes to implement. They will be

completed on a flow basis—we anticipate all will be completed by the end of the next fiscal year.

In addition, SSA has its own formal program of onsite reviews and corrective action. We also use an independent contractor, Deloitte and Touche, to review our systems and overall management of the program. All of this is tracked at the highest levels through an executive internal control committee which I chair and has membership of the Inspector General and key deputies.

Zero Tolerance for Fraud

Finally, I also want to state that we have a zero tolerance at SSA for fraud, waste, and abuse. We believe that our zero tolerance policy has paid off, as evidenced by the fact that almost all of the recommendations made to the Agency by independent auditors in recent years have been of a pre-emptive nature as opposed to a remedy for any actual abuse. Nonetheless, when we have evidence of an abuse of system privileges, addressing the matter is a number one priority of the Agency.

On June 22, 1998, Commissioner Apfel issued a notice to all SSA employees about administrative sanctions to be taken against any SSA employee who abuses his or her systems privileges. The penalties are severe and will lead to termination of employment for any offense that involves selling data. On March 2, 2000 this notice was revised and updated to make it even more relevant to employees.

SSA's IG is committed to the investigation and prosecution of every employee abuse case that is identified. Many of the SSA employee cases turned over to the IG for investigation were first discovered by the Social Security Administration itself. We must keep in mind that overwhelmingly SSA employees are honest, hardworking people.

Contingency

In order to ensure that our mission critical systems are up and running, we have a solid contingency plan in place. In August 2000, we completed a successful test of all SSA critical systems. Also, SSA has in place a hotsite as backup for its critical operations. These are recommendations that Pricewaterhouse Coopers thought it was important for us to complete.

Recent status by PwC noted substantial progress in this area. No new issues were identified as a result of this year's review. We believe all issues have been resolved, but are awaiting PwC's final report.

Moving Away from Mainframe Systems

I want to come back to the broader concerns. Addressing systems security is, and always will be, first of all, a high priority for SSA. By design, the Agency has used a system architecture that relied almost exclusively on mainframe systems and centralized databases. With this architecture we are able to more tightly control computer security than those Agencies who are faced with large numbers of local and/or distributed systems.

As SSA, in the increasingly technological environment, moves away from the mainframe environment to more distributed systems, we carefully consider, at every step of the process, how to build in security features. We have taken a number of steps to ensure that these new systems are as secure as possible.

We are on constant alert to identify both intrusion detection and denial-of-service type attacks. SSA's firewall team uses various services that list current hacker activity in order to identify the different types of attacks and how to respond and avoid them. SSA uses various filters on our routers to deny these specific attacks.

We have supported and will continue to support the independent audit of our financial statements. We have supported the auditors' detailed testing of SSA's systems. We work with the various oversight bodies-the General Accounting Office and the IG, for example, to review what we are doing and identify any issues they believe we need to address. Only in this way can we be assured SSA is getting all the advice that is available to us, and doing its utmost to maintain the security of our computer systems, and the data they contain.

New Emerging Concerns

We are well aware of the daily stories about new viruses, hackers, and security breaches and have taken both preventive and enforcement actions to protect information in Social Security files from any wrongful use by our own employees and from any unauthorized access by outsiders. Mr. Chairman, SSA takes a very proactive approach to identify hacker activity and adopt the proper defensive

posture to prevent interruption to SSA's website services. We use state-of-the-art technology to protect our network. We are on constant alert to identify both intrusion detection and denial-of-service types of attacks. SSA's network is monitored 24 hours a day, not only by SSA technicians but also by contract services.

This is not to say that we are resting on our laurels. We constantly reevaluate and, when necessary, upgrade the security features necessary to maintain the public's confidence that our systems are secure. Computer security is a top management priority.

When Social Security first became independent in 1995, and had its own IG for the first time devoted only to SSA's activities, the Commissioner asked the IG to make employee integrity the number one issue and the IG has done so. SSA has consistently asked for additional resources for the IG and received support from Congress for those requests.

Conclusion

In conclusion, Mr. Chairman, the Social Security Administration has a long-standing tradition of assuring the public that their personal records are secure. Both the Commissioner and the Deputy Commissioner give systems security their highest priority. We all recognize that this is not a one-time task to be accomplished, but rather is an ongoing mission we can never lose sight of. We know we cannot rest on past practice, but must be vigilant in every way we can to assure that these personal records remain secure, and that public confidence in SSA

is maintained.

I want to thank the Subcommittee for holding this hearing and focusing on what we all view as a critical issue. We are glad to know that the Congress shares our concerns, and we will work with the Subcommittee to assure the American people that we are doing all we can to maintain the security of our computer operations. I will be happy to answer any questions you may have.

Mr. HORN. As usual, Social Security is at the top of the heap even though it's a B. So we're used to you getting As under the Y2K situation, and we look forward to you keeping ahead of the pack, shall we say. Thank you very much for coming. Thanks to your colleagues that led to a B grade.

We now go to Daryl W. White, the Chief Information Officer of the Department of the Interior, who has presented us with quite a full platter of documentation. We appreciate that. It's all in the record, and now you have 5 minutes to summarize it.

STATEMENT OF DARYL W. WHITE, CHIEF INFORMATION OFFICER, DEPARTMENT OF THE INTERIOR

Mr. WHITE. Good morning, Mr. Chairman and Mr. Turner. Thank you for the opportunity to appear before you today to discuss the status of computer security at the Department of the Interior. The Department of the Interior appreciates being afforded the opportunity to complete the recent computer security questionnaire. We are pleased to report that we are making substantive progress to improve our computer security posture.

The Department of the Interior recognizes that computer security is of agencywide importance and is actively working to implement a well-structured program to protect our information assets. It is anticipated that the vast majority of issues identified in the questionnaire will be adequately addressed through implementations of our program.

Let me summarize the steps that Interior has taken over the past 14 months to improve our computer security posture. During 1999, Interior performed extensive work in Y2K readiness for mission-critical systems and major data centers. As a result of Y2K preparation, policies and guidance for contingency planning and physical security were issued and several implemented.

In September 1999, we acquired limited funding for contractor services to perform automated vulnerability scanning of our most critical systems. Based on the results of the scanning, remediation was performed where needed.

January 2000, Interior accomplished priority filling of the Department Information Technology Security Manager position with a well-qualified and experienced individual. We were fortunate to have obtained Steve Schmidt from the State Department's Bureau of Diplomatic Security. Mr. Schmidt has brought a wealth of experience and practical knowledge to Interior. It is through his leadership and direction that we have seen a revitalizing of the Department IT Security Working Group.

Also in January 2000, $175,000 was allocated for computer security program development. Funding was obtained through an internal competitive process whereby senior Department managers clearly chose computer security as a high priority issue in competition with other equally important issues. This funding was obligated to obtain contractor computer security services in program development and limited as-needed vulnerability scanning.

February 2000, Interior was successful in including in the fiscal year 2001 President's budget request $175,000 for electronic data security. The House and Senate omitted this funding from their versions of the fiscal year 2001 appropriations bill. Interior contin-

ues to clarify the urgent need for the funding to the Appropriations Committee.

In May 2000, the Departmental Information Technology Security Manager issued the Interior Information Technology Security Plan, fully specifying the National Institute of Standards and Technology [NIST], published generally accepted principles and practices for securing Federal computer systems. This plan provides the basis for ensuring a computer security program that meets or exceeds the minimum Federal requirements as required by public laws, Federal regulations and executive branch directions.

July 2000, the Department issued agencywide budget guidance that further supported Office of Management and Budget instructions on incorporating computer security funding in all information technology projects. This guidance advised that computer security spending should average 5 percent of the total budget for information technology spending and placed a high priority on increasing resources for security.

August 2000, a contract was awarded by the General Services Administration under the SafeGuard program to Science Applications International Corp. to provide computer security program development services to the Department. This is significant to our approach to computer security, and I wish to elaborate further.

One of the primary means to improve IT security across the Department of the Interior is to establish proven structured and self-documenting methodologies for working through the security life-cycle process. I am pleased to report that realizing this goal has begun through the award of the mentioned contract. The associated statement of work divides the task into two phases. The first phase tasks will provide Interior with the technical and administrative assistance to put in place proven structured methodologies for information technology security development. The second phase will produce minimum requirements for risk mitigation in the form of policies for agencywide information technology security issues. From here we will develop technology and product-specific implementation guides. Dependent upon the availability of resources, we will then implement operating capabilities.

In August 2000, an additional $240,000 was obtained for computer security program development. This funding will be used to accomplish the development and implementation of selected security practices.

In closing, it must be noted that our ability to completely implement an adequate computer security program is strongly dependent upon the availability of necessary resources.

This concludes my statement. I will be happy to respond to any questions that you or any members of the committee may have.

Mr. HORN. Well, we thank you very much, Mr. White.

[The prepared statement of Mr. White follows:]

STATEMENT OF DARYL WHITE, CHIEF INFORMATION OFFICER, DEPARTMENT OF THE INTERIOR, BEFORE THE COMMITTEE ON GOVERNMENT REFORM, SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY ON THE STATUS OF COMPUTER SECURITY AT THE DEPARTMENT OF THE INTERIOR

SEPTEMBER 11, 2000

Good morning, Mr. Chairman and Members of the Committee. Thank you for the opportunity to appear before you today to discuss the status of computer security at the Department of the Interior.

The Department of the Interior appreciates being afforded the opportunity to complete the recent computer security questionnaire. We are pleased to report that we are making substantive progress to improve our computer security posture.

The Department of the Interior recognizes that computer security is of agency-wide importance and is actively working to implement a well-structured program to protect our information assets. It is anticipated that the vast majority of issues identified in the questionnaire will be adequately addressed through implementation of our program.

Let me summarize the steps that Interior has taken over the past 14 months to improve our computer security posture:

- During 1999, Interior performed extensive work in Y2K readiness for Mission Critical Systems and major data centers. As a result of Y2K preparation, policies and guidance for contingency planning and physical security were issued and successfully implemented.

- September 1999, we acquired limited funding for contractor services to perform automated vulnerability scanning of our most critical systems. Based on the results of the scanning, remediation was performed where needed.

- January 2000, Interior accomplished priority filling of the Departmental Information Technology Security Manager position with a well-qualified and experienced individual. We were fortunate to have obtained Steve Schmidt from State Department's Bureau of Diplomatic Security. Mr. Schmidt has brought a wealth of experience and practical knowledge to Interior. It is through his leadership and direction that we have seen a re-vitalizing of the Department IT Security Working Group.

- January 2000, $175,000 was allocated for computer security program development. Funding was obtained through an internal competitive process whereby senior Department managers clearly chose computer security as a high priority issue in

competition with other equally important issues. This funding was obligated to obtain contract computer security services in program development and limited "as needed" vulnerability scanning.

- February 2000, Interior was successful in including in the FY 2001 President's budget request for $175,000 for electronic data security. The House and Senate omitted this funding from their versions of the FY 2001 appropriations bill. Interior continues to clarify the urgent need for this funding to the appropriations committees.

- May 2000, the Departmental Information Technology Security Manager issued the Interior Information Technology Security Plan fully specifying National Institute of Technology and Standards (NIST) published generally accepted principles and practices for securing federal computer systems. This plan provides the basis for ensuring a computer security program that meets or exceeds the minimum federal requirements as required by public laws, federal regulations, and Executive Branch directions.

- July 2000, the Department issued agency-wide budget guidance that further supported Office of Management and Budget instructions on incorporating computer security funding in all Information Technology projects. This guidance advised that computer security spending should average 5% of the total budget for Information Technology spending, and placed a high priority on increasing resources for security.

- August 2000, contract award by the General Services Administration under the SafeGuard program to Science Applications International Corporation to provide computer security program development services to the Department.

  This is significant to our approach to computer security and I wish to elaborate further. One of the primary means to improve IT security across the Department of the Interior is to establish proven, structured, and self-documenting methodologies for working through the security life-cycle process. I am pleased to report that realizing this goal has begun through the award of the mentioned contract. The associated statement of work divides the tasks into two phases. The first phase tasks will provide Interior with the technical and administrative assistance to put in place proven, structured methodologies for Information Technology security development. The second phase will produce minimum requirements for risk mitigation in the form of policies for agency-wide Information Technology security issues. From here, we will develop technology and product specific implementation guides. Dependent upon the availability of resources, we will then implement operating capabilities.

- August 2000, an additional $240,000 was obtained for computer security program development. This funding will be used to accomplish the development and implementation of selected security practices.

- Planned October 2000, the Department will conduct an agency-wide Information Technology conference. The conference includes a computer security track that will

focus on the practical aspects of computer security program implementation. Using the conference as a backdrop, the Information Technology Security Working Group will target and prioritize next steps for program implementation.

In closing, it must be noted that our ability to completely implement an adequate computer security program is strongly dependent upon the availability of necessary resources. The Department has made progress through limited funding, and recognizes that additional resources are needed. The Interior Chief Information Officer has identified the specific levels of resources needed for meeting the minimal requirements for centrally managed portions of the program. We are currently working through the FY 2002 budget development cycle to ensure that the program receives the resources necessary for successful implementation.

This concludes my statement. I will be happy to respond to any questions that you or any members of the subcommittee may have.

STATEMENT OF WORK
For
The Department of the Interior
Information Technology Security Plan Development
And Program Implementation

TABLE OF CONTENTS

1.0 Introduction
2.0 Scope
3.0 Tasks
4.0 Deliverables
5.0 Period of Performance
6.0 Government Furnished Information, Property, and Equipment
7.0 Security
8.0 Other Special Requirements
9.0 Travel

1.0 INTRODUCTION

1.1 BACKGROUND

The Mission of the Department of the Interior (DOI) is to protect and provide access to our Nation's natural and cultural heritage and honor our trust responsibilities to tribes.

DOI is composed of the Office of the Secretary, eight bureaus, and a collection of business centers that play a vital role in accomplishing the overall mission of the Department. The work specified in this SOW is being requested by the Department IT Security Manager located in the Office of the Secretary -- Office of Information Resources Management. The products of the specified work will have application across the Department of the Interior.

1.2 OBJECTIVE

Obtain contract services to assist in documenting and developing the Department of Interior Information Technology Security Plan (ITSP), and implementing the associated IT security program. DOI has identified 19 IT security practices that will form the core of its IT security program. Each of the 19 practices requires a structured methodology to take the practice from concept to implementation. As a Federal agency, DOI has an obligation to ensure that its IT security program strictly complies with the letter and intent of statutory requirements. To meet this obligation, DOI intends for its IT security program to rely heavily on structured methodologies and techniques that have been proven effective for other similar Federal agencies.

Outside services are required to provide DOI with the following:

1.2.1 A well documented IT security plan that provides the basis for an DOI-wide response to meeting the statutory and practical requirements that accompany the use of IT processing, storage, and transmission capabilities. This plan will prescribe the minimum IT security practices applicable to all DOI Bureaus, Services, and Offices.

1.2.2 A structured methodology for developing DOI-specific, vendor-neutral standards for implementing generally accepted practices for securing IT systems. These practices are taken from guidance developed by NIST, GAO, CIAO, GSA, and other Federal organizations. The 19 core IT security practices that will be implemented at DOI are:

- Policy Development
- Program Management
- Risk Management
- Lifecycle Planning
- Personnel and User Issues
- Preparing for Contingencies and Disasters
- Computer Security Incident Handling
- Computer Security Awareness and Training
- Security Considerations in Computer Support and Operations
- Physical and Environmental Security
- Identification and Authentication
- Logical Access Control
- Audit Trails
- Cryptography
- Certification and Accreditation
- Intrusion Detection and Monitoring
- Software Patch Management
- Period Assessments and Evaluations
- Malicious Code Detection, Prevention, and Eradication

1.2.3 A structured methodology for developing practical implementation guidance from DOI-specific, vendor-neutral standards.

1.2.4 A structured methodology for transforming practical implementation guidance into functioning operating capabilities.

1.2.5 A structured methodology to develop costing models to assist DOI in determining necessary resource levels for implementing the 19 core IT security practices. DOI operates in a distributed network and management environment. In this environment, there will be aspects of the security practices that should be managed centrally and aspects that should be managed by individuals.

1.2.6 Technical assistance in implementing its IT security plan.

2.0 SCOPE

The Department of Interior has a compelling need to develop and implement a well-structured Information Technology security program. This program is necessary to ensure the protection of National Critical Infrastructure, DOI Mission Critical Systems, DOI Mission Essential Facilities and other sensitive agency systems. Protection of these systems is required in accordance with Presidential Decision Directive 63 (PDD 63), Public Law 100-235 (Computer Security Act of 1987), OMB Circular A-130, Federal regulations, and Executive Branch directions.

DOI has specified the core of its IT security plan to be comprised of 8 principles and 19 practices. The 8 principles and 14 of the practices are taken directly from the National Institute for Standards and Technology (NIST) document, Generally Accepted Principles and Practices for Securing Information Technology Systems (NIST SP 800-14). NIST SP 800-14 was developed at the direction of the Department of Commerce, as required by the Computer Security Act of 1987. NIST SP 800-14 provides the foundation for meeting the minimum requirements for the protection of DOI IT systems and hosted data. The DOI IT Security Manager based on agency-wide discussions has added the 5 additional practices.

DOI now requires contract services to assist in developing methodologies to take the principles and practices, and turn them into operating capabilities. Strongly coupled with this is the need to develop costing models for use in justifying and explaining IT security resources.

3.0 TASKS

3.1 Information Systems Security and Information Assurance

The two primary task areas are security plan development and security program implementation. Security plan development is the first task area requiring completion by the Client Representative. Security program implementation is anticipated as a future need to provide a comprehensive approach to IT security.

Security Plan Development

3.1.1 The industry partner shall provide technical and administrative support to assist DOI in preparing a well documented and complete IT security plan. This plan will provide the basis for a DOI-wide response to meeting the statutory and practical requirements that accompany the Federal use of IT processing, storage, and transmission capabilities. Stated in the plan will be the philosophies, principles, practices, and methodologies. DOI will provide statements concerning philosophies, principles, and practices. The industry partner shall be responsible for providing and assisting in the implementation of well documented, structured methodologies. Specific methodologies include:

3.1.1.1 The industry partner shall provide technical and administrative support to assist DOI with preparing a well documented, structured methodology for developing DOI policies and standards from generally accepted practices for securing IT systems. Specific practices will be stated by DOI and are taken from guidance developed by NIST, GAO, CIAO, and other Federal organizations.

3.1.1.2 The industry partner shall provide technical and administrative support to assist DOI with preparing a well documented, structured methodology for developing practical implementation guidance from DOI policies and standards.

3.1.1.3 The industry partner shall provide technical and administrative support to assist DOI with preparing a well documented, structured methodology for moving practical implementation guidance into functioning operating capabilities.

3.1.1.4 The industry partner shall provide technical and administrative support to assist DOI with preparing a structured methodology to develop costing models to assist DOI in determining necessary resource levels for implementing IT security practices.

Security Program Implementation

3.1.2 The industry partner shall provide technical and administrative support to assist DOI in implementing the IT security plan developed in 3.1.1. Achieving full program implementation is contingent upon many factors including funding resource levels. Further, it is not practical to anticipate that all IT security practices move to full implementation at the same time. The Department wishes to approach the implementation of security practices based on a prioritization schedule to be developed in consultation with the Industry partner. A deliverable schedule will be developed based on the prioritization schedule. Subtasks leading to the completion of this task include:

3.1.2.1 Using the structured methodology documented in the IT security plan, the industry partner shall provide technical support to assist DOI with developing DOI policies and standards from generally accepted practices for securing IT systems.

3.1.2.2 Using the structured methodology documented in the IT security plan, the industry partner shall provide technical support to assist DOI with developing practical implementation guidance from DOI policies and standards.

3.1.2.3 Using the methodology documented in the IT security plan, the industry partner shall provide technical support to assist DOI with moving practical implementation guidance into functioning operating capabilities.

3.1.2.4 Using the methodology documented in the IT security plan, the industry partner shall provide technical support to assist DOI with developing costing models to determine necessary resource levels for implementing IT security practices.

4.0 DELIVERABLES

The industry partner shall submit reports and other deliverables in accordance with the requirements set forth in the table below. All reports shall be submitted in three (3) hard paper copies and one (1) electronic copy. Electronic copies shall be made available on a 3-½ inch high-density diskette or 100MB ZIP Disks as appropriate compatible with a PC operating in a Windows environment using the Microsoft Office Suite (Microsoft Word, Excel or Power Point).

4.1 Reports and other Deliverables

The industry partner shall submit monthly progress reports. Reports shall be classified according to content and as required by the delivery/task order or other instructions provided by the Government Contracting Authority (GCA). The progress report shall contain an executive summary, information on significant activities, progress on work associated with the delivery orders/task orders, and funds status. Additionally, the industry partner shall submit a monthly status report containing: a detailed description of the activities on each open delivery order and task order, status of funding for each open order for the current calendar quarter, and projected fund expenditure profile to task completion. The reports shall be submitted ten (10) calendar days after the reporting period. One (1) copy shall be provided to the Contracting Officer. Additionally the status of individual delivery and task orders shall be provided on a secure WEB server for access by the OIS COTR and by specifically identified Department/Agency representatives. The Web based reports shall be viewable online and capable of being downloaded from the Web by the COTR and other authorized personnel.
Guide.

4.2 Schedule for Deliverables, Reports, and Meetings

No.	Title/Soft Copy Format	SOW Paragraph	Recipients	Draft Due	Final Due
1	Kick-off Meeting/Microsoft Power Point		Primary Client Plus 20 copies for Internal Review	N/A	2 Weeks After Award
2	IT Security Plan Outline /Microsoft Word	3.1.1	Same as above	3 Weeks After Award	4 Weeks After Award
3	IT Security Plan incorporating philosophy, principles, practices, and methodologies /Microsoft Word	3.1.1 3.1.1.1 3.1.1.2 3.1.1.3 3.1.1.4	Same as above	7 Weeks After Award	10 Weeks After Award
8	IT Security Program Implementation	3.1.2		To be determined based on prioritization schedule developed in	

No.	Title/Soft Copy Format	SOW Paragraph	Recipients	Draft Due	Final Due
				consultation with the Industry partner and subject to available funding.	
9	Progress Reports	4.1			Monthly
10	Status Reports	4.1			Monthly
11	Briefings	4.3			As Requested
12	Progress Review Briefing	4.3			Quarterly

4.3 Briefings

The industry partner shall prepare and present briefings to the Government, when requested, on the results of efforts undertaken under this contract. Briefings shall be conducted in appropriately cleared areas. Schedules and format for presentation of these briefings will be specified in the delivery/task order or as mutually agreed to between the industry partner and the COR. In addition, the industry partner shall provide a formal program review briefing on a quarterly basis.

4.4 Documentation

Tasks performed within the scope of this contract shall require contract deliverables. The data required for each task will be specified in each delivery/task order and will reference the contract data requirements number (DRN). "Soft Copy" format requirements will be formalized in initial meeting with the host agency/department.

4.5 Contract Data Requirement

Contract Data Requirements will be used to satisfy the need for industry partner developed documentation. Specific delivery/task orders will reference these data requirements as appropriate or identify additional data requirements as required in each delivery/task order.

5.0 PERIOD OF PERFORMANCE

The period of performance shall be one calendar year from award with three yearly options to renew.

6.0 GOVERNMENT FURNISHED INFORMATION, WORKSPACE, AND EQUIPMENT

6.1 Information

Government provided information and disposition instructions shall be specified in individual delivery/task orders and/or DD 254. This information may take the form of policies, standards, guidelines, technical data, specifications, and other applicable documents. For access to classified and/or sensitive information and/or systems, the industry partner will be required to comply with the appropriate DOI regulations.

6.2 Work Space

It is not anticipated that the Government will provide work space at government operated facilities for the purpose of work performance.

6.3 Equipment

It is not anticipated that the Government will provide equipment for the purpose of work performed under this task order/delivery order.

7.0 SECURITY

7.1 Classified Storage

It is not anticipated that the industry partner will need to store classified information offsite for the purpose of work performance.

7.2 Sensitive Information Access (Personnel Security), Handling, and Disposition

7.2.1 Sensitive Information Access (Personnel Security)

DOI security policies require that personnel having access to sensitive security information have at minimum a Limited Background Investigation (LBI).

7.2.2 Sensitive Information Handling and Disposition

Sensitive-But-Unclassified (SBU) information, data, and/or equipment will only be disclosed to authorized personnel with a need-to-know as described in the delivery/task order and/or DD Form 254. The holder shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control; destroyed; or held until other wise directed. Items returned to the Government shall be hand carried or mailed to GSA or address prescribed in the delivery

order and/or DD Form 254. Destruction of items shall be accomplished by tearing into small parts; burning; shredding or any other method that precludes the reconstruction of the material.

8.0 OTHER SPECIAL REQUIREMENTS

8.1 Protection of property and materials.

The industry partner shall be responsible for properly protecting all information used, gathered, or developed as a result of work under Delivery/Task Orders, and/or DD Form 254 of the contract. Beyond protecting CLASSIFIED information, the industry partner shall also protect all UNCLASSIFIED government data, equipment, etc by treating the information as sensitive.

9.0 TRAVEL

The industry partner shall perform travel as required in the performance of the contract as stated in individual delivery/task orders. Travel shall consist of CONUS/OCONUS travel in support of the contract requirements identified in individual Delivery/Task Orders. Travel requirements will be coordinated with the Task Manager and approved by the Contracting Officer's Representative (COR). Travel requirements will be reported to the COR on a weekly basis for approval. Travel or anticipated travel to OCONUS areas will be coordinated with the GSA/FTS/OIS Security management Staff at the earliest possible date.

The Department of the Interior's Information Technology Security Plan (ITSP)

May 2000

Contents:

I. Summary
II. Philosophy
III. Methodology
IV. Scope
V. Applicability
VI. Authorities
VII. Responsibilities
VIII. Priorities
IX. Principles
X. Practices
XI. Policies
XII. Implementation
XIII. Short-term Goals

I. Summary

The Department of the Interior Information Technology Security Plan (ITSP) provides the basis for an agency-wide response to meeting the statutory and practical requirements that accompany the use of IT processing, storage, and transmission capabilities. The ITSP prescribes the minimum standards for IT security programs for all Bureaus, Services, and Offices. It is important to note that the ITSP does not fundamentally levy new requirements. The standards prescribed in the ITSP are taken from existing public laws, federal regulations, and executive branch directions.

The core of the ITSP is comprised of 8 principles and 19 practices. The 8 principles and 14 of the practices are taken directly from the National Institute for Standards and Technology (NIST) document, Generally Accepted Principles and Practices for Securing Information Technology Systems (NIST SP 800-14). NIST SP 800-14 was developed at the direction of the Department of Commerce, as required by the Computer Security Act of 1987. NIST SP 800-14 provides the foundation for meeting the minimum requirements for the protection of Federal IT systems and hosted data. The 5 additional practices have been added by the Department IT Security Manager based on agency-wide discussions.

The IT security risks of not meeting these requirements include systems and information stores that are readily subjected to unauthorized disclosure, non-approved modification, and lost availability. Resultant losses to the Department include a continuation of those risks already realized including resources consumed by court litigation, losses from financial fraud, loss of financial audit credibility, expenses for recovering from system compromises, unavailable IT services, and public embarrassment. Further, given the strong message on IT security recently communicated by OMB, the Department risks losing funding for continuing and new IT expenditures. Expressed by OMB to the heads of all federal agencies, starting with the FY 2002 budget cycle IT budget requests will be scrutinized in light of an agency's demonstrated attention to IT security. It is important to note that this is not a new requirement, rather an old requirement that OMB intends to ensure compliance with.

Included in this document are brief statements on philosophy, methodology, scope, applicability, authorities, responsibilities, priorities, principles, practices, implementation, and short-term goals. Philosophy is given to provide a broad view of the Department IT Security core values and vision. Methodology, scope, applicability, authorities, and responsibilities are self-explanatory. Priorities discuss the order of precedence for implementation Principles and practices are derived from published national guidance and experience in computer security. Policy development and direction are discussed in general, as well as implementation guides. Finally, short-term goals are discussed.

II. Philosophy

The Department IT Security Manager adopts the following core values and vision on IT security.

Core Values

1. As keepers of the public trust we are bound to ensure that Department IT security is performed in a manner that meets the requirements of all applicable laws, standards, and directives.

2. All government automated information systems possesses some level of sensitivity regarding confidentiality, integrity, and availability and must therefore be afforded adequate levels of security.

3. The Department has a direct responsibility to ensure that adequate safeguards are made available to users of IT systems.

4. The Department has a direct responsibility to ensure that all levels in the organization fully understand the use and limitations of safeguards made available on IT systems.

5. While an aspect of IT security may be difficult to implement, it does not lessen its need to be done.

Vision

We will continually face a situation where the adoption of new technologies will challenge our abilities to implement them securely. A major factor is the need for adequate resources. IT security will continually compete with the numerous demands placed on this organization. The organization must understand that adequate IT security is a mandatory requirement, not an option. Further, not fully understood by most IT users is that IT security is an enabler to accomplish business. Making sure that these facts become common knowledge is a major imperative.

A key goal of the IT security program is to provide dynamic, relevant education and awareness. The education and awareness must be targeted to meet the needs of several groups of people. General system users must understand that computer security is important to ensuring that systems and data are adequately protected. System administrators require training in the technical specifics of what needs to be done on the various systems that they are charged with administering. IT Security managers require training in the complex tasks required to properly perform security functions. Members of management need an understanding of the mandatory requirements for asset protection and the

resources needed to meet those requirements.

The effectiveness of the IT security program will also depend greatly on how well we collaborate and share information. Particularly important is to establish the capability to collect, store, and disseminate knowledge of common interest.

The following gives some of the strategic goals and directions that the Department IT Security Manager sees for the Interior and its Bureaus:

-- IT security efforts must have adequate resources to meet statutory requirements for the protection of IT systems and hosted data.

-- IT security must be understood at all levels of the Department as important to attaining mission goals.

-- IT security requires personnel adequately trained to perform complex computer security functions for a variety of technologies and operational environments.

-- IT security requires collaboration and knowledge sharing by security managers and system administrators on threats, vulnerabilities, and countermeasures.

III. Methodology

The ITSP will be developed as a joint effort between all of the Department's bureaus. The general approach to this development is that a draft ITSP will be distributed for preliminary review to the IT Security Managers (ITSM) with information copies to Deputy CIOs. The Department IT Security Manager (DITSM) will schedule a teleconference whereby the draft ITSP can be discussed between the ITSMs and other representatives. The DITSM will be seeking concurrence from the ITSMs that the IT security practices outlined in the draft ITSP will meet the security needs of their bureaus.

The ITSWG should be prepared to discuss which practices can best be implemented and managed as "Bureau-centric", and those that are more appropriate as "Department-centric". The ITSWG should also be prepared to discuss the prioritization for implementation of the practices.

Specific implementation strategies and procedures will be determined by the ITSWG.

IV. Scope

The ITSP covers the following levels of systems and applications:

-- Those automated information systems and applications designated as National Security Critical as identified in the Department's Critical Infrastructure Protection Plan.

-- Those automated information systems and applications designated as Mission Critical Systems (MCS) or Mission Essential Facilities (MEF) in the Department's Y2K reporting document.

-- Automated information systems and applications as determined by the Department requiring protection from unauthorized disclosure of sensitive information, unauthorized modification of data, and/or loss of availability. These systems and applications will be referred to as "Sensitive".

V. Applicability

The ITSP is applicable to all Department of the Interior automated information processing, storage, and transmission capabilities. This applicability extends to capabilities not owned and/or operated by the Department, but for which the Department has an interest by the system being of a level covered under the scope of the ITSP. Applicability to other agencies using Department capabilities will be determined based on a Department determination of the level of risk to the Department, its users, and connected systems.

VI. Authorities

The Department's must satisfy at a minimum requirements put forth in these Public Laws, Federal Standards, and Executive Branch Directions:

Computer Security Act of 1987
OMB Circular A-130
OMB Circular A-130 Appendix III
Presidential Decision Directive 63
Presidential Decision Directive 67
President's Memo to Heads of Agencies
OMB Memorandum From Director Lew to Head's of Agencies Feb 28, 2000
Financial Manager's Integrity Act
Privacy Act
Trade Secrets Act
NIST SP 800-14

VII. Responsibilities

Reference: Department of Interior Manual 375 Chapter 19 Information Technology Security

VIII. Priorities

The order of priority for full implementation of ITSP practices is National Critical Systems (NCS), Mission Critical Systems & Mission Essential Facilities (MCS/MEF), and Sensitive Systems. Having said this, the practices that the Department must implement are applicable to all levels of systems. The primary difference will be in the rigor and intensity with which the practices are applied. In other words, implementation of ITSP practices for MCS/MEF and Sensitive systems will not be put on hold pending full implementation for NCS systems.

IX. Principles

The Department's IT Security Plan (ITSP) will adhere to these Generally Accepted Principles for Securing Information Technology Systems taken directly from NIST SP 800-14.

1. Computer security supports the mission of the organization
2. Computer security is an integral element of sound management
3. Computer security should be cost-effective
4. System owners have security responsibilities outside their own organizations
5. Computer security responsibilities and accountability should be made explicit
6. Computer security requires a comprehensive and integrated approach
7. Computer security should be periodically reassessed
8. Computer security is constrained by societal factors

X. Practices

The Department's IT Security Plan will incorporate (at least) 19 Generally Accepted Practices for Security Information Technology System. Practices 1 – 14 are taken directly from NIST SP 800-14. Practices 15 – 19 are included based on requirements determined by the Department IT Security Manager.

1. Policy

IT security policies in many ways form the basis for risk management strategy. Policies provide the statement from management that the Department can operate at a determined level of risk, provided that specific policies are followed. Policies will reflect different perspectives including Department-wide, Issue-specific, and System-specific. (800-14 3.1)

2. Program Management

Effective IT security program management will make use of central management through headquarters activities working closely with bureau and system-level activities. (800-14 3.2)

3. Risk Management

Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. (800-14 3.3)

4. Lifecycle Planning

Security, like other aspects of an IT system, is best managed if planned throughout the IT system life cycle. OMB guidance of February 28, 2000 makes it explicit that security must be a part of IT lifecycle planning (800-14 3.4)

5. Personnel and User Issues

Many important issues in computer security involve users, designers, implementers, and managers. A broad range of security issues relate to how these individuals interact with computer and the access and authorities they need to do their job. The Department has established procedures for grading positions for sensitivity and has in place the mechanisms for suitability assessments. Proper implementation of user administration are also important. (800-14 3.5)

6. Preparing for Contingencies and Disasters

Contingency planning directly supports an organization's goal of continued operations. This practice does not propose to supplant the Office of Managing Risks and Public Safety (MRPS) extensive work on issues dealing with Continuity of Operations (COO) and Continuity of Government (COG). This practice will borrow greatly from MRPS' work, and add to it practical aspects of all level of disaster prevention and recovery. (800-14 3.6)

7. Computer Security Incident Handling

A computer security incident can result from a computer virus, other malicious code, or a system intruder, either inside or outside. The Department currently handles incidents in a semi-ad hoc manner. We have made arrangements with FEDCIRC, but currently lack the capabilities to respond in a complete and consistent manner to incidents. (800-14 3.7)

8. Computer Security Awareness and Training

As previously expressed, a major part of the Department's IT security program will be devoted to education and awareness. (800-14 3.8)

9. Security Considerations in Computer Support and Operations

Computer support and operations refers to systems administration and tasks external to the system that support its operations. Failure to consider security as part of the support and operations of IT systems is, for many organizations, a significant weakness. (800-14 3.9)

10. Physical Environmental Security

Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. (800-14 3.10)

11. Identification and Authentication

Identification and Authentication is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability. Identification and Authentication is a technical measure that prevents unauthorized people or processes from entering an IT system. The

Department makes use primarily of static passwords. (800-14 3.11)

12. Logical Access Control

Access is the ability to do something with a computer resource (e.g., use, change, or view). Logical access controls are system-based means by which the ability is explicitly enabled or restricted in some way. (800-14 3.12)

13. Audit Trails

Audit trails maintain a record of system activity by system or applications processed and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. (800-14 3.13)

14. Cryptography

Cryptography provides an important tool for protecting information and is used in many aspects of computer security. Cryptography is traditionally associated with keeping data secret. However, modern cryptography can be used to provide many security services, such as electronic signatures and ensuring that data has not been modified. To enjoy the benefits of cryptography requires a programmatic approach to how it is applied. This includes such things as implementation standards, hardware vs. software, key management, and cryptographic module selection. (800-14 3.14)

15. Certification and Accreditation

IT security certification is a formal evaluation of how well a major application or general support system meets stated security requirements. Accreditation is the formal approval by a designated official that the major application or general support system can be placed into or remain in operation.

16. Intrusion Detection and Monitoring

Intrusion detection and monitoring (IDS) has traditionally been considered part of system audit capabilities, but has developed itself as a distinct practice in IT security. The Department makes extensive use of the Internet and Internet-style technology. The Department has been the victim of various internal and external based attacks. Currently, our IDS response is incomplete and inconsistent.

17. Patch Management

Commonly known operating system and application vulnerabilities have frequently enabled intruders to compromise Department systems. These operating systems and applications generally enjoy wide use throughout the Department. The Department appears to focus primarily on fixing the victim system, but has no formal procedure for making the exploit and countermeasure known to other vulnerable system owners.

18. Periodic Assessments and Evaluations

Period assessments and evaluations of systems are part of an overall risk management strategy. Assessments and evaluations need to be performed to determine if a major application or general support system is still operating within an acceptable level of risk.

19. Malicious Code Detection, Prevention, and Eradication

Also referred to as viruses, Trojans, macro-viruses, worms, mail bombs, etc. malicious code incidents have become almost daily occurrences. Highly connected organizations like the Department that make extensive use of popular operating systems and applications vulnerable to malicious code incidents. The effects of malicious code incidents can be severe and costly to completely contain. Further, system and applications used by the Department mean that a virus incident can quickly spread. The Department's current approach to malicious code management is generally not complete nor comprehensive.

XI. Policies

Existing policies require updating, and new policies need to be developed to address changes in approach brought on by the ITSP. It is anticipated that policy development projects will often occur as parallel efforts. Critical to success is close collaboration and information sharing by all members of the development teams.

XII. Implementation Guides

Pollicies generally provide a broad view of what needs to be done. To actually do often requires implementation guides, sometimes also referred to as handbooks. A very simple example: We write a policy that states that desktop operating systems will be configured to prevent general system users from accessing local administrator functions. For the security and system administrator, the question is how exactly is this accomplished for desktop Windows NT/2000 or UNIX systems. This implementation guide would provide the specific instructions for what the configuration needs to be and how to do it. While there will be several implementation guides, the Department can benefit from an economy of scale because of our common use of systems.

XIII. Short-Term Goals

The Department IT Security Manager places a priority on attaining the following goals in 2000:

1. Finalize the IT Security Plan Framework and obtain concurrence from DOI bureaus.

2. Based on input from DOI bureaus, select at least three generally accepted practices for fast track development.

3. Work with DOI bureaus to develop FY 2002 budget submissions for all aspects of IT security program development.

Mr. HORN. Our next presentation is from Edward Hugler, the Deputy Assistant Secretary for Administration and Management, Department of Labor.

STATEMENT OF EDWARD HUGLER, DEPUTY ASSISTANT SECRETARY FOR ADMINISTRATION AND MANAGEMENT, DEPARTMENT OF LABOR

Mr. HUGLER. Thank you, Mr. Chairman and Ranking Member Turner. I will be brief, as you requested.

We share your view that computer security is a high priority, a priority that the Department of Labor takes very seriously at the highest levels. Quite frankly, I am disappointed at the grade we received today, and in some small measure dismayed by it.

Following a successful transition or the century date change, we have directed significant attention to enhancing our security program and strengthening our security perimeter to defend against its attack. While this surely is an ongoing and very complex task, I am pleased to report that we have made solid progress to date and are continuing to improve our ability to defend against cyber attacks.

As we began the fiscal year, we had a number of security-related issues identified by our Office of the Inspector General in their audit of our financial statement. The issues encompassed work to done in six areas of Department-wide security program planning and management structure. The good news is, because computer security is a high priority, we had already identified areas that needed attention and had plans under way for corrective action. This proactive posture was acknowledged by the OIG in their audit findings.

At this stage we have resolved all of the audit report issues at the departmental level and are working toward closing out the remaining issues with specific agency systems.

In addition to dealing with immediate day-to-day issues, such as continued attempts to gain unauthorized access to our systems and responding to malicious codes such as the I Love You virus, we have invested substantial effort in planning ahead. Led by the Department's Chief Information Officer, our strategy in this undertaking has been twofold: First, align our information technology investments with legislative mandates and other direction; and second, bring a departmental focus to our information technology investments where a unified approach and economies of scale are advantageous.

Information technology approaches that are common across the Department, such as the implementation of a common architecture and needed improvements in the infrastructure, lend themselves to a common cross-cutting strategy. The use of a common strategy then enables us to effectively leverage the use of individuals' expertise and other scarce resources for the good of all at the Department of Labor.

Utilizing this approach for fiscal year 2001, the Department identified three cross-cutting areas for investment, one of which is computer security. The computer security cross-cut represents approximately 18 percent of the Department's information technology cross-cutting investment portfolio for fiscal year 2001. It includes

plans to ensure that the information security policies, procedures and practices of the Department are adequate, as well as reflect the first step toward implementing a multiyear plan for protecting our critical infrastructure. Notably this will be a separate budget activity, and the funds will be administered by the Department's Chief Information Officer to ensure an organized, disciplined approach to implementing a stronger security program.

Mr. Chairman, our plans for next year should not, however, overshadow what we've accomplished this year, 2000. I would like to submit a brief highlight of those accomplishments for the record, if I may.

Mr. HORN. Without objection, it will be in the record at this point.

Mr. HUGLER. Thank you, Mr. Chairman.

Mr. Chairman, we concur with the need to assess the overall state of the Federal Government's computer security environment, and we welcome the opportunity to work with you and the subcommittee to devise an instrument that will provide the flexibility necessary to accurately assess agencies' progress. We also recognize that work remains to be done at the Department of Labor to further improve our computer security.

I share with you your confidence that we will come through as we did with the year 2000 challenge. I am confident as well that we have sound plans for making these improvements and the skill on hand to do so. However, the key to our success, as has been mentioned by other witnesses at the table this morning, will be making the necessary funding available.

Thank you, Mr. Chairman. I appreciate the opportunity to be here, and I will be happy to take your questions.

Mr. HORN. Well, thank you very much.

[The prepared statement of Mr. Hugler follows:]

STATEMENT OF MR. EDWARD C. HUGLER
DEPUTY ASSISTANT SECRETARY, ADMINISTRATION AND MANAGEMENT,
UNITED STATES DEPARTMENT OF LABOR
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY
September 11, 2000

Good morning Mr. Chairman, Ranking Member and Members of the Subcommittee. I am pleased to appear before you to discuss computer security at the Department of Labor. We share your view that computer security is a high priority - a priority that the Department of Labor takes very seriously at the highest levels.

Following a successful transition with the Century date change, we have directed significant attention to enhancing our security program, and strengthening our security perimeter. While this is surely an ongoing and complex task, I am pleased to report that we have made solid progress to date, and are continuing to improve our ability to defend against cyber attacks.

The Department of Labor is also on track to meet its responsibilities under Presidential Decision Directive 63 (PDD-63) which directed development of a National Plan for Information Systems Protection. PDD-63 established milestones for Federal agencies that are broken down into Phases, with each Phase having its own discrete set of deadlines. The Department of Labor follows the "Phase II" requirements and milestones. While the Department has not been identified as a lead agency for an infrastructure sector, we take our responsibility for protecting our critical infrastructure seriously. We are pleased to report that the Department has met the PDD-63 deadlines stipulated in the National Plan for Information Systems Protection for Phase II agencies. Nevertheless, we recognize that significant work remains to achieve the overall FY2003 PDD-63 goal.

At the beginning of the fiscal year, the Office of the Inspector General (OIG) identified a number of computer security related issues in the financial statement audit findings. The issues encompassed work to be done in six areas of Department-wide security program planning and management structure. These six areas include establishing a security program planning and management structure; access controls; application software development and change controls; system software policies and procedures; segregation of duties; and service continuity through documented and tested contingency plans. The good news is - because computer security already was and continues to be a high priority - we had already identified areas that needed attention and had plans underway for corrective action. This proactive posture was also acknowledged by the OIG who cited the following in their audit findings:

> "The Office of the Chief Information Officer (OCIO) has developed a draft Computer Security Handbook which is in the approval process. This handbook addresses all of the

above-mentioned [six] areas of concern."

At this stage, we have resolved all of the Department-wide audit report issues and are near to closing out the remaining issues with specific agency programs.

In addition to dealing with immediate day-to-day operational issues, such as continued attempts to gain unauthorized access to our systems, and responding to malicious code, such as the "I Love You" virus, we have invested substantial effort in planning ahead. Led by the Department's Chief Information Officer, our strategy in this undertaking is two-fold: First, align our information technology investments with legislative mandates and other direction, including OMB, NIST and GAO guidance. And, second, bring a Departmental focus to our information technology investments where a unified approach and economics of scale are advantageous. Information technology approaches that are common across DOL agencies, such as the implementation of a common architecture and needed improvements in the infrastructure, lend themselves to be addressed using a common, cross-cutting strategy. Use of a common strategy enables us to effectively leverage the use of individuals' expertise and other scarce resources for the good of all.

Utilizing this approach, during the FY2001 budget formulation process the Department identified three "crosscutting" areas for investment, one of which is computer security. The computer security cross-cut represents approximately 18% of the Department's cross-cutting budget for Information Technology for FY2001 - and includes plans to ensure that the information security policies, procedures and practices of the Department are adequate, as well as reflect the first step toward implementing a multi-year plan for protecting our critical infrastructure. These funds will be administered by the Department's Chief Information Officer to ensure an organized and disciplined approach to implementing a stronger security program.

Mr. Chairman, the Department recently completed a self-assessment of its security posture using the Computer Security Questionnaire from your Subcommittee. The Department was able to answer 18 out of 29 questions affirmatively. We did have difficulties answering the remaining 11 questions with an unqualified "Yes" due to the fact that these questions could have multiple answers depending on which system was being reviewed and where that system resides within the life-cycle. For example, one questions asks "Have ***all*** significant threats to the physical well-being of sensitive and critical resources been identified and related risks determined?" The Department has undertaken extensive preparations to ward off ***known*** threats to ensure critical systems continue to operate without major interruptions. However, we cannot in good faith state that "Yes", ***all*** significant threats have been identified given the dynamic environment we face as those who threaten us become more innovative by the hour.

Mr. Chairman, we concur with the need to assess the overall state of the Federal government's computer security environment and welcome the opportunity to work with the Subcommittee to refine the Questionnaire and devise an self-assessment instrument that will provide the flexibility necessary to assess agencies' progress.

We also recognize that work remains to be done to further improve our computer security at the

Department of Labor. I am confident, however, that we have a sound plan for making those improvements, and the skill to do so. Key to our success will be making the necessary funding available to fully fund our FY2001 budget request.

Thank you for this opportunity to provide an opening statement, and I am available for any questions you may have.

Mr. HORN. And our next presenter is Ira L. Hobbs, the Deputy Chief Information Officer for the Department of Agriculture.

Mr. Hobbs.

STATEMENT OF IRA L. HOBBS, DEPUTY CHIEF INFORMATION OFFICER, DEPARTMENT OF AGRICULTURE

Mr. HOBBS. Thank you, Mr. Chairman. Good morning, Mr. Chairman and Ranking Member Turner.

I am pleased to appear before the committee this morning to update you on the status of the computer security program of the U.S. Department of Agriculture. With your permission, I will make a few brief comments and submit my written testimony for the record.

USDA's programs touch the lives of every American every day. We manage a diverse portfolio of over 200 Federal programs throughout the Nation and the world at a cost of about $60 billion annually.

The information we manage, which includes Federal payroll data, market-sensitive data, geographical data, information on food stamps and food safety, proprietary research data, is among USDA's greatest assets.

The Department is committed to protecting its information assets as well as the privacy of its customers and its employees. Audit reports conducted by both USDA's own Office of the Inspector General and the General Accounting Office have identified significant weaknesses in our overall computer security program, which we are working hard to correct. As an example, the Department is acquiring and installing necessary equipment to upgrade security at our highest priority Internet access points, and we are strengthening our intrusion detection capabilities. We are working diligently to correct all of the deficiencies that have been identified by the reports and hope to be able give you a much more expanded impact in terms of the changes that we have made.

Reports such as those cited above, as well as internal security reviews mandated by the Secretary of Agriculture in July 1999, made it clear that the Department requires an overall coordinated and corporate approach to cybersecurity if it is to succeed.

The USDA agencies include some security funding in their respective budgets. Departmental funding is critical to ensuring the creation of a standard security infrastructure, and departmental leadership is required to ensure that we have a comprehensive set of policies and guidelines.

The Secretary's security review also resulted in a multiyear action plan to strengthen USDA's information security, which addresses program organization, staffing needs, policy and program operations, and security and telecommunications technical infrastructure. When fully enacted our plan will align USDA security practices with those of leading organizations.

Our recent focus primarily has been upon building upon the competency and skill of our security staff. We are extremely fortunate working with the Secretary to establish the first Associate Chief Information Officer for Cybersecurity at the Department of Agriculture and able to select a senior level executive, Mr. William Hadesty, formerly with the Internal Revenue Service, as our first

CIO for Cybersecurity. With the recent addition of Mr. Hadesty, we have already started to implement the priority actions in our action plan.

The Congress provided a $500,000 budget increase for the Office of the Chief Information Officer for security in fiscal year 2000. With these funds and existing resources, we are assembling a well-qualified staff of security experts to lead the Department's efforts.

Since joining with us in February 2000, the Associate CIO for Cybersecurity has carefully analyzed and made adjustments to our ongoing program. In addition, our most critical information resources, including the National Information Technology Center in Kansas City and the National Finance Center in New Orleans, have been or are now undergoing critical review. We recognize, though, that we still have a long way to go.

The Office of the Chief Information Officer's fiscal year 2001 budget request included an increase in funding for cybersecurity of approximately $6.5 million. If enacted as requested, our security budget will provide the resources to complete the development of a USDA risk management program, continue to expand our cybersecurity office, increase our capacity to conduct onsite reviews, and provide training and hands-on assistance to augment the skills of our agency's security staff. Additionally our project plans call for a major effort in 2001 to further define requirements for a security architecture and begin its redesign and implementation.

In fiscal year 2002, we will continue to develop and implement our USDA-wide computer security program. The information survivability program and the sensitive systems certification program we plan to establish will complete USDA's computer security umbrella.

Mr. Chairman, we believe that fulfillment of our cybersecurity action plan will position the Department to comply with Federal computer security guidelines and best management practices. The reality is, though, that until our computer security program is fully funded, we will remain much too vulnerable.

I appreciate the opportunity to speak to the committee. I look forward to being able to answer any questions you may have.

Mr. HORN. Thank you very much, Mr. Hobbs.

[The prepared statement of Mr. Hobbs follows:]

Statement by
Ira L. Hobbs
Deputy Chief Information Officer, USDA
Before Congressman Stephen Horn, Chairman
Subcommittee Government Management, Information, and Technology

September 11, 2000

Mr. Chairman, members of the Committee, I appreciate the opportunity to appear before the Committee to update you on the Department of Agriculture's (USDA) computer security program.

USDA's programs touch the lives of every American, every day. We manage a diverse portfolio of over 200 Federal programs throughout the nation and the world, at a cost of about $60 billion annually; with over 100,000 employees. The Department is committed to maintaining the availability, integrity, and confidentiality of USDA information technology systems and telecommunications resources that are vital in delivering USDA's programs.

The Security Problem

Both Federal and industry organizations are moving quickly toward an electronic, Internet-based mode of doing business. Likewise, USDA is rapidly developing and deploying Internet applications, based on requirements arising from legislative mandate, customer expectations, and the promise of a more effective and economical way of conducting business. At the same time, the Department's embrace of this new

technology has also made USDA's organizations and the information resources we manage more vulnerable to unlawful and destructive penetration and disruptions.

USDA computer systems support billions of dollars in benefits. The vast amount of USDA's information, which encompasses Federal payroll data, market sensitive (crops, farm, commodities, statistical) data, geographical data, information on food stamps and food safety, and proprietary research data, is among USDA's greatest assets. Yet, threats to USDA's information systems are too numerous to delineate, ranging from outright transferring of funds and personal/customer/program information -- to cyber-attacks that leave our information systems crippled or inoperable.

These attacks by hackers on USDA computer systems are occurring more frequently and with increasing complexity every passing month. Furthermore, audit reports conducted by both USDA's Office of Inspector General and the General Accounting Office have identified significant weaknesses in our overall computer security program. Specific vulnerabilities and corrective measures cited in these reviews include the following:

- The Department needs to materially strengthen control mechanisms to ensure encryption of sensitive and Privacy Act data transmitted over the Internet.

- Major weaknesses have been identified in security at some individual agency sites, attributed to the need for a more structured and integrated computer security program.

- The Department lacks an effective corporate telecommunications network management and monitoring system.

- Several major Internet access nodes for USDA currently have not installed sufficient firewalls and intrusion detection hardware and software. (The Department is acquiring and installing the necessary equipment to upgrade the highest priority nodes and is strengthening its intrusion detection capabilities. In the last quarter alone, we have repelled some 250 attacks by hackers on our information security systems).

The Secretary's Mandate

Reports such as those referenced above, as well as his own concern for computer security, led Secretary Glickman to require an internal review of USDA's information security management program, which was conducted during the month of July, 1999. Through this process and other internal assessments, it became apparent that although USDA agencies include some security funding in their respective budgets, the Department requires an overall coordinated and corporate approach to cyber-security if it is to succeed. Departmental funding is critical to ensuring the creation of a standard security infrastructure, and a comprehensive set of policies and guidines. The

Secretary's security review also resulted in a strategy that identified both immediate and longer range actions necessary to substantively improve the Department's cyber-security program and bring it into alignment with the best practices of leading organizations. Our multi-year "Action Plan to Strengthen USDA Information Security" provides a comprehensive approach for building a sound cyber-security program.

The plan addresses program organization, staffing needs, policy and program operations, and security and telecommunications technical infrastructure. Fulfillment of our Cyber-Security Action Plan will position USDA to meet its mandated and internal computer security obligations and, at the same time, address broader information resource management requirements, including the customer and legislative demands of E-government.

Actions to Date

With the recent addition of an Associate CIO for Cyber-Security, we have already started to implement the priority items in our action plan. The Congress provided a $500,000 budget increase for the Office of the Chief Information Officer (OCIO) for security in fiscal year 2000. With these funds, and existing resources, we have begun assembling a well-qualified staff of cyber- security experts to provide leadership in this critical area. The Associate CIO for Cyber-Security has over 20 years of experience in the computer security field. Since joining the Department in February, he has carefully analyzed and made adjustments to the Department's existing security program. In addition, some of the Department's most critical information resources have been or are

now undergoing critical review. These include our two major data centers, (1) the National Information Technology Center in Kansas City and (2) the National Finance Center in New Orleans; the Foundation Financial Information System, which is designed to vastly improve USDA's financial management capabilities; and USDA's Service Center Initiative – the major information technology modernization initiative designed to provide our county-based agencies the technology they need to operate effectively in the 21st century. Security vulnerabilities are aggressively being identified and addressed for these and other mission-critical information systems.

A Look Ahead

The Office of the Chief Information Officer's (OCIO) fiscal year 2001 budget request includes an increase in funding for cyber-security of approximately $6.5 million. In FY 2001, our security budget, if enacted as requested, will provide the resources to complete the development of a USDA risk management program, the cornerstone of any effective cyber -security program. The Department will expand its Cyber-Security Office and continue to bring to USDA the requisite skills and expertise necessary to implement an effective security program. Our plans include Cyber-Security Program staff members conducting numerous on-site reviews to both identify security weaknesses and to provide training and hands-on assistance to augment the skills of our agency security staffs. Additionally, our project plan calls for a major effort in FY 2001 to further define requirements for a security architecture and begin its re-design and implementation.

In FY2002, we propose to continue developing and implementing our USDA-wide computer security program to protect the Department's invaluable information assets while maintaining the privacy of our customers and our employees. The Information Survivability Program and the Sensitive Systems Certification Program we plan to establish will complete USDA's computer security umbrella. These programs will both protect the Department's critical infrastructure and position our agencies to better serve their customers by taking advantage of new advances in technology.

Based on best practices of leading organizations and guidance from Federal oversight agencies, the USDA Cyber-Security Program will build on the previous year's work in the areas of risk management and security architecture development. We will focus on strengthening internal oversight as well as providing agencies additional hands-on problem solving. In addition, because cyber-security is an ever-widening challenge, new aspects of the program will be initiated to address the complete range of computer security disciplines that are necessary for sound computer system management.

Conclusion

Mr. Chairman and members of the Committee, USDA is committed to strengthening its computer security program. We believe that fulfillment of our cyber-security action plan will position the Department to comply with Federal computer security guidelines and best management practices and will ensure the safety and availability of USDA's invaluable information assets. Because resources are limited, we

are required to address the plan according to an established priority that aligns with our budget expectations. This means that unless and until our computer security program is fully operational, we remain much too vulnerable. And, although we have begun to improve our computer security program, and have been able thus far to repel efforts at intrusion without major damage, we must act quickly to strengthen our corporate and agency level approach to security. The rapid change in technology will require us to maintain a strong, effective, and ongoing computer security program. We welcome this committee's help in this regard. Thank you very much, and I will be pleased to address any questions you may have.

Mr. HORN. Our next presenter is Mark A. Tanner, Information Resources Manager, Federal Bureau of Investigation, Department of Justice.

Mr. Tanner.

STATEMENT OF MARK A. TANNER, INFORMATION RESOURCES MANAGER, FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF JUSTICE

Mr. TANNER. Good morning, Mr. Chairman, Mr. Turner and other members of the audience. I thank you for inviting us here to discuss computer security at the FBI. The FBI shares your conviction that computer security is a vital concern. That concern is manifested in a variety of levels: First, the concern within the FBI as to how the FBI collects and handles sensitive personal information; the concern as a member of the U.S. intelligence community where there is a growing awareness and desire to achieve a collaborative sharing of intelligence information while at the same time securing highly sensitive and classified sources and techniques; the concern as a member of the law enforcement community often called upon to investigate, identify and apprehend those responsible for hacking into government systems and critical infrastructures of this Nation; and the concern as a Federal law enforcement agency called upon to investigate computer and computer-related crimes as diverse as a pedophile seeking to prey on a youngster, Internet fraud crimes which victimize all elements of our society, including persons and businesses, and those who would seek to enrich themselves by manipulating stock prices.

The FBI's internal computer policies and practices present a somewhat unusual picture as far as Federal agencies are concerned. The FBI is, as I have stated, an agency charged with investigating many computer-related crimes and it is charged with the conduct of all counterintelligence activities in the United States.

In addition, the FBI operates several systems on which State and local law enforcement agencies have come to rely as a necessity. As such, the FBI must operate both classified and unclassified systems, and many of those unclassified systems have strong requirements for the protection of personal data about American citizens as well as a need to maintain instant availability.

In addition, the nature of some of these, some of these systems presents special requirements in that the data represents information gathered through a variety of methods, each requiring its own specialized method of handling and protecting the information. These methods includes Federal grand jury subpoenas which are subject to the requirements of rule 6(e) of the Federal Rules of Criminal Procedure, material identified as Federal taxpayer information, and thus, subject to specialized handling and disclosure requirements, as well as other many other specialized requirements. Of course, the specific requirements of classified information such as that obtained as a result of title 50, the Foreign Intelligence Surveillance Act, activities or by other intelligence community agencies, which must be respected.

To accomplish these tasks, the FBI operates 35 general support systems and 12 major applications; 24 of the 35 general support systems are classified and 6 of the 12 major applications are classi-

fied. In other words, the FBI operates 30 national security systems. It should be noted that the vast majority of the FBI's classified systems are currently internal systems and thus do not have external connections to nonsecure or unclassified systems.

The FBI's information systems security policy is codified in our Manual of Investigative Operations, section 35. A copy of this policy has previously been provided to this subcommittee. The policy is a compilation of requirements which are outlined in section 35–11 of this policy. In general, let me state that because of the variety of types of systems used by the FBI, our practice, where practical, involves using a hierarchical approach to any requirement from these sources based on the selective system's criticality and risks. This is to avoid any possible confusion as to whether or not a system should follow this or that set of rules and regulations. To choose any other course of action would be folly.

The FBI's policy is coordinated with the Information Systems Security Unit which is a part of our National Security Division. The security unit works closely with the Department of Justice entities which oversee classified and unclassified computer systems. In addition, they maintain a good working relationship with the national entities responsible for computer security policy, such as the NSTISSC and NIST and the Security Policy Board to ensure that the latest information is available.

There are many challenges which face the FBI in today's computerized world. One of the biggest challenges involves the rapidly changing environment and the rapidly changing world in which we all live. New technologies are moving into the marketplace at a frenetic pace; old technologies are undergoing metamorphosis. Each of these new products presents particular problems and a careful and thoughtful analysis to ensure that the FBI continues to maintain a policy which recognizes the business needs of the computerized world and still providing meaningful security practice.

The FBI is practicing risk management approach in its certification and accreditation of all computer system security. As I previously noted, most systems are internal and not connected to nonsecure unclassified systems. This isolation provides some sense of comfort in that these systems are not connected to the outside and far less vulnerable to compromise and attack. In this manner, our approach has been to identify both systems which pose the largest risk in terms of their data and sensitivity of the data. These systems are approached before systems which play a lesser role in either their data or sensitivity. The FBI is currently engaged in a series of activities which will hopefully lead to the speedy completion of the certification and accreditations. Resources have been on loan from the Department of Justice as well as other intelligence community under the ICAP program.

The FBI has undertaken a—an effort to make system owners cognizant of system security requirements in their initial and lifecycle development of plans for systems, in that way ensuring that systems security is built into all systems and that the continuing costs are specifically identified as a separate line in each proposal.

In conclusion, let me just reiterate that the FBI appreciates the interest of this subcommittee, indeed the interests of all parts of Congress in this area where we share your interests and concern.

Our efforts will continue to ensure that all systems, including those of the FBI, meet the expectations of the American public to appropriately protect that information which must be protected. The FBI respects the trust placed in it by the American public and the Congress and will do the utmost to maintain that trust.

Thank you.

[The prepared statement of Mr. Tanner follows:]

STATEMENT OF MARK TANNER

INFORMATION RESOURCES MANAGER (IRM)

FEDERAL BUREAU OF INVESTIGATION

BEFORE THE COMMITTEE ON GOVERNMENTAL REFORM

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,

INFORMATION, AND TECHNOLOGY

U. S. HOUSE OF REPRESENTATIVES

September 11, 2000

Good morning, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me here to discuss the FBI's efforts in the area of computer security. The FBI shares your conviction that computer security is of vital concern. That concern is manifested in a variety of levels --- the concern within the FBI itself as to how the FBI collects and handles sensitive and personal information; the concern as a member of the U S. intelligence community where there is a growing awareness and desire to achieve a collaborative sharing of intelligence information while at the same time securing highly sensitive and classified sources and techniques; the concern as a member of the U. S. Government often called upon to investigate, identify and apprehend those responsible for hacking into Government systems and the concern a Federal law enforcement agency called upon to investigate computer and computer-related crimes as diverse as a pedophile seeking to prey on a youngster, internet fraud crimes which victimize all elements of our society including persons and businesses and those who would seek to enrich themselves by illegally manipulating stock prices.

The FBI's internal computer policies and practices present a somewhat unusual picture as far as Federal agencies are concerned. The FBI is, as I have stated, agency charged with the investigation of many computer-related crime and it is charged with the conduct of all counterintelligence activities in the United States. In addition, the FBI operates several systems on which local and state law enforcement agencies have come to rely as a necessity. As such, the FBI must operate both classified and unclassified systems, and many of those unclassified systems have strong requirements for the protection of personal data about American citizens as well as a need to maintain instant availability. In addition, the nature of some of the unclassified systems presents special requirements in that the data represents information gathered through a variety of methods each requiring its own specialized method of handling and protecting the information. These methods include the use of Federal Grand Jury subpoenas and are thus subject to the requirements of Rule 6e of the Federal Rules of Criminal Procedure, material identifiable as Federal Taxpayer information and thus subject to specialized handling and disclosure requirements, as well as other specialized requirements. Of course the specific requirements of classified information material obtained as a result of Title 50 (FISA) activities or other intelligence community agencies must also be respected.

To accomplish these tasks, the FBI operates 35 general support systems and 12 major applications. 24 of the 35 general support systems are classified. 6 of the 12 major applications are classified. The FBI also operates 30 national security systems. It should be noted that the vast majority of the FBI's computer systems are currently internal systems and thus do not have external connections to non-secure/unclassified systems

The FBI's information systems security policy is codified in our Manual of Investigative Operations, Part II, Section 35. A copy of this policy has previously been made available to this

subcommittee. The policy is a compilation of requirements from a number of sources which are outlined in Section 35-11 of this policy. In general, let me state that because of the variety of types of systems used by the FBI, our practice, where practical, involves using a hierarchical approach to any requirement from these sources. This is to avoid any possible confusion about whether or not a system should follow this or that set of rules and regulations. To choose any other course of action would be folly.

The FBI's policy is coordinated by the Information Systems Security Unit (ISSU) which is part of our National Security Division (NSD). ISSU works closely with both of the Department of Justice entities which oversee the classified and unclassified computer systems. In addition, ISSU maintains a good working relationship with national entities responsible for computer security policy such as the NSTISSC and NIST and the Security Policy Board to ensure that the latest information is available.

There are many challenges which face the FBI in today's computerized world. One of the biggest challenges involves the rapidly changing environment and the rapidly changing world in which we all live. New technologies are moving to the marketplace at a frenetic pace; old technologies are undergoing metamorphosis. Each of these new products presents particular problems and a careful and thoughtful analysis to ensure that the FBI continues to maintain a policy which recognizes the business needs of the computerized world while still practicing meaningful security practices.

The FBI is currently practicing a risk management approach in the certification and accreditation of its computer systems. As I have previously stated, most FBI systems are internal and not connected to non-secure/unclassified systems. This isolation permits some sense of comfort in that systems not connected to the outside are far less vulnerable to compromise and

attack. In this manner, our approach has been to identify those systems which pose the largest risk in terms of their data and the sensitivity of that data. Those systems are approached before systems which play a lesser role in either their data or their sensitivity. The FBI is currently engaged in a series of activities which will hopefully lead to the speedy completion of certification and accreditation activities of all systems. Resources have been loaned to the FBI from the Department of Justice and additional assistance is being sought from the U. S. intelligence community under their ICAP program.

Moreover, the ISSU has undertaken a series of steps to ensure that system owners and developers assume some of the initial and continuing responsibilities for a system. ISSU has developed and made available to all other FBI employees templates of system security plans and examples of risk assessments so that the efforts of the other entities will be more productively focused while at the same time lifting the operational and/or consulting efforts. In addition, ISSU has undertaken to develop a robust computer security education program for all users of its systems.

Future direction of the FBI's information systems security program include a focusing of the security requirements as an initial and life cycle requirement of all systems of the system owners and developers By insuring that security is "built into" all systems and that the continuing costs are identified as a separate line in proposals, the FBI will continue to meet the expectations of the American public and this Congress as to computer security. As the FBI increases its connections to external systems, additional demands will be placed on those responsible for security. These responsibilities include such methodologies as network operating/monitoring centers to include intrusion detection.

In conclusion, let me reiterate that the FBI appreciates the interest of this Subcommittee,

indeed the interest of all parts of the Congress, in this area where we share your interests and concerns. Our efforts will continue to work with you to ensure that all computer systems, including those of the FBI, meet the expectations of the American public to appropriately protect that information which must be protected, while at the same time sharing that information which may be shared. The FBI respects the trust placed in it by the American public and this Congress and will do its utmost to continue that trust.

Thank you.

Mr. HORN. Well, thank you Mr. Tanner. We appreciate very much what the FBI has done in tracking down a lot of these hackers, and some I believe are in Federal prison now. So we thank you for that effort, and I think you were very on top of the situation in the Philippines when that occurred.

Our last presenter before questions is Solveig Singleton, Director of Information Studies for the CATO Institute. Am I correct to say the CATO Institute would be called a libertarian-based institute?

Ms. SINGLETON. Yes.

Mr. HORN. OK. Ms. Singleton, it's all yours for 5 minutes.

STATEMENT OF SOLVEIG SINGLETON, DIRECTOR OF INFORMATION STUDIES FOR THE CATO INSTITUTE

Ms. SINGLETON. Thank you, Mr. Chairman. My testimony today is going to offer examples of some of the types of data bases maintained by Federal agencies and offer a big-picture perspective on the significance of any security problems within those data bases.

With the power to command, powers of arrest, police, courts and armies, the government has powers that the private sector lacks. You can hang up on an annoying telemarketer but it's hard to hang up on the IRS. Recognizing that in the Constitution we have the fourth amendment which limits the means by which government may collect information and we also had the idea originally of a government of relatively limited powers, and inherently a government of more limited power has less need for hundreds and hundreds of data bases than a government of broader powers.

Now, for better or for worse, we have drifted away from this concept of limited government, and there's a natural consequence. The amount of detailed information about private citizens in Federal files has grown by leaps and bounds.

To underscore the importance of keeping this information secure, I will offer an overview of the types of information that are held by Federal agencies.

Essentially, Federal agencies collect an enormous array of information. The Federal Government will inexorably record, obviously, your name, your address, your income, but also your race, details of how you spend your money, your employer, updated quarterly, whether you've asked for information from government agencies, student records, whether your banker thinks you've engaged in any suspicious activities like making an unusually large withdrawal or deposit, and finally, of course, a surprising number of agencies hold different types of medical records and not simply Health and Human Services.

I am going to run down some of the departments that we looked at very quickly and offer a very small number of examples of the type of information that they hold. Let me start with the Commerce Department.

One file maintained by this Department keeps individual and household statistical surveys which include individual's names, age, birth date, place of birth, sex, race, home business phone and address, family size and composition, patterns of product use, drug sensitivity data, medical, dental, and physical history and other information as they consider necessary.

The Department of Education has the national student loan data system and, among other items, a registry of deaf-blind children nationwide.

The Department of Energy maintains, among some very sensitive counterintelligence data bases, records of human radiation experiments.

The Federal Bureau of Investigation, obviously, is home to the FBI central records system, alien address reports, witness security files and information on debt collection and parole records.

The Department of Health and Human Services has massive quantities of medical record information, filling hundreds of data bases. Some of these data bases include the personal Medicaid data system and the national claims history billing and collection master records system.

Next comes the Department of Housing and Urban Development. Now, this agency is perhaps best known among privacy advocates over the last few years, urging that residents of Federal housing agree to warrantless searches of their apartments in their lease agreements. This agency holds data such as single family research files, income certification evaluation data, and tenant eligibility verification files.

The Department of Labor has a lot of data bases including a data base with information on applicant race and national origin, records from the workers' compensation system and records from the national longitudinal survey of youth, which is a longterm study of certain individuals as they grew up over the past few decades.

Obviously the Social Security information collects information on lifetime earnings, as well as information related to insurance and health care and census data. What may be less well known is the extent to which they share and match information with Health and Human Services, the IRS, and other agencies. So, for example, one data base at the Social Security Administration is—matches Internal Revenue Service and Social Security Administration data with census survey data and records of Cuban and Indo-Chinese refugees.

The Department of Treasury, last but not least, holds a financing data base which contains millions of reports of banking activities of privately named U.S. citizens. They have also got the national data base of new hires, which holds records of the income and employment of every working American, updated quarterly.

Now, to sum up, I don't want to suggest that all this data is part of some kind of sinister plot and we should all go around wearing tinfoil hats on our head, nor do I want to denigrate the well-intentioned efforts that have been made to make many of these data bases more secure, but what I would like to point out is that the growth of these data bases makes security and the need for internal controls against unauthorized use by government employees a systemic problem rather than an occasional problem, and it generally—the growth of these data bases threatens to shift the balance of power between individuals and the Federal Government. So this really is a systemic issue and it will be become more and more acute as we move away from a vision of limited government and

want the government to be involved more and more in our day-to-day lives.

Thank you.

[The prepared statement of Ms. Singleton follows:]

A Constitutional Perspective on Databases Maintained by the Federal Government

Testimony
Solveig Singleton
Lawyer, The Cato Institute
1000 Massachusetts Ave NW
Washington, DC 20001
(202) 842-0200

Before the

U.S. House of Representatives Committee on Government Reform and Oversight Subcommittee on Government Management, Information, and Technology.

Hearing, Sept. 11, 20000

Mr. Chairman, my name is Solveig Singleton and I am a lawyer and the director of information studies at the Cato Institute. My testimony will provide examples of some of the types of databases maintained by federal agencies, and offers a constitutional perspective on the significance of the growth of such databases.

- The constitutional vision of the founders of this country was one of limited government--and limits on the power of government to collect information, because government has many powers that the private sector lacks.
- The amount of detailed information about private citizens in federal files has grown by leaps and bounds in recent years (examples are supplied below).

- Inadequate computer security arrangements at many government agencies could result in the compromise of this data by persons with criminal intent or intent on an abuse of power.

Information Collection in a Constitutional Government

With the power to command the armies, police, and courts, governments have unique powers of investigation, arrest, and trial that the private sector lacks. These unique powers make the possession of information by government alarming in a way that uses of information in the private sector are not. It is one thing if an auto repair shop or your neighbor wants to know what kind of car you drive; it's quite another to be asked by the police. And you can hang up on the most annoying telemarketer--but one had better not hang up on the IRS.

This fundamental distinction between public and private information-gathering is a part of this country's constitutional structure. The Fourth Amendment explicitly limits the means by which the government can collect information through searches and seizures.[1] But there is more to it than that. The

[1]The Fourth Amendment of the United States Constitution provides that:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or Affirmation, and particularly describing the

constitution was intended to create a government of limited powers. As James Madison noted in the Federalist No. 45, "[T]he powers delegated by the proposed Constitution to the federal government are few and defined."[2] The Constitution enumerates those delegated powers in Article 1, section 8 of the Constitution. A government of limited powers has little inherent need to collect information about people.

As long has we have turned away from recognition of the fundamental need to restrain government power across the board, we will continue to loose our privacy to civil servants. Just in the past decade, massive government databases have grown up. Beyond the census, social security, and the Bank Secrecy Act, there's a National Directory of New Hires with everyone in it (child support), federal mandates for drivers' licenses and birth certificates, pilot programs for "employment eligibility confirmation" (immigration), the evolution of the social security card into a de facto national identifier, a new employment database for the Workforce Investment Act, a national medical database with unique health identifiers, and the National Center for Education Statistics. On top of those new databases have come new proposals for monitoring and tracing citizen's activities,

---

place to be searched, and the persons or things to be seized.

[2] James Madison, The Federalist No. 45, in THE FEDERALIST PAPERS 292 (Clinton Rossiter

such as FIDNET. For now, the civil servants supervising these databases are well-intentioned, for the most part--but few governments throughout the course of human history have remained well-intentioned for long.

Government Information about Private Citizens, By Agency

Our research so far shows that federal agencies collect an enormous array of data about private U.S. citizens, far beyond what most Americans are aware. The federal government inexorably records your name, your race, your income and how you spend your money, your employer (updated quarterly!), and your address, whether you have ever asked for information from a government agency, your student records, and whether your banker thinks that you have engaged in any "suspicious" activity (like frequently making cash deposits or withdrawals), and finally, of course, your medical records. Several agencies besides the IRS may hold detailed financial information about individual accounts, and medical information is held by a surprising array of agencies.

The databases below are by no means an exhaustive list of all the files held by each agency; most agencies more databases than could be listed here, many of which might hold information about private citizens. The following are selected by

---

ed., 1961).

way of illustration.

Commerce Department. This department keeps Individual and Household Statistical Surveys," which includes individual's name, age, birth date/place, sex, race, home/business phone and address, family size and composition, patterns of product use, drug sensitivity data, medical/dental/physical history, and "such other information *as is necessary*." Other lists include those of "Minority-Owned Business Survey Records," "Individuals Identified in Export Transactions" and records of "Users of Public Search Room of the Patent & Trademark Office.

Department of Justice. Databases held here include the Inmate Physical and Mental Health Records System and other information relating to prisoners, as well as an "Information File on Individuals and Commercial Entities Knows or Suspected of Being Involved in Fraudulent Activities." They also hold Registration and Propaganda Files Under the Foreign Agents Act of 1938, and track citizen's purchases under the DEA Essential Chemical Reporting System. They also hold some medical records and are home to the "Automated Intelligence Records System" known as Pathfinder.

Department of Education. The department of Education holds "National Student Loan Data System," and among other items a "Registry of Deaf-Blind Children/Regional-National)."

Department of Energy. The department maintains records of Alien Visits, Counterintelligence Investigative Records, records of Power Sales to Individuals, as well as Human Radiation Experiments Records and records of participants in experiments, studies, and programs.

Federal Bureau of Investigation . The Clinton administration reportedly obtained hundreds of FBI files, including those several Bush and Reagan staff. The FBI is home to the FBI Central Records System, Alien Address reports, the Witness Security Files Information System, information on debt collection and parole records.

Department of Health and Human Services. This agency holds massive quantities of medical records filling hundreds of databases. Some databases include the "Person-Level Medicaid Data System," the "National Claims History; Billing and Collection Master Record System."

Department of Housing and Urban Development. This agency is perhaps best known among privacy advocates for trying to get residents of federal housing to agree to warrantless searches in their lease agreements. The agency holds data such as Single Family Research Files, mortgage files, and "Income Certification Evaluation Data Files" and "Tenant Eligibility Verification Files."

Department of the Interior. Databases held by this department include

"Individual Indian Monies," "Indian Student Records," and lists of "Foreign Visitors and Observers."

Department of Labor. This department holds a astonishing large number of databases, including a database with information for the "Applicant Race and National Origin System," Job Corps Student Records, records from the "injury Compensation System," and records from the National Longitudinal Survey of Youth. Also included are many databases containing records from Worker's Compensation programs or records otherwise relating to medical problems occurring on the job.

Social Security Administration Obviously, the Social Security Information collects information on the lifetime earnings of all Americans, as well as certain information relating to insurance and health care and census data. They share information with Health & Human Services and other agencies. Databases at SSA include "Matches of Internal Revenue Service and Social Security Administration Data with Census Survey Data," the Kentucky Birth Records System, and databases on Cuban and Indochinese refugees.

Department of the Treasury. This department holds the FinCEN Data Base, which contains millions of reports of the banking activities of individual named U.S. citizens, as well as database of Relocated Witnesses, files of "Derogatory

Information" about which no action has been taken, Electronic Surveillance Files, and the Office of Thrift Supervision's "Confidential Individual Information System." Treasury was also directed to establish (within the IRS) the "National Database of New Hires," which holds records of the income every working American, updated quarterly--the database was intended to track down dads that owe child support, but if you have a job, you're in it, even if you're a 50 year old woman with no kids.

Types of Abuses of Government Data

This century alone contains far too many examples of governments--including our own--that have abused information they were entrusted with. These examples include:

- During World War II, U.S. census data was used to identify Japanese-Americans and place them in internment camps.
- In 1995 over 500 Internal Revenue Service agents were caught illegally snooping through tax records of thousands of Americans, including personal friends and celebrities. Only five employees were fired for this misconduct.
- In response, the IRS developed new privacy protection measures. These measures were useless, with hundreds of IRS agents being caught in early 1997,

again snooping through the tax records of acquaintances and celebrities.

- Recently a web site operated by Arizona state exposed the credit card numbers and expiration dates of Arizona car owers due to a security lapse.

These examples provide examples of two different types of gvernment abuse of information.

No. 1--Public Abuse of Information. The first example, involving the Japanese, is an example of an abuse of data that occurred as a matter of public policy, sanctioned by high authorities in government themselves.

No. 2--Individual Government Employee Abuse of Power . The next examples show a different type of abuse, the use of data by government employees for their own personal or political purposes.

No. 3--Access by Criminal Intruders. The third type of abuse is suggested by the last example, the use of government data by hackers, identity thieves, or other intruders.

Conclusion: A Survey of Solutions

Vast amounts of sensitive and detailed information about you are in the hands of federal agencies. The security of this data is an important issue. The underlying battle for our security against government intrusions, however, will never be truly won until we have returned to a vision of a much smaller

government.

Mr. HORN. We thank you and now begin the questioning. What we'll do is alternate the questioning, 5 minutes for myself and 5 minutes for the ranking member and back and forth until we get the questions out of our system.

I'm going to start with the Department of Agriculture. As I recall in your statement, Agriculture repelled 250 hacker attacks. Were any of these successful attacks, Mr. Hobbs, and if so what kind of damage was done?

Mr. HOBBS. In some instances, Mr. Chairman, the attacks were successful. They resulted in things like changes to Web pages. We report all of our intrusions. Some of them like changes to Web pages. We were able to identify where people had been able to access systems, but in no instance were there any major or significant damages done. In most instances we've taken the necessary steps to shut down what we consider to be backdoor ways that people were getting into the systems, and are trying to be more vigilant in our monitoring and tracking of those activities and those kinds of concerns.

Mr. HORN. On the Agriculture, you completed the security questionnaire and it states the Department doesn't really feel that the system accreditation is important. A lot of other agencies feel the system accreditation, where possible, is important. Why isn't accreditation that important to the Department of Agriculture?

Mr. HOBBS. I don't think that we said that it was not important. I believe that what we are doing is we have a prioritized program that we are working toward completion of, with systems accreditation being a part of that. So I don't think we said it was unimportant. I think what we said is we have a prioritized effect—direction in terms of which we're trying to proceed, and that we're moving with deliberate speed in that sense of looking at all aspects and all phases of our security program.

Mr. HORN. Well let me ask Mr. Willemssen, on behalf of the General Accounting Office, as I understand, system accreditation is a formal management process to test and accept the adequacy of the system's security before putting it into operations. So how important is it to an agency's security computer programs that they're accredited; and could you explain that process and why most of the Departments are doing that where they can?

Mr. WILLEMSSEN. We believe system accreditation is especially critical, and it represents management's judgment that they have gone in, made an assessment of the risk of a particular system and the associated data; that given the risk associated with the system and data, appropriate controls have been put in place to fend off any attacks that may occur, and that management is therefore making a declaration that the appropriate controls are there to deflect or at least be aware of any such attacks that may happen. We think it's especially important. Most agencies agree. We do see at times differences in nomenclature. Some agencies may actually be doing something similar to accreditation but may call it something else.

Mr. HORN. Moving to the Department of Labor, Mr. Hugler, as I looked at the information, the computer security questionnaire indicated weaknesses in all six general control areas and the weaknesses were confirmed by the Inspector General's audit results. So

I'm curious, what does the Department consider to be its most critical weaknesses?

Mr. HUGLER. Well, Mr. Chairman, I think you're correct to state what the Inspector General found last year and they did find weaknesses in all six areas. I think what's important to recognize is that we have now addressed all of those issues, and in fact the Inspector General's audit findings, as I recall, acknowledged that if we did two important things, one is put out the rules for the Department's computer security and put out the rules for the Department, in terms of systems development and life-cycle criterion rules, if we did those two things, that we would have addressed all six of the categories with which they found issues.

We have done that and, more importantly I think, we have gone ahead aggressively with implementing those rules. And the example, I would cite to you, is our experience with the I-love-you virus. We have incident response procedures now in place at the Department. We had some 33,000 attacks from that virus. A small number of computers, 243 as I recall, were infected. I think the most—the best measure of our response, however, was the fact that we notified our employees of that virus and what to do with it 3 hours in advance of the official Federal notification.

So I would commend your attention to that as an example of the kind of things we've been able to do over the last year. So really the OIG's findings from last year are just that, a year old, and we have improved dramatically since then.

Mr. HORN. And so you would say the corrective action for these has been completed?

Mr. HUGLER. Yes, sir. At the Department level we have done that and I am very comfortable with that.

Mr. HORN. I now yield 5 minutes to the gentleman from Texas, Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman. As I listen to each of you who come from your respective agencies, it causes me to come back to a comment Mr. Gilligan made about the importance of cross-government initiatives. As many of you know, I have been an advocate of having a Federal CIO, a chief CIO for the Nation, someone who had the expertise, the competence, the leadership role, as well as the budgetary support necessary to be sure that we can have stronger cross-government initiatives in the area of information technology and certainly in the area of computer security.

And I think I'd like to ask you, Mr. Gilligan, to expand upon your assessment of the need for these cross-government initiatives, and I would be interested in your insight on it, because not having nearly the expertise in the area that you do nor the experience in the area, I still am left, after hearing all this testimony, with the conviction that the area of information technology certainly provides the potential for the expenditure of vast sums of Federal dollars in a very inefficient way. And I would be interested in your comments on the idea of more emphasis on cross-governmental initiatives and what kind of leadership might be necessary to ensure that happens.

Mr. GILLIGAN. Mr. Turner, I'd be happy to comment. What I have found in my activities in the CIO Council is that the potential that you allude to for enormous sufficiencies as a result of cross-govern-

ment IT efforts is there, but that potential is difficult to realize because our fundamental government structures in the executive branch and in the legislative branch tend to be stovepipe-oriented on particular agencies and particular missions, and in fact, what I have found is the most difficult efforts to get support for are cross-government initiatives. And relatively small sums of money that would have enormous benefits often fall through the cracks because there is no clear forum for advocacy. And individual committees, whether they be in the executive or the legislative branch, tend to be very narrowly focused on that portfolio to which they're assigned responsibility.

In my testimony, I noted our best security practices effort. This is an effort that is enormously compelling. The objective is to pull together best security practices from across the Federal Government, provide a Web repository where they can be accessed easily, and to share this wealth of experience that we have across the government.

We have found that getting small sums, hundreds of thousands of dollars for this initiative, is very difficult, and it's not that the effort is not supported. It is supported. And when I talk to members in the administration and Members of Congress, it is supported. But the question is, "who should pay for it and where should that funding come from?"

The Federal incident response capability, FedCIRC, which is our government's central point for disseminating information on viruses and patch updates, is funded through a set of committees. It is sponsored by Department of Defense, the FBI and GSA. We have found in the recent remarks that the report has not been strong, and again I don't think it's because the merits of this effort are not supported in general. It's that there is no central focus that helps bring this together and to help identify that these individual, relatively small dollar items in individual budgets, are in fact of far greater importance than their small dollars would indicate.

And so I think as you suggest, this is an area where we desperately need to focus attention. I think not only in the security area will it help us improve security, but we can far better leverage the enormous resources that we do have in attacking a whole range of information technology issues.

Mr. TURNER. Thank you.

Mr. Spotila, I know you have worked in this area, and one of your duties at OMB is to try to be sure that we move toward the kind of things Mr. Gilligan is talking about. I know there is a Presidential directive that established two tiers of agencies. It strikes me, and you might want to explain that a little bit, but it strikes me that it is certainly appropriate to acknowledge that the importance of computer security may vary from agency to agency, and that when we try to focus our resources, perhaps we should choose certain agencies over another. If we did that, we would expect to see different grades from the agencies because we would have made a choice regarding where to place the initial dollars to improve security. But describe for us a little bit that Presidential directive that established those first, those two tiers.

Mr. SPOTILA. Yes, Mr. Turner. First of all, let me just mention that OMB has been very supportive, as I've testified to the commit-

tee before, of these cross-cutting initiatives. We share Mr. Gilligan's belief that these are very important, that they would make a great deal of difference, and that they do need support.

The President, in May 1998, put out a Presidential Decision Directive aimed at critical infrastructure protection. It was at that time that he designated Mr. Richard Clark as his adviser on counterterrorism. He's worked with the committee and has been very active. The Critical Infrastructure Assurance Office was then established.

What we have tried to do in the administration is to prioritize in this area. I mentioned in my testimony that OMB's focus has been on the same 43 high-impact programs that we focused on during the Y2K effort. We have more than 26,000 systems in the government. If we're going to enhance our ability to serve the American people by promoting effective information security, we need to prioritize. We need to start with the areas that have the greatest impact, whether they be agency by agency, or, more accurately, within agencies, program by program, system by system.

The Critical Infrastructure Assurance Office has tried to zero in on those areas, those agencies, and those aspects within agencies that have the greatest importance and perhaps would be at risk the most. We've tried to work at OMB at focusing on the programs that we think have the greatest impact on the American people; as I'd mentioned, Medicare, Medicaid and the like. We think that we have to begin with the most important things. That's where we're going to have the most significant improvement and have the most significant benefit, which is not to say that we ignore all the other areas. We put out general guidance. We're working with the agencies. We're relying on the agencies to try to improve their efforts in this regard across the board.

But in terms of White House attention, we're obviously starting with the things that matter the most.

Mr. TURNER. Thank you.

Mr. HORN. Let me add to that the following. This is the last month of a fiscal year. This is the time Cabinet officers, deputy secretaries, assistant secretaries, all of them sit around and say, what can we do with the surplus we have in our budget? And having been in administration, I know exactly what they do, and this is the time, if they're serious about this, to reprogram some of that money into what everybody's saying, oh, we've got to have new money. That isn't the way we started with Y2K. We started when I urged a lot of the people to start reprogramming.

When Dr. Raines came in as budget director, he said, You're absolutely right, and that's what I'm going to tell them. And he did, and that's how we got the job done. We also made sure Congress provided the money. But if they're serious in these various executive branch agencies, this is the time to get a few million here and there.

And then besides that, let's just talk about a few simple steps such as policies requiring regular changing of passwords, safeguarding equipment, turning off computers. That doesn't cost a thing. That just costs doing it, if any. And I guess I would ask, because energy has certainly been in the papers for the last 2 years

on this, but I'd ask, is there in OMB the concern about policies to just get those basic areas done?

Mr. SPOTILA. Let me respond in a couple of respects.

First of all, I agree with you, Mr. Chairman, that some agencies are going to have discretionary funds available this September. We would certainly hope that they would apply them to this area. I know that the various CIOs at this table and others around government are going to do all they can to try to impress that upon their agency heads. So I think that we do need to be serious; just as all of us need to be serious, the executive and the legislative branch, because this is a really important area.

We have a lot of policy out there, even things that you mentioned about passwords, changing passwords and the like. The key is getting people to implement and follow the policy that may be out there. One of the things I emphasized in my testimony today and in my written testimony is that, in order to have effective security, it is essential that nonsecurity people buy in, that they participate, that they understand the significance and that they buy into it. Because we can have all the policies in the world and we can have all the centralized supervision in the world, but if that person at the desk doesn't follow it, it doesn't do any good.

You know, we tell the story about having very complex passwords that people write on little yellow sticky notes and paste to their computer screen. You can't have effective security without cooperation at all levels, and it's a message that we're trying to impart throughout the government. I think it will be an ongoing challenge to continue to do that.

Mr. HORN. I thank you very much.

Let me ask Mr. Dyer, who's got the B grade, the social security system, there is—apparently you're farther along than most other agencies now. Do you have a best practices that others might implement and what are they?

Mr. DYER. Mr. Chair, I think it's just like when we approached Y2K. Early on we saw it coming, and we institutionalized the process, the resources to deal with it. And we've done the same thing with security. It's part of our life cycle with our programs. Anytime we think about bringing up a new system, we look at the security aspects. Any modification to any system, we check the security all the way through and how it could roll over into other security systems.

I pick up on what GAO said and what John Spotila said. The biggest challenge we're finding is managing it. You can have good procedures, policies, rules in place, but you constantly have to be working with your managers, your employees that they follow them, and that's where we've been putting a tremendous amount of our effort.

We've had conferences across the country. We've set up centers so that we're able to make sure that we have people in place that are doing the dogging and checking it. We change passwords every month now. We found that it just didn't happen the way it should. So we have instituted it. We're going through. We found out that they change the passwords to something they could remember. We now have software to check to see if it's dates of birth or names

of family members or whatnot so you can start to screen those things out.

So, to me, it's a constant management challenge. You can do the systems, but you've got be there, right there on top of it all the time.

Mr. HORN. In my 26 seconds remaining, Mr. Willemssen, anything you want to add to that as to what might be done that isn't being done?

Mr. WILLEMSSEN. One thing that I would add, Mr. Chairman—and it somewhat extending off of Mr. Spotila's comment—and that is, it's one thing for agencies to have the policies and procedures which I think in many cases they do. It's quite another to see whether the accompanying practices have actually been put in place.

That's been particularly the case when we and Inspectors General go out and we test whether these policies and procedures are actually being implemented. They often have not been. And that really is a key distinction I think often between what the agencies believe is going on and what may actually be happening, although I think there is clearly many of the agencies are on the road for improvement in that direction, also.

Mr. HORN. I now yield 5 minutes to the gentleman from Texas, Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman.

The designation of the Presidential directive—is it tier 1, tier 2, phase 1, phase 2, whatever it's called—I'm curious as to what kind of impact that has and how is that designation significant; and I'd like, Mr. Hugler, if you would, to comment on that because I know Department of Labor is a tier 2 designation.

Mr. HUGLER. Yes, sir. Thank you, Mr. Turner.

It is an important distinction, because it is important to recognize that some agencies handle more sensitive information and have more sensitive systems than others do. We certainly believe that our mission is important to American workers, but, frankly, we do not have critical information that directly implicates national security. So, as such, if we are going to prioritize funding and implementation priorities, I think it is appropriate for the Department of Labor to be a phase 2 agency or tier 2 agency.

I think it's also important to note, though, that we take those responsibilities as a tier 2 agency as important and that we meet them and we are on target to meet all the milestones for which we are accountable.

Mr. TURNER. Mr. Spotila, when you think about funding for these various agencies to be sure they move forward in the area of computer security, do you make budgetary recommendations based on this phase 1, phase 2 designation?

Mr. SPOTILA. What we do in the first instance is to actually have the agencies themselves come to OMB with their own determinations as to what they'd like to accomplish and what they feel they need in the information security area. They do so within their overall budget submissions when they go through the OMB review process.

With the guidance that OMB put out earlier this year, focusing on the next budget year, we've made it very clear that information

security needs to be part of that agency initial analysis. It needs to be integrated within the entire area of information technology planning for budget purposes because we don't believe that doing it as an add-on is effective at all.

Within the budget review process, obviously if an agency is a higher priority, if the need is greater, that will be recognized in the process. Very often, the budget issues turn more on whether or not the proposal has been well thought out, whether it is likely to be a good use of money and a good expenditure of money and one that is likely to contribute not only to increased security but the agency's performance of its mission. Those are the kinds of factors that OMB takes into account, just as later on the Congress will take that into account.

And your comment earlier about the risk, that money could be wasted in this area, is also something that we take very seriously. You can't just fund a proposal because it sounds good or because the agency is an important agency or the area is an important area. You have to make certain that the proposal will work, that it will contribute something that will add value and will involve money well spent. And so this analysis is actually a very comprehensive and thorough one.

We think in the next budget cycle we're going to get better submissions from the agencies. We've been working with the agencies directly one on one to get them to understand the change. We're expecting that in the IT area we are going to receive budget submissions that are better thought out and that will have better justifications.

Mr. TURNER. Mr. Gilligan made a strong case for greater emphasis on cross-agency initiatives. What has OMB done to promote greater cross-agency efforts?

Mr. SPOTILA. We've actually been doing a variety of things. We've worked closely with the CIO council, which I've chaired since last year until their DDM was confirmed. We've worked closely with John and his committee in that regard trying to identify areas. We've worked closely with Dick Clark and the Critical Infrastructure Assurance Office and the national security community and with others throughout OMB and the agencies trying to identify areas where crosscutting initiatives would help.

John mentioned public infrastructure which would enable us to authenticate signatures. We think that's an important area. We know we need better intrusion detection capability. We think we need expert review teams that can get out onsite in the various agencies and help them not only assess security but try to improve their efforts in security. We think we need more efforts in the R&D area. We need scholarships for people to start learning this area so that the Federal Government can get the kind of personnel it needs with the kind of experience and educational background it needs to work in this area over the long term.

So we have tried to identify areas of need, working closely with all these other parties, and then within the budget process we've actually given it a huge amount of support to try to help develop proposals that make sense, that will have credibility with the Congress, that will work once implemented.

I think that the reality is we do start with a stovepipe approach. We all need to think outside of the box. We need to make certain that, as we do crosscutting initiatives, that they work so that we can buildup credibility and support for further efforts in the future. That's something we take very seriously, and I think that will be an ever-growing need in the future.

Mr. TURNER. How many dollars have you expended on cross-agency initiatives and how many of them have been accomplished?

Mr. SPOTILA. Well, I think the reality is that in the past, as John has said, when there have been efforts like crosscutting initiatives, for example, support of the CIO Council and its efforts, we've done that by what John indicates is passing the hat. Under the Clinger-Cohen Act, we have some ability to do that, to have agencies contribute toward support of crosscutting measures.

The President's budget, as I outlined in my testimony, not only includes an increase for computer security in general, but it highlights crosscutting initiatives that we think are very important. John mentioned that for $50 million an awful lot can be accomplished. I think the President's request is actually greater than that in this area because we're also focusing on research and development and on cyberscholarships and the like. Still, we're looking at a relatively small amount of money. $150 million would make a huge impact in this area. The key is to get it appropriated.

And so when we talk about past crosscutting initiatives it's hard to track because we haven't had the kind of appropriations in large numbers that we're talking about here. We have used relatively small amounts of money to support the CIO Council and some other developmental areas along these lines. The GITS Board, for example, worked on the PKI—public key infrastructure— issue for some time. The Board has now been rolled into the CIO Council. We've identified a need to do much more of this going forward. I think the key now will be to see what happens in the appropriations process this fall.

Mr. TURNER. You've requested how many dollars for cross-agency initiatives?

Mr. SPOTILA. We have a list in my testimony that I can just mention, highlight real quickly.

Mr. TURNER. Where would that be found?

Mr. SPOTILA. In my written testimony?

Mr. TURNER. I mean in the budget itself. Is it appropriations in OMB? Is that where the money would reside currently?

Mr. SPOTILA. No. Actually, although these are crosscutting initiatives in the budget, they appear in the departmental submissions. So, for example, the Department of Commerce is seeking $5 million for NIST to establish an expert security review team that can then go to agencies, to a number of different agencies outside of Commerce. That's an example. When we talk about crosscutting initiatives, because of the nature of the appropriations process, it needs to appear in an individual agency's budget. Part of the difficulty is—not to single out Commerce—if that particular appropriations committee or subcommittee doesn't think it a priority, that an expert security review team at Commerce will be helping 25 other agencies, they might give it less support. That's where the difficulty comes in the budget process.

So all of these so-called crosscutting initiatives still appear in individual agency budget submissions.

Mr. TURNER. I think that's one of the things that I have concern about, that perhaps we need some central location, some leadership for this that would flow through our Federal CIOs to be sure that these things happen. Because I think what you're left with, even after you secure the appropriations agency by agency, you're still in the pass-the-hat mode, which I think is one of the problems that we perhaps face in the area that we are discussing.

Thank you, Mr. Chairman. I know my time's expired.

Mr. HORN. Thank you.

Let me followup on that again. There's obviously a concern when you have these cross—the boundaries, if you will, initiatives. Now, can—on reprogramming, you know, $5 million, that's chicken feed to any agency. They have got the—they can reprogram that.

So you don't really need to worry too much. But you're right. If they're trying to help four or five other agencies, the appropriations and authorizers here might say, hey, not on my beat, put them somewhere else. So—but, hopefully, that's why OMB is there, to sort of help straighten it out.

I am not going to embarrass any of the CIOs here, the chief information officers, but have the secretaries and heads of the agencies within the executive branch been responsive to the efforts to strengthen computer security? And I just—perhaps Mr. Gilligan on behalf of the CIO Council, Chief Information Council, do you get a feeling in those meetings that some of them just—these are not, obviously, here. They're other places. But do you get a feeling that they're not getting good backing from the top executives in the agency?

Mr. GILLIGAN. It's my clear sense that the senior executives across the agencies are getting the message. It's a complex issue, and I think the difficulty, as I addressed in my testimony, is understanding both that cybersecurity is important, and understanding what to do about it are two different things, and I think that's, in many cases, where agencies are stuck. It is not an issue that can be delegated down. It has to be undertaken and aggressive leadership has to be provided by senior management, as we found with Y2K.

So I reiterate, I think the actions of the senior levels of the administration, and of this committee and others are going to be important in helping to get that message across. While there are complex technical issues that equate to rocket science, there is a foundation that must be built that is just good sound management practice that requires aggressive involvement at the senior levels.

Mr. HORN. Let me move to another question, that when we had this discussion a few minutes ago on the libertarian suggestions, what message do the grades that we have given you send to the American people regarding the security of the citizens' personal information? Should we have a special category in that as to how that's dealt with in an agency and on those files that such as the census and others are the obvious one over in Commerce? Should we have a category as to how high in the agenda and hierarchy of things to be done that you first protect the information of the American citizen from getting out for people making use of those

data and, therefore, perhaps as we've seen what's happened in credit card operations is some of these idiots take exactly the whole name and number and all the rest of it, and the result is that those poor souls can never get a loan again because somebody's running around the country with their credit card. Well, isn't that also true in some of the agencies here? What do you think, Mr. Spotila?

Mr. SPOTILA. Well, let me start by saying that we take very seriously the importance of preserving the confidentiality of information that the government holds. As we've been discussing throughout this morning, we recognize that, although a lot of progress has been made, we are not done. We cannot afford to be complacent because the challenge in this area is a dynamic one. The threat changes; new technology, new threats can appear. And so, on a day-by-day basis, we need to continue to do the best we can and to improve our efforts.

Without getting into the grades themselves, we all agree here that there is room for improvement. I'm perhaps more sanguine in the sense that I think that the information that we're talking about here is not at great risk. I think the agencies are very careful about protecting that information, as John Dyer indicated at Social Security. They take it very seriously and realize the importance of it. This is not to say that we're complacent. A new threat could emerge tomorrow that hasn't been anticipated, and a part of what you need in the security area is the ability to detect intrusions and to react to them and to correct problems when they surface.

So I would say to the American people that we take security very seriously and that we all need to work together on behalf of the American people in this area.

Mr. HORN. Mr. Willemssen, you've looked at a lot of agencies over the years. What is your answer to that question and how worried should the American people be about this situation?

Mr. WILLEMSSEN. Well, I think—point one, Mr. Chairman, I think it's imperative to point out that absolute protection is not possible, and so we've got to look at this from a risk perspective. And in doing those risk assessments, the higher the sensitivity of systems and data, then the more rigid and tight the controls need to be and agencies need to make that up-front judgment on how much risk for particular systems and data they're willing to accept and, given that acceptance of risk, then put in the appropriate controls.

And I think in many cases we still have agencies who haven't done the in-depth risk assessments of systems and data in order to come to those judgments because not all systems and data are created equal. There has to be some judgments up front on what we absolutely have to protect as best as possible, again recognizing that there is no absolute as it pertains to protection but that we can narrow the margin significantly.

Mr. HORN. Ms. Singleton, would you like to get your licks in, shall we say?

Ms. SINGLETON. I'd like to offer one additional comment along those lines, which is to say that part of the problem that I think the American people might perceive with this system as a whole is that in the private sector if you leak a document—say you work in a law firm and you leak a document about a client. The law firm

stands a good chance of losing its client and you stand a good chance of losing your job. But there's a greater perception I think on the part of the American people—and partly it's correct that, in a Federal Government agency, if there's a leak or a mistake or an error, that there will be relatively lesser consequences for the agency as a whole and for the employee of that agency than there would be in the private sector.

For example, if somebody in the agency does lose your file or give it to the wrong person, you still have to deal with that agency. You can't go to say another Department of Agriculture or another Department of Labor and find a, you know, better security practice there. So I think that also goes to the issue of some of the expense involved, is that it would be very helpful for the perception of the American people to have an understanding that if these policies are violated that there will be real consequences for the agency and for the employees involved.

Mr. HORN. Well, we thank you on that.

I'm going to have a few closing words, and I want to thank the staff and tell you what we're doing tomorrow here.

It's clear that a great deal of attention must be focused on this vital issue. There's a lot of computer security policy out there, but it isn't necessarily being followed by some agencies and others. And when we look at all of the State governments you've got another matter there in terms of privacy. What does it take, legislation? You can be assured if it does we will continue to monitor the government's progress in this area.

This report card sets a baseline for the future oversight. It also is a wake-up call for Federal departments and agencies to begin taking the necessary steps to ensure that the sensitive information contained in the computers will be protected.

Tomorrow at 10 a.m. the subcommittee will hold a related hearing to examine two proposals that would establish the position of a Federal chief information officer. The gentleman from Texas has proposed that. Among other responsibilities, this governmentwide position would be responsible for the government's computer security efforts, and that's one approach, and that's in essence what we asked the President to do in the summer of 1997, was get somebody to put them in charge.

Now, they didn't move for about a year, but when they did move that was exactly what was needed to get the coordination, somebody to be assistant to the President as Mr. Constant was when he was brought back into government, and he did a very fine job of pulling all the pieces together. Because I would ask, has the President brought this up at a Cabinet meeting?

And, Mr. Spotila, I don't know if you know the answer to that, but in the Eisenhower administration, that thing would have been up there 10 years before. That's what Social Security was under the Y2K. They were on their own. There was no administration. They went through three of them in that period that didn't really face up to it until the bells were really ringing.

So that's one of our concerns. But I think the next round we'll have a better feel for how accurately and diligently the agencies are doing it.

I want to thank each of these witnesses today, and I want to thank the staff on both the minority and majority: J. Russell George, staff director, chief counsel of the subcommittee; Randy Kaplan, counsel; on my left, your right, Ben Ritt, professional staff member on loan from the GAO and the one that has had a lot of effort on putting this particular hearing together; Bonnie Heald, director of communications; Bryan Sisk, clerk; Elizabeth Seong, staff assistant; Earl Pierce, also a professional staff member; and George Fraser, intern.

On Mr. Turner's side, Trey Henderson, minority counsel; and Jean Gosa, minority clerk.

Court reporters, Colleen Lynch and Melinda Walker.

May I say that we're now going to end this, and I know the media have wanted to have some questions, and those of you that would like to stay, please, gentlemen, and Ms. Singleton, you're welcome to stay. You're the experts in a lot of these, and I'm sure they'd like to ask you a few questions, but we won't do it in a formal hearing, and we—I don't know how the oath spreads over to a press conference, but we're in recess here. So—till tomorrow anyhow.

[Whereupon, at 11:50 a.m., the subcommittee was adjourned.]

○