128301

UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

FOR RELEASE ON DELIVERY
EXPECTED AT 9:30 AM, EST
TUESDAY, OCTOBER 29, 1985

STATEMENT OF

WILLIAM S. FRANKLIN

ASSOCIATE DIRECTOR

INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

COMMITTEE ON SCIENCE AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ON

AUTOMATED INFORMATION SYSTEMS SECURITY IN FEDERAL CIVIL AGENCIES

033657/128301

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss the status of computer and telecommunications security for selected automated information systems within federal civil agencies. I have with me Dr. Harold J. Podell, Group Director from the Information Management and Technology Division, and Mr. Raymond J. Wyrsch, Senior Attorney from our Office of General Counsel.

Mr. Chairman, as the government becomes increasingly dependent on computers to do its work, automated information systems security takes on even greater importance than before. By using two questionnaires and through subsequent interviews, we surveyed the security status of 25 mission-critical[1] automated information systems at 17 civil agencies.[2] Our survey involved systems that (1) make monthly payments to millions of beneficiaries of various government programs, (2) process electronic funds transfers involving financial institutions, or (3) maintain on-line information essential to safeguarding human safety and the economic vitality of key United States industries. Effective security in these systems is needed to prevent undesirable events, such as denial of benefits to citizens, unauthorized disclosure of sensitive information, loss of government money, waste of federal resources, human injury, and in extreme cases, loss of life and endangerment of the national welfare.

---

[1]Mission-critical systems are defined as those systems that significantly affect agency programs, finances, property, and other resources.

[2]For further details on our objectives, scope, and methodology, see appendix I.

We believe that good automated information systems security consists of two elements: management responsibilities and the establishment of actual security safeguards. Management responsibilities include such steps as those prescribed in Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum No. 1, which requires agency heads to establish policies and procedures and assign responsibilities for automated information systems security. Actual security safeguards are those measures necessary, both in and around automated systems, to protect sensitive mission-critical data. As agreed to by experts, weaknesses in actual security safeguards increase system vulnerabilities and are often attributable to a lack of implementation of management responsibilities.

Generally, the results of our survey showed that each of the systems is vulnerable to abuse, destruction, error, fraud, and waste. Specifically we found that,

--key management responsibilities were missing. For example, many agencies do not use a risk management approach as part of implementing a security program, and

--the actual safeguards needed to protect systems from potential threats were not always in place. For example, computerized techniques (passwords) allowing access to systems were not always periodically changed.

In determining the status of agency automated information systems security, we primarily used the results of the questionnaires, interviews, and existing governmentwide criteria, which included

OMB policy, the National Bureau of Standards' (NBS') Federal Information Processing Standards (FIPS), Office of Personnel Management (OPM) instructions, and expert opinion. We also used the Department of Defense's (DOD's) Trusted Computer Systems Evaluation Criteria, which is being considered for future application by civil agencies. Detailed questionnaire results and potential effects of security problems are presented in the appendices to my statement.

I will now discuss in some detail the status of automated information systems security.

AGENCY SECURITY MANAGEMENT NEEDS IMPROVEMENT

Generally, we found that agencies have not executed all the management responsibilities, most of which are prescribed in current OMB policy and supplemented by NBS guidelines and OPM instructions. These management responsibilities are: risk management, training, assigned responsibility, budgeting and accounting for security costs, automatic data processing (ADP) personnel security, contingency plans, independent audit and evaluation, and written procedures. All of these responsibilities must be implemented in order to establish an effective combination of security safeguards. For example, ADP personnel security is needed to adequately protect the system from undesirable employee actions.

As you can see in our first chart, no one management element was implemented for all of the 25 systems. Note also that training, ADP personnel security, assigned responsibility, and

budgeting and accounting for security costs were implemented for only a few systems. Two of these key management responsibilities, namely, automated information systems security training and risk management, deserve special mention.

Security training is important to ensure that agency personnel involved in the management, operation, programming, maintenance, or use of information technology are aware of and know how to meet their security responsibilities. This point was recognized in your Subcommittee's April 1984 report[3] on computer and communications security and privacy, which recommended that expanded training for all employees associated with automated information systems is needed so that they understand their roles for protecting sensitive data. While most agencies have some security training policies and/or procedures, only two have made efforts to formalize their approach by identifying, for example, audiences, course subjects needed, frequency of training, etc. Without a formalized approach, agencies cannot provide the necessary foundation for improving the security of automated information systems.

The second management responsibility we would emphasize is risk management. The objective of this approach is to strike an economic balance between the expected loss associated with the risk and the cost of protective safeguards. The approach should include

---

[3]Computer and Communications Security and Privacy. (Report prepared by the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology, dated Apr. 1984.)

determinations of (1) data sensitivity; (2) system vulnerabilities, threats, and risks; (3) alternative safeguards, their costs, and relative benefits; and (4) the most appropriate safeguards. Otherwise, agencies have less assurance that they are properly protecting the automated information systems effectively and economically. Risk management was applied to only eight of the systems studied.

In looking at the other management responsibilities, we also found weaknesses. For example, while contingency plans were developed for 18 systems, only 9 of them were tested. Failing to meet responsibilities like this one can have an undesirable effect on the security of systems. For example, without developing and testing contingency plans, organized recoveries in the event of a major emergency are not assured.

Chart 2 shows examples of potential effects of missing management elements. Such deficiencies are of particular concern because they can lead to weaknesses in the security safeguards, my next topic.

USE OF PHYSICAL, TECHNICAL, AND ADMINISTRATIVE SAFEGUARDS NEEDS IMPROVEMENT

There are three categories of safeguards: physical, technical and administrative. These are established in OMB Circular A-71, Transmittal Memorandum No. 1. The necessary protection levels and combinations of safeguards should be identified in the risk management process. Although there is no such thing as absolute security, a balance of these three categories of safeguards is needed.

Without such a balance, existing controls may be more easily circumvented. For example, without adequate separation of duties technical safeguards may be bypassed.

As you can see from chart 3, only five systems contained each of the physical, technical, and administrative safeguards evaluated. I would now like to briefly discuss each of the three categories of safeguards.

Physical safeguards include measures, such as locks, badges, alarms, or similar devices, to protect personnel and property from damage by accident, fire, loss of utilities, environmental hazards, and unauthorized access. This category does not have as severe problems as other categories. However, as the chart shows, only 16 out of 25 mission-critical systems were protected by physical perimeters, such as fences or detection devices, outside the computer facility. Although agencies have taken steps to implement many of the physical safeguards, one might reasonably expect a computer center processing mission-critical systems to have some form of each of these.

Technical safeguards are automated system features that help control access, limit user privilege, maintain program and data integrity, and provide the needed tools for detecting security violations. For criteria in assessing technical safeguards, we used selected provisions of the DOD Trusted Computer Systems Evaluation Criteria--to date the most comprehensive criteria for establishing technical safeguards. We used selected provisions that we believe are most appropriate for civil agency implementation.

One of the important technical safeguards is the capability of the system to identify and authenticate users. Mechanisms such as passwords and user identification are generally accepted techniques to accomplish this objective. It is necessary that these mechanisms be protected by the system so their identity cannot be compromised. Twenty-three of the 25 systems contained this capability.

Another important technical safeguard is the maintenance of audit trails. An audit trail is a record that collectively provides documentary evidence of processing and should disclose (1) all attempted or actual accesses to the systems, programs, or files; (2) deletion or modifications of files; and (3) all system activity initiated by computer operators, system administrators, and/or system security officers. Only 10 systems meet these criteria.

The final category shown on the chart involves administrative safeguards. These are non-automated techniques for safeguarding information systems and include procedures, practices, separation of duties, and a broad range of other techniques. Administrative safeguards are essential to complement physical and technical safeguards to ensure that the risks to automated information systems are reduced to an acceptable level.

Agencies have weaknesses in key administrative safeguards. One of the major threats to any automated information system is from inside the organization, namely, intentional and unintentional actions of employees. For instance, separation of duties is

intended to prevent unauthorized actions by employees. We found that written procedures and/or organizational structures did not always provide for separation of duties necessary for the execution of critical functions.

We also found five instances where data processing security procedures were not tested to ensure that they were effective. Also, agencies responded that passwords were required for 24 systems. However, we found three cases where passwords were not required to be changed.

Chart 4 shows the potential effect of not having selected safeguards in place. For example, without audit trails there are limited means to track actions or security violations or to determine quickly, the impact of unauthorized access to the system or agency. Without testing security safeguards there is less assurance that they are working.

In conclusion, no agency met all management responsibilities, and only five systems evaluated contained each of the safeguards studied. Improvements are needed in both of these important areas. With regard to making these improvements, officials of several agencies cited reasons for the shortfalls in implementing management responsibilities and security safeguards. These included a lack of (1) management commitment, (2) funds and resources, and (3) assistance in implementing policy and guidance. Therefore, Mr. Chairman, these determinations lead us to conclude that the automated information systems studied are vulnerable to threats and their potential effects. It is the responsibility of agency heads to ensure that policy and guidance emanating from the

responsible central agencies are implemented. Our survey indicates that such policy and guidance often are not implemented.

- - - - -

This completes my prepared remarks. We would be pleased to answer any questions that you may have.

Contents

OBJECTIVES, SCOPE AND METHODOLOGY

On August 7, 1984, the Chairman, Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology requested that we assess the extent to which selected federal agencies are protecting the data in automated information systems for which they are responsible. For our review, we selected 25 mission-critical automated information systems at 17 federal civil agencies. After selecting the agencies and the systems, we met with Subcommittee staff to obtain their concurrence.

To assess the security status of these systems, we used existing criteria and two questionnaires which focused on two interrelated issues to collect relevant information about the security status of the systems.

One issue primarily involved Office of Management and Budget (OMB) policy reflected in OMB Circular A-71, Transmittal Memorandum No. 1, which focuses on automated information systems security management responsibilities. Criteria used to develop this management questionnaire were supplemented by National Bureau of Standards (NBS) Federal Information Processing Standards (FIPS), Office of Personnel Management (OPM) instructions, and expert opinion.

The second questionnaire focused on the actual security safeguards for mission-critical automated information systems. The questions were developed primarily using the Department of Defense (DOD) Trusted Computer System Evaluation Criteria, NBS Federal Information Processing Standards, and expert opinion including NBS, National Computer Security Center (NCSC), and the Department of Defense Computer Institute (DODCI).

We also developed scenarios of the potential effects of problems in areas such as those covered in the aforementioned questionnaires. These scenarios show how systems are vulnerable when certain management responsibilities and security safeguards are not in place. We validated these potential effects with the NBS, the NCSC, and the DODCI.

Follow up interviews were held at several agencies to validate the responses received from the two questionnaires, and exit conferences to present the results of our survey were held with all agencies. This survey did not involve testing the effectiveness of the management responsibilities and safeguards.

The following appendices reflect the aggregated detailed results of the survey and disclose (1) a list of the 17 agencies surveyed, (2) aggregated survey results of the questionnaires including general information; management responsibility elements; physical, administrative, and technical safeguards; and other

security information obtained from the questionnaires, (3) management responsibilities and scenarios of potential effects of weaknesses in the responsibilities assigned, and (4) physical, administrative, and technical safeguards and scenarios of potential effects of safeguards not in place. Appendix III identifies the potential effects of weaknesses in management responsibilities, such as those identified in appendix II, and appendix IV identifies the potential effects of weaknesses in security safeguards also shown in appendix II.

APPENDIX I

FEDERAL AGENCIES INCLUDED
IN
AUTOMATED INFORMATION SYSTEMS SECURITY SURVEY

DEPARTMENT OF AGRICULTURE

DEPARTMENT OF COMMERCE

DEPARTMENT OF EDUCATION

DEPARTMENT OF ENERGY

DEPARTMENT OF HEALTH AND HUMAN SERVICES

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

DEPARTMENT OF INTERIOR

DEPARTMENT OF JUSTICE

DEPARTMENT OF LABOR

DEPARTMENT OF STATE

DEPARTMENT OF TRANSPORTATION

DEPARTMENT OF TREASURY

FEDERAL RESERVE SYSTEM

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

SMALL BUSINESS ADMINISTRATION

VETERANS ADMINISTRATION

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS [1]
GENERAL INFORMATION	
Length of Time this Information System has been Operational	
Less than 1 year	1
At least 1 year	2
At least 5 years	11
10 years or more	11
People/Institutions having System Accounts	
0	2
1 - 25	5
26 - 200	5
201 - 1,000	6
1,001 or more	7
MANAGEMENT RESPONSIBILITIES	
Risk Management	
Risk analysis within past 5 years	19
Risk management procedures	14
Risk analysis used to determine current level of security control	14
Contingency Plans	
Plan exists	18
Plan is tested	9
Assigned Responsibility for Computer Security	
Security officers' position description contain security responsibilities	20
ADP personnel position descriptions contain security responsibilities	4
Information Systems Security Officer (ISSO) Assigned	23
Written Procedures for Computer Security	
Facility procedures	22
Overall policies & procedures	13
ADP Personnel Security	
Position sensitivity levels designated	17
Use of new OPM regulations	2
Use of old OPM regulations	18

[1]Systems do not always add to 25 because of non-response to certain questions.

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS
Computer Security Costs	
Budgeted and accounted for separately	1
Computer Security Training Program	
Policies and/or procedures	19
Formal program	2
Audits and/or Evaluations	
Evaluation performed	22
Independent and within past 3 years	19
PHYSICAL SAFEGUARDS	
Physical Perimeter	16
Physical Access	All
Electronic Monitoring	
Computer room	7
Computer room access halls	9
Building access	13
Badge Entry	23
Security Guards	22
Cypher Locks	14
Various Detectors	
Metal	3
Smoke	23
Heat	24
ADMINISTRATIVE SAFEGUARDS	
Written procedures for safeguarding this system's information contained on microcomputers and related storage media at the information center	2 *
Written procedures for safeguarding this system's information while it is being transmitted between the microcomputers and related storage media at the information center	1 *

*Not applicable to all systems reviewed.

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS
ADP positions at the information center designated in terms of sensitivity.....	17
Federal Personnel Manual, Chapter 732, used for ADP positions at the information center	3
Background investigations in compliance with Federal Personnel Manual 732 for information center personnel	
Data entry personnel	15
End Users	12
Security officers	21
Systems Programmers	20
Contractors	16
Systems Analysts	17
Application Programmers	18
Computer Operators	18
ADP Auditors	11
Data base Administrators or Managers	18
Communications personnel	16
For the ADP personnel at the information center, to what extent does the organization comply with the background investigations provisions of OPM's FPM, Chapter 736	
To little or no extent	1
To some extent	None
To a moderate extent	2
To a substantial extent	10
Fully	9
Tested the Physical, Administrative and Technical Procedures	20
Review Audit Trail Information	10
Formal Security Procedures Manual at the Information Center	
For all systems	16
For this system	3
Separation of Duties in the Following Areas	
Input processing	21
Error correction	21

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS
Software design, development, test and operation	19
System programming and data base administration	21
Computer operations, telecommunications, and maintenance	24
Computer and telecommunications security	19
System access - retrieval	18
System access - update processing	19
Unescorted System Maintenance Personnel Access to System	13
Unescorted System Maintenance Personnel with Clearances at Highest Level of Data Processed	10
Inactive Accounts Purged?	
Never done	2
Upon reassignment or employment termination	21
Upon termination of a system account	9
At least once a year	14
Longer than a year	1
Frequency of Password Changed for this System	
Not required to be changed	3
At least every 3 months	9
Between 3 and 6 months	6
Between 6 and 12 months	5
More than 12 months	1
Passwords are Changed by	
User	12
System administrator/security administrator	11
System, centrally managed by an administrator	4
System, independent of an administrator	1
Passwords are Distributed by	
Letter	8
Electronically from the system	3
Discussion with ISSO	7
User creates and maintains	11

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS
TECHNICAL SAFEGUARDS	
Identification and Authentication	23
Audit Trails or Logs	10
Discretionary Access Controls (Authorization) ..	24
Restrictive Markings Limit Access to Data	10
Users have Access to all Data in the System	2
Software Changes are Recorded	
Manually	20
Automatically	15
Not recorded	None
No changes are allowed	1
Uses Add-On Security Software	17
Users are Automatically Informed at each Log-on of the Time and Date of Last Log-on	5
Users are Automatically Notified at each Log-on of Invalid Attempts to Use the System Account	2
Use Encryption (encoding) Techniques	Few*
TELECOMMUNICATIONS SECURITY	
Off-hours Access Via Leased or Dial-up Lines ...	16*
Anti-Hacker Devices	
Dial back capability	Few*

*Not applicable to all systems reviewed.

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS
Never Permit Maintenance Personnel to Perform Hardware/Software Diagnostics Via Unclassified Dial-up Lines	13*
Lines Leaving Afforded Transmission Protection	Few*
CONTRACTOR SECURITY	
Role of Contractors for the Hardware Operation and Maintenance	
Operated and routinely maintained by agency personnel	2
Operated by agency personnel but routinely maintained by contractor	14
Operated and routinely maintained by contractor	9
Operated by contractor but routinely maintained by agency personnel	None
Role of Contractors for the Software Operations and Maintenance	
Operated and routinely maintained by agency personnel	14
Operated by agency personnel but routinely maintained by contractor	3
Operated and routinely maintained by contractor	7
Operated by contractor but routinely maintained by agency personnel	None
CONTINGENCY PLANS	
Center Experienced an Unplanned Operational Discontinuity	19
Unplanned Discontinuity Occurred	
Less than 1 year ago	13
From 1 to 3 years	6
More than 3 years ago	None

*Not applicable to all systems reviewed.

QUESTIONNAIRE RESULTS

ELEMENTS EVALUATED	NO. OF SYSTEMS
Uninterruptible Power Supply	13
Type of Uninterruptible Power Supply	
Battery	1
Generator	2
Both generator and battery	12
SECURITY MANAGEMENT APPROACH	
Staff Effort Devoted to System Security Functions	
None	None
1/2 staff year or less	7
More than 1/2, but less than 1 staff year ...	4
1 staff year, but less than 3 staff years ...	5
3 staff years, but less than 5 staff years ..	3
5 staff years or more	5

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
Agencies should establish an agency computer (automated information) security program at a management level commensurate with responsibilities involved and with sufficient authority to enforce established requirements.	AGENCY SECURITY PROGRAM	
	An agency computer and telecommunications (automated information) security program at appropriate management level.	Inadequate program can lead to inadequate implementation and control.
	Authority to enforce program requirements	Insufficient authority tends to perpetuate known weaknesses and prevent identification of unknown weaknesses.
The program should		
1. Establish a formal ADP System Security Organizational Framework that	1 ORGANIZATIONAL FRAMEWORK	
	Formal (written) responsibility and authorities that	
—assign responsibilities and authorities for security of data processing installations, security officers, users, operators, and contractors via procedures and contract clauses.	are clear and not overlapping or fragmented.	Unclear, overlapping and fragmented responsibilities can lead to organizational procrastination in identifying and implementing safeguards and duplication of effort. Control problems go undetected or uncorrected for periods longer than necessary.
	clearly define responsibilities of (see next page)	

APPENDIX III

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
	—data processing installation personnel,	Effective management can be negated if security is not perceived as part of total job responsibility and stated in employee position descriptions. Causes procrastination and duplication since the position description is a major source of accountability and enforcement.
	—managers,	(SAME EFFECT AS ABOVE)
	—primary users,	If responsibilities and accountabilities are not spelled out in position descriptions, persons/organizations most knowledgeable of data sensitivity and possible harm or loss may not be involved in automated information systems security decisions.
	—monitoring entities (evaluation),	Adequacy of automated information systems security program and controls may not be evaluated, if position descriptions are devoid of responsibilities for automated information systems security.
	—contractors,	Insufficient contract clauses specifying contractor responsibilities and authorities causes enforcement, procrastination, duplication and other problems.
	—security officers.	Position descriptions that do not clearly describe responsibilities and authorities for automated information systems security can cause unresolved clashes with ADP operations and users. Clashes among security officers also may not be resolved. Needed controls can go unimplemented or problems undetected.

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
2 Formulate a comprehensive ADP Systems automated information systems security policy.	2 ADP SYSTEM SECURITY POLICY The existence of policy.	Absence of, or unclear policy can result in no clear organizational position. Controls could not be implemented or enforced because of confusion.
3 Develop written comprehensive ADP systems security standards and procedures applicable to all organizational units responsible for processing and protecting data.	3 STANDARDS AND PROCEDURES For developing, implementing and operating the automated information systems security program. They should cover	
	—appropriate organizational entities and people.	If entities and employees are uninformed of their role for effective security, control violations or problems can be created.
	—risk management and data sensitivity.	Failure to require and use data sensitivity and risk management can lead to overprotection or underprotection. Appropriate levels of controls to afford cost-effective protections can not be determined.

APPENDIX III

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
	—budgeting and costing.	Lack of security budgeting and costing can result in uncontrolled overprotection, failure to identify inadequate controls, resource conflicts leading to inadequate safeguards, inability to monitor cost-effectiveness of controls, compare costs, monitor plans, etc.
	—training.	See "training and awareness programs."
	—security planning.	Inadequate planning can lead to inadequate program implementation and exposed vulnerabilities because of inadequate controls.
	—types of data and processing covered.	Sensitive data in hands of those unaware of protection requirements is a vulnerability. Importance increased because of end user computing. Information processes not covered also represents a vulnerability.
	—mechanisms for corrective actions (reporting and follow up).	Poor or no procedures or mechanisms for assuring effective corrective actions can lead to control problems detected which are not always corrected, or corrective actions which do not work effectively.

APPENDIX III

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
4 Require the formulation and testing of backup and recovery contingency plans.	4 CONTINGENCY PLANS	
	The existence of plan.	Mission can be impaired with significant discontinuity if no plan exists. Human safety can be endangered in some applications.
	Testing of plans.	If existing plans are not tested, backup plans may not be effective, again leading to potential mission impairment.
5 Assign responsibilities for conducting periodic risk analysis and implement cost effective technical, administrative, and physical safeguards based on a risk management approach.	5 RISK MANAGEMENT	
	Responsibilities assigned for conducting periodic risk analysis.	Unclear assignment of responsibilities may result in not conducting or improperly conducted risk analysis. This can impact control effectiveness since it forms basis for selecting proper mix of controls.
	Use of risk management approach for implementing controls.	Insufficient compliance in performing risk analysis and using risk management approach can lead to not identifying or implementing cost effective controls (underprotection). Costly overprotection (without closing vulnerability) is also a possible result.
	Determining data sensitivity and data sensitivity levels.	If data sensitivity determinations are not being made or levels not established, then risk management can result in inadequate controls for highly sensitive data leading to high risk (underprotection). Data sensitivity, including criticality and value, is a key factor in risk management. Its absence negates the risk management process.

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
	Elements of risk management approach employed (data sensitivity, vulnerabilities, threats, risks, alternative safeguards, costs, relative effectiveness, etc.).	Not using risk management approach can result in cost effective safeguards not identified or implemented. Over or underprotection is possible while vulnerabilities remain.
	Frequency of risk analysis and changes in circumstances.	Major changes in circumstances may create new vulnerabilities, threats and increased risks which need to be identified and safeguarded. If risk analysis is not done periodically or when circumstances change (modification, new site, employee changes, and changes in processing procedures) they may not be identified.
6 Establish personnel security policies for screening all individuals participating in design, operation, maintenance, or having access to data in federal computer systems.	6 PERSONNEL SECURITY	
	Existence of policies for screening personnel.	Absence of policy may result in overscreening or underscreening.
	Responsibilities for implementing policy.	Unclear responsibilities can result in organizational procrastination or duplication. Personnel control (screening) may be inadequate.
	Effectiveness of implementing policy.	Ineffective policy may result in overscreening or underscreening.

APPENDIX III

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
	Designation of sensitive positions	If ADP positions are not designated in terms of sensitivity, then there may be an inappropriate basis for performing background checks. A major threat to systems is employees. Employees in sensitive positions can exploit controls and commit fraud and abuse.
	Use of sensitivity levels for ADP positions.	Levels of sensitivity needed are for managing extent of personnel control.
	Background investigations performed	
	for all applicable personnel.	Employees are a major threat to systems. If checks are not performed for all applicable personnel there is insufficient basis for trust. Controls can be exploited.
	updates of background investigations.	Since people and circumstances change, infrequent updates of investigations may result in not identifying a new threat.
	clearance information used in risk management.	Threat of unauthorized access is increased if clearance information is not used in performing risk management.

APPENDIX III

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
7 Establish management control process	7 MANAGEMENT CONTROL	
a) to budget and account for computer and telecommunications security costs and resources, for planning, risk management, and control purposes.	Budgeting and accounting and/or estimating where appropriate for security costs and resources.	Lack of awareness of security costs and related cost components for systems and agencies can result in uncontrolled overprotection, failure to identify inadequate controls, and inability to monitor cost-effectiveness of controls, etc.
	Use of budget and cost for planning, and control.	Management planning and control is not fully effective without knowledge of costs.
	Use of budget and cost in risk management.	Risk management is not effective without knowledge of costs of alternative controls.
b) to evaluate risk analysis.	Agency evaluation of risk management approaches.	Risk management approaches used may not be appropriate if not evaluated. Impact on control effectiveness is a possible result.
	Agency evaluation of risk analysis conducted.	Risk management effort may not be adequate if not evaluated. Impact on control effectiveness is a possible result.

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL EFFECT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
c) involving procedures and mechanisms to assure that exposed vulnerabilities or corrective actions recommended are adequately and effectively acted on.	Follow up on recommendations.	Failure to act on recommendations to correct problems (vulnerabilities, etc.) because of poor or no procedures or mechanisms for taking corrective actions, can result in vulnerabilities which remain (unsecured), and controls in place which may not be totally effective.
8 Establish an annual security plan.	8 ANNUAL SECURITY PLAN	
	Existence of plan	Inadequate planning can lead to inadequate control.
9 Establish comprehensive automated information Security Training and Awareness Programs and manage it to assure its effectiveness.	9 TRAINING AND AWARENESS PROGRAMS	
	Existence of training program, which should include	Employees responsible for sensitive data, if untrained, may be unaware of controls available, responsibilities, potential impacts, etc. Existing controls may not be effective.
	audience.	If user awareness of vulnerabilities and controls are not a primary target, then the user may be unaware of how to effectively implement controls.
	training content (topics).	Proper subjects not presented to employees can render controls ineffective.

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL IMPACT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
	feedback to determine effectiveness (testing etc.).	Making an assumption that training is effective without requiring and receiving feedback can result in inadequate controls implemented by employees or commission of errors causing damage.
	training of security officer.	Inadequate training of security officers can lead to inadequate controls.
10 Establish agency program for conducting audits and evaluations to determine the compliance with and cost effectiveness of the security program.	10 AUDITS AND EVALUATIONS (MONITORING)	
	Existence of periodic independent audits.	Without independent evaluation, there is no validation that cost effective controls exist.
	Certifications and recertifications.	Without certification and/or recertification, inadequate controls may continue to exist.
	Implementation of recommendations.	Without sufficient follow-up, needed controls and safeguards may not be implemented or may not work effectively.

MANAGEMENT CRITERIA, AND POTENTIAL IMPACTS ON SAFEGUARDS
Analysis of Management Responsibilities for Computer and Telecommunications Security

MANAGEMENT CRITERIA AND STANDARDS	CRITICAL RESPONSIBILITIES	POTENTIAL IMPACT OF WEAKNESSES (ON SAFEGUARDS AND CONTROLS)
11 Actively monitor the application of computer and telecommunications security by contractors performing data processing for the federal government.	11 SECURITY BY CONTRACTORS	
	Monitoring of contractor security measures.	Without monitoring, needed controls may not be implemented. Also controls implemented by contractor may not be effective.
	Procedures for protecting assets when contractors change.	Vulnerability is created by changes in contractor/ employees. Assets and data are vulnerable.

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARDS NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Physical		
Physical Controls	Physical security controls should exist and be adequate.	Poor physical security allows unauthorized access to information resources. Physical security is becoming increasingly important because of portability and size of micro-computer systems.
Administrative		
Testing Procedures	Security procedures and features should be tested.	Without independent testing of security safeguards there is less assurance that controls are in place and/or working effectively.
Separation of Duties	Procedures and/or partitions should exist to ensure separation of duties.	Major threat is from inside the organization. Separation of duties is a key internal control (administrative safeguard) to prevent internal intrusion without collusion.
Position Sensitivity Levels	Personnel positions at the information (computer) center should be designated in terms of sensitivity.	If positions are not designated in terms of sensitivity there is little basis for decisions about the level of access to be granted to individual employees, the extent and nature of background checks, duties to be separated, procedures for disgruntled employees etc.

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARD NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Position Sensitivity Designation	OPM FPM Chapter 732 INSTR 311 should be used to identify sensitivity levels for ADP and other key positions.	Without using a standard to identify sensitivity levels for federal personnel involved in ADP processing, differences in criteria can lead to unidentified potential threats.
Background Investigations	Background investigations should be performed in accordance with OPM FPM 732, Chapter 736.	Insufficient background investigations may result in the failure to disclose a primary threat to the information system.
Update Background Investigations	Updates of background investigations should be performed periodically.	Circumstances and habits change and updates are needed to disclose significant changes which may pose a threat to the system.
Change Passwords	Password changes should be required and performed frequently.	Not changing passwords leave systems vulnerable to attack by former employees.
Generation of Passwords	Users should not generate their own passwords when they are changed (unless NBS FIPS is used).	Undertrained users may not be sufficiently aware of the pitfalls of using passwords that are easy to break. Users may be inclined to use birth date, wedding anniversary, names, short passwords or other personal identifiers that are more easily broken based on personal knowledge of the individual. Use of NBS FIPS is needed for sensitive systems.

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARD NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Audit Trails Reviewed	Reviews of audit trails for security should be made, performed frequently and effectively.	Existence of an audit trail (a technical control) is not sufficient. Frequent reviews are needed to determine if irregularity exists. Audit trails are not an effective violation detection mechanism unless such reviews are effectively performed and detection is followed up.
Microcomputer Procedures	Procedures should exist for protecting data while residing on microcomputers and for protecting information being transmitted between microcomputers and mainframe computers.	Without procedures, data from or for system may not be protected on microcomputers. Sensitive or costly information on microcomputers must be protected regardless of its source. Sensitive information being transmitted between computers must be safeguarded to an extent dependent on risk management.
Security Procedures Manual	There should be a formal security procedures manual at the information center (computer center).	Without formal procedures, training and actual use, implementation of control can be haphazard. Some employees, e.g. new hires, may be unfamiliar with controls and accidently violate them.
Restrictive Markings	There should be restrictive markings that limit access to data at the information center (computer center).	Without restrictive markings for sensitive data, employees may not be aware of its sensitivity, and may not implement effective control in its handling and use.

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARD NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Clearances-maintenance personnel	Unescorted maintenance personnel who have access to the system should have appropriate clearances or authorizations.	Maintenance personnel represent a threat of unauthorized access to the system. Escorts and clearances are basic safeguards against this threat.
System Accounts Purged	The status of individual system accounts should be reviewed periodically and inactive accounts purged.	Access accounts should be up to date to be an effective technical control. Reviews should be done frequently and when an individual is reassigned or terminated. Failure to review and purge inactive accounts can lead to use of accounts of terminated or reassigned employees to access the authorization.

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARDS NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD*	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Technical		
Discretionary Access Control	Software or hardware protection should exist to protect user files via access control lists, file passwords or class of user. (LEVEL C1)	May not have the required technical access control needed to deter unauthorized access (e.g. extent of complexity, sophistication and cost), which should be dependent on risk levels, and risk management. The overall system effectiveness of technical access controls rest to a large degree on the balance of administration of password updates and changes, personnel and other administrative controls with the supporting technical controls. Poor administration of these technical controls can potentially result in their circumvention leading to system violation.

*Minimum level requirements contained in the DOD Trusted Computer System Evaluation Criteria.

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARDS NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD*	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Identification and Authentication	The system should possess identification/ authentication features e.g. log on/password which uniquely identifies an individual and is protected by the software/hardware from unauthorized acquisition and modification. (LEVEL C1)	The system does not identify the source of authorization and identification e.g. institution or user. This is needed to determine potential sources of intrusion, leak, usage history and to effectively validate user's authority. Passwords and other identification and authentication mechanisms are not protected and are more easily disclosed.

*Minimum level requirements contained in the DOD Trusted Computer System Evaluation Criteria.

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARDS NOT IN PLACE

CATEGORY OF TECHNICAL CONTROLS	TYPE OF SAFEGUARD*	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Audit	System should have capability to record in an audit trail or console log attempts at log on, file accesses, network access, security violations, user privilege changes, security review actions, and console operator actions. It should record users actions by individual identity and/or security level. (LEVEL C2)	No means to track system/ network accesses or security violation. Unable to monitor actions being taken by persons responsible for performing security reviews. Unable to identify user privilege changes by computer. Audit trail weaknesses limit the means for detecting unauthorized access to system and to determine, quickly, the impact on the system and agency. Can also impede effective recovery. Poor administrative control related to audit trail (e.g. failing to review audit trail frequently, or at all for security purposes) could render this detection, and correction technical control ineffective.

*Minimum level requirements contained in the DOD Trusted Computer System Evaluation Criteria.

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARDS NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Uninterruptable Power Supply	Uninterruptable Power Supply should be used where justified.	Mission can be degraded or impeded and data can be lost.
Transmission Protection	Telecommunications lines should be encrypted or physically secured where justified.	Transmission over telecommunications lines represents a vulnerability to the unauthorized access, monitoring, or altering of automated data.
Log-on Notification	The system should inform user at log on of prior (last) log on date and time.	Without control for sensitive systems, user is not aware of unauthorized use of his/her access code. Control could lead to the identification (detection) of unauthorized access to system.
Invalid Attempts Notification	The system should notify the user (at log on) of invalid attempts to use system accounts.	Absence of control could delay or prevent timely detection of unauthorized access and delay or prevent timely apprehension of perpetrator. Notifying security officers may be even more desirable.

APPENDIX IV

POTENTIAL EFFECTS OF SAFEGUARDS NOT IN PLACE

CATEGORY OF SAFEGUARD	TYPE OF SAFEGUARD	POTENTIAL EFFECT IF SAFEGUARD NOT IN PLACE
Encryption	Encryption should be used to secure sensitive or compartmented data.	In critical or particularly sensitive systems, encryption is dependent on risk management. However encryption of key data such as passwords, as well as sensitive data (at certain levels) may be a cost effective control.
Error Reports	The system should produce reports that specify actual or estimated error rates.	Integrity and accuracy are significant considerations in system security. Errors and sources need to be detected and corrective action taken. A system can detect and/or correct many types of (but not all) errors. Erroneous data can lead to mission impairment, uneconomical actions, and human safety problems.

COMPUTER SECURITY MANAGEMENT EVALUATION

Management Responsibilities*	Number of Systems Meeting Requirements
Risk Management	8
Training	2
ADP Personnel Security	2
Assigned Responsibility	4
Budgeting and Accounting for Security Cost	1
Contingency Plans (exist and tested)	9
Independent Evaluation or Audit	19
Written Procedures	11

*Elements of criteria used to evaluate agency implementation of each of these management responsibilities are shown in appendix II.

CHART 1

POTENTIAL EFFECTS
MANAGEMENT RESPONSIBILITIES
NOT IN PLACE

RESPONSIBILITY	POTENTIAL EFFECT
Lack of Risk Management	Controls missing and/or not cost effective.
Lack of Continuity of Operations Plan and Testing the Plan	Mission can be impaired and human safety endangered.
Lack of a security training program	Employees unaware of controls needed.
Lack of independent audits and evaluations	No validation that controls exist.

CHART 2

PHYSICAL, TECHNICAL, AND ADMINISTRATIVE SECURITY SAFEGUARDS

	SYSTEMS HAVING SAFEGUARDS
PHYSICAL SAFEGUARDS	
Physical Perimeter	16
Entry by Badge or Cypher Lock	24
Use of Security Guards	22
Use of Smoke and/or Heat Detectors	24
TECHNICAL SAFEGUARDS	
Identification and Authentication	23
Audit Trails or Logs	10
Discretionary Access Controls (Authorization)	24
ADMINISTRATIVE SAFEGUARDS	
Separation of Duties	15
Physical, Administrative and Technical Procedures Tested	20
Audit Trail Information Reviewed	10
Passwords Required to be Changed	21
HAVE ALL SAFEGUARDS	5*

*Although these systems contained all evaluated safeguards, they may still be vulnerable because (1) GAO evaluated selected safeguards only, and (2) all evaluated management responsibilities were not implemented. GAO does not know how vulnerable the systems may be because this survey did not involve testing the effectiveness of the safeguards.

CHART 3

APPENDIX V

POTENTIAL EFFECTS PHYSICAL, ADMINISTRATIVE, AND TECHNICAL SAFEGUARDS NOT IN PLACE

SAFEGUARD	POTENTIAL IMPACT
Lack of Physical Safeguards	Unauthorized access possible.
Lack of Testing Security Procedures	Less assurance that safeguards are working.
Lack of Separation of Duties	Threat of employee fraud and abuse is increased.
Lack of Audit Trails	Detection of unauthorized access limited.

CHART 4

32653