

GAO

Report to the Chairman, Information,
Justice, Transportation, and Agriculture
Subcommittee, Committee on
Government Operations, House of
Representatives

October 1993

**CLASSIFIED
INFORMATION**

**Costs of Protection Are
Integrated With Other
Security Costs**





United States
General Accounting Office
Washington, D.C. 20548

National Security and
International Affairs Division

B-253976

October 20, 1993

The Honorable Gary A. Condit
Chairman, Information, Justice,
Transportation, and Agriculture
Subcommittee
Committee on Government Operations
House of Representatives

Dear Mr. Chairman:

This report is in response to the former Chairman's request that we review the costs involved in protecting national security information. Specifically, we obtained annual cost information pertaining to classified information safeguards at selected levels and areas of the government, as agreed with subcommittee staff. Some categories of information are aggregated on a governmentwide basis but much of it applies to the Department of Defense, two of its component agencies, and the Department of State. Costs for the Department of Energy, Central Intelligence Agency, and special access programs are excluded. We also obtained information on Defense Department efforts to standardize and reduce costs. (See app. VI for a more detailed discussion of our objective, scope, and methodology.)

Results in Brief

We were able to identify governmentwide costs directly applicable to national security information totaling over \$350 million for 1992. This included at least \$239 million for security clearances; \$58 million for safes, secure telephones, and commonly used encryption devices; \$49 million for courier services, and \$6 million for declassification work.

However, the U.S. government also spends additional billions of dollars annually to safeguard information, personnel, and property. The portion of these costs that is additionally incurred because of national security information requirements is not readily discernable. The Department of Defense, for example, spent about \$6 billion on security activities in 1991, but \$3.1 billion was for physical safeguards to protect much more than just classified information. Another \$1.4 billion was spent to secure communications and computers that can also be used for sensitive, but unclassified, information. It was also estimated that the Department incurred costs of \$674 million to perform administration and management tasks associated with safeguarding information.

The Defense Department has taken action to standardize procedures, consolidate programs, and reduce some security costs.

Background

Executive Order 12356, National Security Information, provides the foundation for classifying, declassifying, and safeguarding information related to the national defense and foreign relations of the federal government. The order, implemented in 1982, continued the three-tier security classification system of confidential, secret, and top secret. It also required that agencies establish (1) controls to ensure that classified information is adequately protected when used, processed, stored, reproduced, transmitted, and destroyed and (2) procedures for the systematic and mandatory declassification of classified information. On April 26, 1993, a Presidential Review Directive was issued directing that the order be reviewed, with a view toward drafting a new executive order that reflects the need to classify and safeguard national security information in the post-Cold War period. The review is to be completed on November 30, 1993.¹

The General Services Administration's Information Security Oversight Office oversees and monitors federal agency implementation of the executive order. According to the Oversight Office, 6.3 million classification decisions were made by government agencies in fiscal year 1992. The total consisted of 562,031 top secret decisions, 4.3 million secret decisions, and 1.5 million confidential decisions. Classification decisions can range from classifying a few words in a document to an entire document.

Few Governmentwide Costs Identified

Some governmentwide activities and procurement are sufficiently discrete to allow for the identification of the costs of protecting classified information. We identified a total of over \$350 million spent by the government in fiscal year 1992 for safeguarding classified information. Even though the items we identified were primarily purchased for national security classification uses, some of the equipment may be used for other purposes.

During fiscal year 1992, the U.S. government spent at least \$239 million on investigations and analyses of results in order to grant or continue personnel security clearances. The Department of Defense spent

¹In May 1993, we made recommendations regarding the retention of national security information. See Classified Information: Volume Could Be Reduced by Changing Retention Policy (GAO/NSIAD-93-127, May 24, 1993).

\$210 million and the State Department spent \$7 million. The Office of Personnel Management spent about \$100 million to perform background checks for other agencies, but only \$21.7 million could be directly attributed to national security. Regarding equipment purchases, the government spent \$72 million for security containers, or safes, during fiscal years 1990 through 1992. However, security container procurement showed a decline from \$27.3 million in fiscal year 1990 to \$18.5 million in 1992. Similarly, other equipment purchases declined during this period, with purchases for the most common type of encryption devices declining from \$55.3 million to \$14.3 million and procurement of secure telephones (STU-III) from over \$55 million to \$26 million.

Other identifiable costs during fiscal year 1992 included \$32.4 million for the Defense Courier Service and \$17 million for State's Diplomatic Courier Service. Declassification activities at the National Archives and Records Administration cost slightly more than \$2 million, while the State Department spent about \$4 million for this activity.

Costs of Protecting Classified Information Not Separately Identified

U.S. government activities to protect classified information are often integrated with security safeguard measures that provide protection for many purposes, or are part-time duties that are performed along with regular nonsecurity related functions. Thus, even if the costs for security functions are accumulated accurately, it is difficult to discern what portion is purely applicable to national security classification. Moreover, whether government units actually incur additional costs because staff have part-time security duties is even more difficult to discern. These circumstances are not only applicable at the departmental level, but also at the two Defense component agencies that we examined in more detail, the Defense Mapping Agency and the Advanced Research Projects Agency.

In 1992, the Department of Defense commissioned the Institute for Defense Analysis, a federally funded research and development center, to identify the Department's total security costs. The Institute subsequently estimated that the fiscal year 1991 costs totaled \$5.9 billion.² Physical security was the largest element with guard forces and other personnel costs accounting for \$2.3 billion of the \$3.1 billion total. However, the guards, for example, can be assigned at facilities to protect equipment, personnel, and property, in addition to classified information. The second largest cost element of \$1.4 billion was for communications and computer

²The Institute published its results in a September 1992 report, Resource Estimates for Counterintelligence and Security Countermeasures.

security. However, these systems are also used to protect various types of sensitive, but unclassified, information as required by the Privacy Act and the Computer Security Act.

The Institute did identify many administrative and management tasks that relate to information safeguards which, for the most part, involve classified information. More than 5,000 equivalent staff years were attributed to full-time positions, with attendant costs of \$212 million. Approximately, another 13,000 equivalent staff years, costing \$462 million, were attributed to part-time and collateral duties.

Defense Department Efforts to Standardize and Reduce Costs

Some Defense Department actions have been taken or are planned to standardize procedures and reduce costs. For example, a standardized background investigation was introduced throughout the government and implemented by the Department in fiscal year 1992 to standardize background investigations for top secret and special access clearances. The Department plans to consolidate the number of facilities where personnel security investigations are reviewed to grant clearances. Cost savings projected from this consolidation were \$21.9 million through fiscal year 1999. (See app. I for more details.)

In response to a congressional requirement in the Intelligence Authorization Act for fiscal year 1992 (P.L. 102-183), the Assistant Secretary of Defense for Command, Control, Communication, and Intelligence directed that the military services and defense agencies provide data on security activities and costs for the fiscal year 1994-95 annual budget submissions. The objective is to develop an integrated counterintelligence and security countermeasures program to (1) improve resource management accountability and oversight and (2) ensure security policy ties to programs. Department of Defense components are required to report costs such as: physical security (with subcategories for equipment, antiterrorism, personnel, organizations, and nuclear weapon and nuclear weapon system security); automated information system security; communications security; compromising emanations (TEMPEST); industrial security, information security; personnel security; counterintelligence support; operation security; and special access programs.

According to Department of Defense officials, preliminary analysis of data submitted showed that defense components and the military services are accounting for these costs in different ways. Moreover, the accuracy of the

data could not be validated because of uncertainty over its origination within various organizations. Department of Defense officials said that they plan to request that the services and defense components submit another round of data on a more standard basis.

The Defense Mapping Agency conducted a study to identify its potential cost savings if incoming source materials were decompartmentalized from Sensitive Compartmented Information³ and downgraded to either secret or unclassified. Since almost all of the Defense Mapping Agency's classification decisions are derived from the classification levels assigned to its source materials by others, the Agency's study illustrates how original classification decisions influence security costs at agencies that subsequently use the information.

Preliminary results of the study show that 48.4 staff years and \$5.5 million could be saved by the Defense Mapping Agency if the Sensitive Compartmented Information source materials (controlled by the Director of Central Intelligence) were decompartmentalized and downgraded to secret and 68.5 staff years and \$6.2 million could be saved if they were made unclassified. These savings would be achieved in physical security, information security, industrial security, production, personnel security, and computer operations. The largest cost savings, \$4.9 million, would be achieved in computer operations. This is because the Defense Mapping Agency has a separate computer system for sensitive compartmented information and downgrading would allow it to consolidate this system with other existing systems.

Observations

U.S. government costs for protecting classified information are substantial, but the safeguards are often integrated with other functions and the additional cost impact is not discernable. Even so, better information could be consistently accumulated by the agencies to evaluate needs and to identify cost reduction opportunities. In this regard, we believe that the Department of Defense's effort to develop a standardized system to track security type costs among its various components is a good initial step.

Costs, by themselves, however, are not necessarily a determining factor of whether classification and subsequent protection are justified. The basic question is whether classification requirements and processes can be

³Sensitive compartmented information includes all information and material that require special access within compartmented intelligence systems.

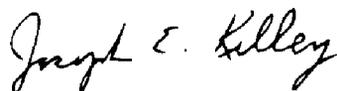
adjusted or relaxed as world conditions change. The presidential directive, issued in April 1993 to reexamine the protection of national security information, should result in a new executive order addressing the issue. If it is determined that some requirements can be reduced, then it can be expected that the attendant costs will also be reduced.

Appendixes I through V discuss the cost considerations in more detail. As requested, we did not obtain written agency comments on these matters. However, we discussed the report's contents with agency officials at the Department of Defense and several of its components—the Advanced Research Projects Agency, the Defense Mapping Agency, the National Security Agency, and the Defense Investigative Service; the State Department; the Federal Bureau of Investigation; the Office of Personnel Management; the National Archives and Records Administration; and the General Services Administration's Information Security Oversight Office. The officials generally agreed with the report and provided some clarification and additional factual material. We made revisions to the report as appropriate based on their comments.

Unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its issue date. At that time, we will send copies to the heads of the agencies previously mentioned and interested congressional committees. We will also make copies available to others upon request.

Please contact me at (202) 512-4128 if you or your staff have any questions concerning this report. Major contributors to this report are listed in appendix VII.

Sincerely yours,



Joseph E. Kelley
Director-in-Charge
International Affairs Issues

Contents

Letter		1
Appendix I		10
Security Clearance	Investigations Directly Attributed to National Security	11
Investigations and	Background Investigations Indirectly Attributed to National	12
Analyses	Security	
	Office of Personnel Management	12
	Federal Bureau of Investigation	13
	Costs of Adjudications	13
Appendix II		15
Physical Security	Security Container Purchases	15
	Physical Security Costs Indirectly Attributable to the Protection	16
	of Classified Information	
Appendix III		18
Communications and	Communications Security	18
Computer Security	Computer Security	20
	Maintenance Costs	22
Appendix IV		23
Security	Security Training	24
Administration and	Classified Courier Services	25
Management		
Appendix V		26
Central Storage,	Centralized Storage	26
Declassification, and	Declassification Activities	27
Destruction	Destruction of Classified Materials	28
Appendix VI		30
Objective, Scope, and		
Methodology		

Appendix VII
Major Contributors to
This Report

32

Tables

Table I.1: DIS Personnel Security Investigations	11
Table I.2: OPM Personnel Security Investigations	12
Table II.1: Unit Cost Comparison of Safes and Filing Cabinets	15
Table V.1: Fiscal Year 1992 Rental Cost of NARA Vault Space Versus Regular Space for Unaccessioned Records Storage	27

Figure

Figure V.1: Destruction Costs and Quantities for Fiscal Year 1992	29
---	----

Abbreviations

ARPA	Advanced Research Projects Agency
DIS	Defense Investigative Service
DMA	Defense Mapping Agency
DOD	Department of Defense
FBI	Federal Bureau of Investigation
NARA	National Archives and Records Administration
NSA	National Security Agency
OPM	Office of Personnel Management
SSBI	Single Scope Background Investigation
STU-III	Secure Telephone Unit

Security Clearance Investigations and Analyses

During fiscal year 1992, the U.S. government spent at least \$239 million on investigations and analyses of the results in order to grant or continue personnel security clearances.¹ This amount does not include any costs for investigations conducted by the Central Intelligence Agency, nor do the reported amounts always capture all attributable costs. Furthermore, another \$133 million was spent on background investigations, from which the portion applicable to security clearances rather than employment suitability cannot be determined.

The three primary types of investigations are national agency checks, background investigations, and periodic reinvestigations. National agency checks are used to determine suitability for government employment and can also be used to grant clearances up to secret. These checks vary in scope: from only a check of basic federal agency records to more in-depth records checks with written inquiries and interviews. National Security Directive 63, issued on October 21, 1991, established a standardized background investigation to be used by all agencies for access to top secret and sensitive compartmented information.² The standard, a Single Scope Background investigation (SSBI), includes a national agency check plus a review covering the past 10 years, or to age 18, of the subject's background with an independent verification of birth, citizenship, credit, education, employment, and appropriate public records. There is also an effort underway to standardize investigations for secret and confidential clearances, but to date this effort is not yet completed. Periodic reinvestigations are required every 5 years for those who have top secret and above clearances. For secret clearances, periodic reinvestigations are currently being conducted every 15 years, with a goal of every 10 years. Clearances for top secret and special access information require more extensive reinvestigations.

The Defense Investigative Service (DIS), the Office of Personnel Management (OPM), the Federal Bureau of Investigations (FBI), and the Central Intelligence Agency conduct most of the personnel security investigations. DIS and OPM conduct the largest number of investigations, with DIS conducting more than 600,000 in fiscal year 1992 and OPM conducting almost 200,000. Other agencies such as the National Security Agency (NSA), Drug Enforcement Agency, State Department, Internal

¹For security clearance costs, we identified for 1986 and 1987, see Information Security: Update of Data on Employees Affected by Federal Security Programs (GAO/NSIAD-89-56FS, Mar. 7, 1989).

²Sensitive compartmented information includes all information and material that require special controls for restricted handling within compartmented intelligence systems.

Revenue Service, and U.S. Information Agency also conduct background investigations.

Investigations Directly Attributed to National Security

The DIS, State Department, Central Intelligence Agency, and NSA conduct background investigations primarily for national security purposes. The Central Intelligence Agency did not provide us with cost data for its background investigations. NSA spent about \$154,000 in fiscal year 1992 for its background investigations.

DIS conducts investigations for Department of Defense (DOD) civilian, military, and contract personnel who need access to national security information. It also conducts investigations for other government agencies. Its cost for conducting this personnel security investigative program was \$154 million in fiscal year 1991 and \$157 million in fiscal year 1992. This cost includes its direct program obligations and 80 percent of its total overhead costs,³ but excludes free support provided by host installations worldwide. Additionally, DIS was charged \$7.7 million and \$6.5 million by the FBI for name and fingerprint checks in fiscal years 1991 and 1992, respectively. These costs were passed on to the military services.

Table I.1 shows the number of DIS investigations for fiscal years 1991 and 1992, by category. DIS expects to conduct fewer background investigations in fiscal year 1993. However, due to the more stringent SSI requirements, the same amount of resources will be required to conduct these investigations.

Table I.1: DIS Personnel Security Investigations

Type of investigation	Fiscal year 1991	Fiscal year 1992
National agency checks	409,013	376,568
Background investigations	127,031	98,010
Periodic reinvestigations	95,989	155,856
Other investigations ^a	9,049	10,542
Total	641,082	640,976

Source: DIS.

^aThese are special investigations resulting from questions arising after clearance decisions were made.

³The remaining 20 percent is attributed to the DIS industrial security program.

Since DOD is hiring fewer employees, fewer national agency checks and background investigations were conducted in 1992, but DIS increased its efforts to reduce its periodic reinvestigations backlog. Periodic reinvestigations had not been required for people with secret clearances until 1989, resulting in an enormous backlog at DOD. Further, according to DIS officials, many of the reinvestigations for secret have become much more work-intensive.

The State Department spent approximately \$6.3 million in fiscal year 1992 for national security investigations of its own applicants and employees as well as for investigations conducted overseas for other agencies. This amount included salaries for contractors, field agents, and field managers, but did not include travel, supply, or other overhead costs.

Background Investigations Indirectly Attributed to National Security

OPM and the FBI conduct background investigations for (1) subjects in positions that require access to national security information and (2) positions that only require an investigation of a subject's suitability for employment. However, the costs of these investigations are generally indistinguishable and, therefore, neither agency can fully determine what portion is attributable to national security.

Office of Personnel Management

OPM conducts background investigations for civilian and contract personnel for most agencies. Its total costs were \$90.7 million in fiscal year 1991 and \$99.1 million in fiscal year 1992. According to the Chief of Investigations Operations, the increase was due to new FBI user fees for fingerprint and file search services for national agency checks. Of the \$99.1 million spent in fiscal year 1992, \$21.7 million was for SSBIS and directly attributed to national security. However, costs for the remaining portion of investigations could not be specifically attributed to national security. Overall, OPM's investigations decreased by about 16 percent from fiscal year 1991 to fiscal year 1992, as shown in table I.2.

Table I.2: OPM Personnel Security Investigations

Type of investigation	Fiscal year 1991	Fiscal year 1992
National agency check with inquiries	177,282	146,265
Background investigations	34,238	31,085
Standard reinvestigations	28,939	24,905
Total	240,459	202,255

Source: OPM.

Federal Bureau of Investigation

The FBI conducts background investigations for both national security and employment suitability on its own applicants, employees, and contractors as well as for other federal agencies and miscellaneous investigations. Its total costs decreased slightly from \$56.4 million in fiscal year 1991 to \$55.2 million in fiscal year 1992. According to FBI officials, the new SSBI requirement did not increase costs for its own applicants because it was already using more stringent standards.

FBI investigations increased from 15,838 in fiscal year 1991 to 17,027 in fiscal year 1992.⁴ The increase occurred primarily as a result of an increase in reinvestigations for FBI employees, and to a lesser extent, as a result of a slight increase in the number of miscellaneous investigations. Investigations for other agencies and FBI applicants decreased.

Costs of Adjudications

The process by which the investigation results are reviewed by officials to determine whether an individual is suitable for employment and will receive or continue to be granted clearance for access to national security information is referred to as adjudication. While adjudication of DOD, State, and NSA investigations are primarily attributed to national security, other agencies conduct adjudications for both national security and employment suitability.

DOD components perform their adjudication processes at 18 different locations and it estimates that the total costs for fiscal year 1992 were about \$45 million. NSA said that it spent \$1.24 million in fiscal year 1992 for adjudication salaries. Similarly, the State Department reported adjudication costs of \$637,869 for salaries only.

In a 1991 study of its adjudication operations, DOD considered two options for consolidation to promote greater efficiencies, a more consistent implementation policy, and greater oversight. The first called for consolidation under seven authorities: the Army, the Navy, the Air Force, the Joint Chiefs of Staff, the Washington Headquarters Service, the Defense Intelligence Agency, and the Directorate for Industrial Security Clearance Review. The second suggested the consolidation of all adjudicative operations under a senior intelligence community official. DOD chose the first option which will result in a reduction of 55 out of 428 total civilian personnel, and is projected to save \$800,000 in fiscal year 1994,

⁴The FBI provided data for background investigations based on the number of completed cases, except for initial investigations for FBI applicants. Data for FBI applicants is only maintained by the total number of cases initiated.

**Appendix I
Security Clearance Investigations and
Analyses**

\$3.1 million in fiscal year 1995, and a total of \$21.9 million through fiscal year 1999.

Physical Security

The U.S. government spends billions of dollars each year on physical security to safeguard information, personnel, property, and equipment. At DOD, for example, physical security costs are estimated to be about \$3 billion annually with a large portion expended for guard forces. However, most physical security costs are not solely attributable to the protection of classified information. The largest directly attributable cost was \$72 million for the purchase of security containers, or safes, during fiscal years 1990 through 1992.

Physical security is the sum of all measures designed to control access to a facility to safeguard personnel, property, and information against espionage, sabotage, damage, and theft. It includes measures such as guards, fences, safes, and alarm and camera systems. The protection of classified materials is only one of several reasons for undertaking physical security measures.

Security Container Purchases

During fiscal years 1990-92, the federal government spent \$72 million through the General Services Administration to procure safes for storing classified information. However, these costs decreased from \$27.3 million in fiscal year 1990 to \$18.5 million in fiscal year 1992.

All new security containers procured by the General Services Administration since March 10, 1992, are equipped with an electromechanical combination lock for use in protecting all levels of national security information. To illustrate the incremental costs of security containers, table II.1 compares the costs of two- and five-drawer legal size safes, using the new single electromechanical combination locks with locking file cabinets. The higher cost for safes reflects the difference in materials and the use of technology, such as the new electromechanical combination locks which cost approximately \$500 more than mechanical locks.

Table II.1: Unit Cost Comparison of Safes and Filing Cabinets

Size of container		Unit cost		Unit cost differential
		For unclassified document use	For classified document use	
Two-drawer legal size with single lock	Average	\$84.28	\$1,554	\$1,469.72
Five-drawer legal size with single lock	Average	\$174.17	\$2,160	\$1,985.83

Physical Security Costs Indirectly Attributable to the Protection of Classified Information

Many physical security costs address multipurpose security activities and are indirectly related to the costs of protecting classified information. The Institute for Defense Analysis estimated that DOD's physical security expenditures accounted for \$3.1 billion of the \$5.9 billion in documented security costs for fiscal year 1991. Personnel, including guard forces, accounted for approximately \$2.3 billion of the physical security cost, while \$550 million was for equipment. According to the Institute, the military services have substantial manpower devoted to guarding installations; conventional weapons and munitions; nuclear weapons; and information, personnel, and property at overseas diplomatic posts.

At the Defense Mapping Agency (DMA), for example, only a small portion of physical security costs can be directly attributed to the protection of classified holdings. DMA estimates that it spent about \$5.2 million on physical security in fiscal year 1992, of which \$4.8 million was for personnel. However, it estimated that only 5 staff years—of the total 162 personnel involved in physical security—could be eliminated at a savings of \$132,000 if sensitive compartmented information were decompartmentalized and downgraded to secret or unclassified. These 5 staff years represent guard positions protecting sensitive compartmented information areas within DMA facilities.¹ Thus, the vast majority of DMA's physical security costs would continue to exist even if the sensitive compartmented information were decompartmentalized, because these costs are attributed to the protection of personnel, property, equipment, and other information as well as classified information.

Many expenditures for equipment are one-time investments rather than annual costs. For example, The Advanced Research Projects Agency (ARPA), in developing a security system for its new location in 1991, stated that the procurement of its Cardkey access system, alarms, and monitors, at a cost of \$223,400 with installation, would save it money in the long run. Prior to June 1991, ARPA paid \$96,384 annually to lease and maintain security equipment. Currently, it pays \$21,634 annually for the maintenance of the new security equipment purchased, an annual savings of \$74,750.

At many State Department posts overseas, guard forces are also used to protect personnel, property, and equipment along with classified information. In compliance with Information Security Oversight Office directives, State Department regulations call for Marine guards to be

¹Although access to DMA facilities is restricted, sensitive compartmented information areas have further restrictions necessitating additional guards for these areas.

present at embassies and facilities where top secret information is maintained. However, the volume of classified documents at a location does not directly affect the number of guards or their cost. For example, at the overseas post we reviewed, the Marine security guards and local guards are primarily geared to the security of American personnel, although the Marine security guard's presence is required to protect classified information. In fiscal year 1992, the cost of salaries for Marine security guards was \$160,000, and the cost of salaries, equipment, and supplies for the local guard force was \$5.1 million. As of October 1, 1992, the overseas post had 15 Marine security guards and 342 local guards.

Communications and Computer Security

Expenditures to secure communications and computer systems are substantial and represent the second largest category of security costs behind only those for physical safeguards. For example, the Institute for Defense Analysis estimated that DOD spent \$1.4 billion to purchase, operate, and maintain secure communications and computer systems in fiscal year 1991. The bulk of these costs were for personnel rather than for equipment purchases. Equipment purchases have declined because large numbers are already in place and requirements are being reevaluated. Although purchases for secure telephone units (STU-III) and the most common type of encryption devices are decreasing, the government spent more than \$40 million for these items in fiscal year 1992.

The applicable costs for protecting national security information, however, are not readily discernable from the total expenditures to secure communication and computer systems. These systems are also used to protect sensitive, but unclassified, information, as required by the Privacy Act of 1974 and Computer Security Act of 1987. Examples of sensitive unclassified information include medical, personnel, financial, investigative, or any other information which, if released, could cause substantial harm, embarrassment, inconvenience, or unfair treatment to the agency or to an individual.

NSA administers many of the U.S. government's communications and computer security programs. Communications security controls access to national security information and/or sensitive unclassified information. Computer security is designed to prevent deliberate or inadvertent unauthorized access, disclosure, acquisition, manipulation, modification, or loss of information in a computer system. With greater interconnectivity between communications and computer networks, it is increasingly difficult to distinguish between the two.

Communications Security

The Institute for Defense Analysis estimated that DOD, including NSA, spent more than \$1 billion to purchase, operate, and maintain secure communications systems during fiscal year 1991. The majority of these costs were related to personnel engaged in these activities. NSA could not provide us with governmentwide communication security costs but said that, in fiscal year 1992, it obligated \$410 million for procurement, research and development, and operations and management for its own communications security programs.

Secure communications require cryptographic equipment such as encryption/decryption devices and STU-IIIs for protecting the transmission and communication of classified and sensitive unclassified information. NSA is the primary agency for the procurement of these devices for the government.

According to NSA, the government spent about \$98 million to procure thousands of the most common type of encryption device between fiscal years 1990 and 1992. However, the volume of these purchases declined from \$55.3 million in fiscal year 1990 to \$14.3 million in fiscal year 1992.

The STU-III is the standard secure phone used by U.S. agencies and the military services. According to NSA, the government has purchased over 252,000 STU-IIIs since the inception of the program in 1984. Initially, each unit cost about \$3,000; however, a standard model currently costs \$1,660. Furthermore, the number being procured has also declined. Government agencies purchased 21,032 STU-IIIs for over \$55 million in fiscal year 1990 and 13,790 units for about \$26 million in fiscal year 1992. STU-IIIs are more expensive to repair than standard phones, and they also require encryption keys which are updated electronically through the key control system.

According to State Department and DOD officials, both the encryption devices and STU-IIIs are used to protect the transmission of sensitive unclassified information as well as classified information. An ARPA official said that many of their contractors use STU-IIIs for conversations containing proprietary information because of the threat of industrial espionage.

At the State Department's overseas posts, communications security costs vary according to the post's size and its assessed vulnerability to human and electronic intelligence threats. According to State officials, the typical communications security equipment costs for a medium-sized overseas post assessed to have a high electronic security threat, is currently estimated to be over \$1 million. This includes cryptographic equipment, computerized classified information handling systems or classified local area networks, STU-IIIs, TEMPEST equipment,¹ and construction of shielded enclosures.²

¹TEMPEST equipment is specially protected with copper shielding around the periphery of the device in order to reduce compromising emanations from leaving a controllable area.

²New embassies assessed to have either a high or critical electronic threat level are required to have specially constructed enclosures around their communications centers to help protect against electronic signal emanations.

Computer Security

The Institute for Defense Analysis estimated that DOD spent \$363 million in fiscal year 1991 for computer security. According to NSA, State, and DOD officials, the costs of TEMPEST equipment have been major computer systems security costs in the government. Other costs include accreditation/certification of computer systems as well as maintenance.

TEMPEST Countermeasures

NSA officials said that prior to 1988, TEMPEST equipment was purchased in large quantities by DOD and the rest of the government at a time when world tensions were high and security budgets were well-funded. In 1988, however, a new national policy was adopted to relax TEMPEST requirements within the continental United States because of a reduced threat. NSA officials said that the new policy reflected concerns that TEMPEST costs were too great, and that countermeasures must be based on the actual threat.

DOD and NSA officials said that it is extremely difficult to determine how much is spent on TEMPEST countermeasures because expenditures are embedded in programs, facility costs, contractors, and other overhead costs. For example, TEMPEST costs for the State Department are not visible budget items, but are embedded under overall computer system costs. According to a State official, no one knew how much the Department spent on TEMPEST equipment and maintenance prior to 1992, because such data was not tracked.

NSA recommends that before TEMPEST countermeasures are implemented, a comprehensive security versus cost-benefit analysis be performed. In 1992, State undertook such an analysis to determine what savings could be achieved by purchasing non-TEMPEST equipment and adopting a countermeasure known as TEMPEST "zoning".³ The analysis showed that of the \$39 million State spent on new computer equipment in fiscal year 1991, approximately \$16 million were TEMPEST purchases. According to the analysis, State could have spent \$8 million less in automated information system equipment if TEMPEST zoning was employed. For example, State spent

- \$2.2 million for 386 TEMPEST personal computers, which would have cost \$580,000 for non-TEMPEST;
- \$780,000 for TEMPEST 14-inch color monitors, which would have cost \$184,000 for non-TEMPEST; and

³TEMPEST zoning is a countermeasure that takes advantage of a facility's natural barriers such as walls and obstructions to prevent electronic emanations.

- \$1.3 million for TEMPEST removable 80MB hard disks, which would have cost \$660,000 for non-TEMPEST.

State did not conduct a similar analysis of TEMPEST expenditures for fiscal year 1992. However, according to NSA and State officials, more government agencies are reducing TEMPEST equipment procurement and have adopted TEMPEST zoning as the primary TEMPEST countermeasure domestically. NSA and DOD officials told us that a revised TEMPEST policy, set forth in 1992, assessed a low domestic threat. Accordingly, a new DOD strategic plan for counterintelligence and security countermeasures calls for less spending on TEMPEST equipment.

Accreditation

Accreditation/certification is a formal declaration that the computer system is approved to operate in a particular security mode using a prescribed set of safeguards. Systems must be accredited whether they are used for classified or sensitive unclassified information. Some security procedures taken into account during the accreditation process are virus protection, encryption of data, and the use of passwords.

NSA, the Defense Intelligence Agency, the Central Intelligence Agency, and the Joint Chiefs of Staff accredit all systems that will contain sensitive compartmented information. For systems operating without sensitive compartmented information, the accreditation is often done within the agency, as in the case of DMA. According to an NSA official, there is no single governmentwide standard for information protection or computer accreditation. Such guidance is needed by security planners and accreditors who have been asked to interface systems belonging to two different government departments or agencies.

We were not able to collect any specific cost data on accreditation, but NSA has an accreditation group, consisting of six people who work on accreditation and two who work on accreditation policy full-time. Additionally, the Defense Intelligence Agency has 10 full-time employees in its accreditation office, the Office of the Secretary of Defense and Defense Information Systems Agency have accreditors on staff, and individual agencies, such as DMA, have staff that work on accreditation. ARPA hired a contractor to prepare its automated information systems and the accompanying documentation required for accreditation at a cost of \$80,000 in fiscal year 1992.

Maintenance Costs

The Institute for Defense Analysis estimated that the military services spent \$153 million in fiscal year 1991 for specialists to maintain communications security equipment. An ARPA official provided an example of the maintenance costs for secure equipment. Secure fax machines have an \$800 annual maintenance contract per machine, because they require annual inspections to ensure that security functions are operating. Regular fax machines are only repaired as needed.

The State Department's maintenance costs to support all communications and computer security equipment handling classified information at overseas posts totaled about \$22.1 million in fiscal year 1992. The total maintenance figure includes some, but not all, labor costs for 105 technicians supporting overseas equipment that handles classified information, travel and per diem, as well as training.

Security Administration and Management

Large numbers of U.S. government personnel perform security related administrative and management tasks which, for the most part, involve classified information. Many of these tasks are performed as collateral duties such as document control, security monitoring, and training, but there are aspects of these activities and others that are performed as full-time duties. The significance of this is reflected at DOD where the Institute for Defense Analysis estimated that costs for these operations totaled \$674 million in fiscal year 1991. It was estimated that an equivalent 18,000 staff years were expended, of which more than 5,000 were attributed to full-time positions associated with base-level security and local security organizations with attendant costs of \$212 million.

In previous years, the responsibilities for overseeing and administering security functions within DOD's components were often fragmented in many offices. Currently, defense agencies, such as ARPA and DMA, have separate security offices. For example, ARPA has a Security and Intelligence Office for which it spends about \$400,000 for annual salaries. The Office is responsible for all aspects of security, including providing security briefings, processing security clearance applications, reviewing security guides, and overseeing security contracts, such as for guard forces. DMA has security offices at its headquarters and each of its major components, with a total annual cost of over \$2 million.

Both ARPA and DMA have document control centers or registries to primarily account for classified documents. ARPA has a document control center staffed by contract employees who barcode incoming classified documents and log them into a computer system. ARPA's cost was \$254,166 in fiscal year 1992 for the document control center which includes maintenance of the software for the barcode system and the four employees. DMA estimated that the operating costs for its registries were approximately \$850,000 for salaries and supplies.

Additional costs are incurred by individuals whose primary responsibility is not security, but who nonetheless spend time on securing classified materials or act as security monitors. For example, DMA has designated 300 staff to act as part-time security monitors. They attend hour-long meetings 4 to 12 times a year to discuss security matters.

At the State Department, the Bureau of Diplomatic Security formulates policy and directs the implementation of its worldwide security programs. Domestically, the Department relies on bureau personnel who have as collateral duties unit security functions at its headquarters. Officials from

the European Bureau stated that the cost of control and oversight of classified documents, domestically, cannot be ascertained because everyone handles classified information daily. Moreover, the European Bureau's unit security officers carry out a variety of other duties, some of which are not directly related to securing classified information, such as door lock checks.

The Bureau of Diplomatic Security has regional security officers assigned to overseas posts, who are responsible for various security activities, including managing the post's programs to protect national security information, supervising Marine security guards, and developing and overseeing emergency action plans designed to defend the post against bomb threats and other emergencies or problems. At the medium-sized overseas post we visited, the regional security office spent \$287,000 on personnel and supplies in fiscal year 1992.

Security Training

Each U.S. government agency that creates or handles national security information conducts its own security training. DOD spent \$3.4 million in fiscal year 1992 to operate its security training institute in Richmond, Virginia, with student travel and per diem costing approximately \$1 million more. This does not include the costs for other security training conducted at military units and DOD's many agencies.

At DMA, we found that the specific costs of security training are sometimes integrated with other training costs or are otherwise not readily identifiable. For example, every new employee attends training that includes a module on security. Additionally, every employee receives training on automated information systems security that is the same for people using systems with classified information as for those using systems with only sensitive information.

At ARPA, security training costs are included in the total operating costs of its security office. The ARPA security office provides security awareness education through messages relayed on its computer network, an annual security briefing, a monthly news bulletin, and ad hoc in-house courses as needed. In fiscal year 1992, the security office gave nine presentations of a security briefing, allowing ARPA personnel to fulfill their annual security training requirement. ARPA security officials also attend occasional security related classes and conferences, but are not required to take a specific number of courses or to get "certified" in any way.

The State Department provides various types of security courses and briefings for foreign service officers, foreign service specialists (e.g., communications personnel), and civil service personnel. In fiscal year 1992, the State Department spent about \$1 million on security training, primarily on teacher's salaries. Included in some of the security training courses and briefings are sections that deal specifically with the protection of classified information.

Classified Courier Services

Transporting classified information through DOD's Defense Courier Service and the State Department's Diplomatic Courier Service cost government agencies about \$53 million in fiscal year 1991, and \$49 million in fiscal year 1992. Classified materials transported worldwide and other materials sent to high security threat locations overseas are escorted by either courier service. Materials classified secret are also sent via registered mail within the United States at a cost of \$4.50 plus postage. Confidential materials mailed to contractors must be registered or certified.

The total cost for the Defense Courier Service to transport and escort materials between its 36 worldwide stations was \$35.7 million in fiscal year 1991 and \$32.4 million in fiscal year 1992. The volume decreased from over 10 million pounds in fiscal year 1991 to less than 9 million in 1992. According to a Defense Courier Service official, the volume decreased due to a reduction in U.S. military forces, a greater reliance on the use of advanced communications security technology, the use of lightweight paper, and a significant reduction in large-scale military exercises.

The Diplomatic Courier Service's operations costs totaled somewhat over \$17 million annually in fiscal years 1991 and 1992, excluding salaries. Although the costs decreased slightly, the volume increased from 4.3 million pounds in fiscal year 1991 to 4.8 million pounds in fiscal year 1992. The State Department said that the volume grew primarily because U.S. agencies are generating more materials for overseas deliveries.

Central Storage, Declassification, and Destruction

When classified information becomes dated and has outlived its operational use, it is archived, stored, declassified, or destroyed. The total costs of storing, declassifying, and destroying classified materials are difficult to obtain because these activities are widespread throughout the government. Some identifiable fiscal year 1992 costs include over \$489,000 for storage of classified records by the National Archives and Records Administration (NARA), \$6.3 million for NARA and the State Department to declassify information, and \$1.1 million for DOD and State to destroy classified materials at centralized facilities in the Washington, D.C., area.

Centralized Storage

Storage of classified information is widespread throughout the government. The related costs, such as for safes, were discussed in appendix II. In addition, NARA stores records at central facilities around the country for all agencies, but the incremental costs for storing the majority of classified documents are marginal compared to that for unclassified documents. NARA stores two types of records: those with historical value that have been transferred (or accessioned) into the National Archives of the United States and those that agencies no longer need for current business, but are not yet eligible for destruction or transfer to the National Archives (unaccessioned).

NARA officials said that all accessioned records are highly protected because of their historical value. All the storage facilities are equipped with alarms and other security devices and thus the cost differences for storing classified versus unclassified permanent records are minimal. The additional costs of protecting permanent classified records are primarily the one-time construction costs of vaults or facilities for sensitive compartmented information and the cost of security clearances for personnel. For example, according to NARA officials, it cost \$2,500 to convert a vaulted area into a sensitive compartmented information facility at the National Archives in Washington, D.C.

All unaccessioned documents are also protected to ensure the integrity of the records for ongoing legal, administrative and financial needs of the federal agencies. However, storage of unaccessioned classified documents can cost substantially more than unclassified documents at the various storage centers around the country because of vault space costs. Table V.I shows the rental rates for vault space versus warehouse space for unaccessioned records at various locations.

Appendix V
Central Storage, Declassification, and
Destruction

Table V.1: Fiscal Year 1992 Rental Cost of NARA Vault Space Versus Regular Space for Unaccessioned Records Storage

Location of record center	Cost of regular space per square foot	Cost of vault space per square foot	Size of vault in square feet	Additional cost of vault space
Atlanta	\$6.30	\$19.39	576	\$7,540
Boston	12.16	30.24	1,742	31,495
Chicago	7.76	27.41	4,921	96,698
Dayton	5.31	22.54	2,288	39,422
Kansas City	6.06	22.26	740	11,988
Los Angeles	14.28	35.48	3,058	64,830
New York	6.39	29.80	1,580	36,988
St. Louis (Civilian personnel records)	6.18	14.13	1,001	7,958
St. Louis (Military personnel records)	7.41	16.61	2,991	27,517
Seattle	5.79	23.08	790	13,659
Suitland	9.37	10.66	117,000	150,930
Total			136,687	\$489,025

Source: NARA.

Most of NARA's unaccessioned classified documents are stored at its facility in Suitland, Maryland, where it costs only \$1.29 more per square foot, according to rental rates determined by the General Services Administration. At other locations, vault space costs between \$8 and \$23 more per square foot, which is a direct cost of protecting unaccessioned classified materials.

Declassification Activities

Executive Order 12356 requires government agencies to review and declassify documents as soon as national security considerations permit. Agencies also incur costs for reviewing documents under provisions of the Freedom of Information Act. At DOD, these activities are not centralized and total costs are not accumulated; however, at both NARA and the State Department these activities are centralized and costs are available.

NARA's declassification division performs two types of declassification activities: systematic reviews of entire blocks of classified records that are at least 30 years old and reviews of individual classified records requested by researchers under the Freedom of Information Act or Executive Order 12356. The declassification division's total costs for fiscal year 1992 were slightly more than \$2 million, consisting of personnel costs, security clearance expenditures, and supplies and equipment. These costs are all

directly attributable to the protection of classified information, because other offices review requests for unclassified materials held by NARA.

NARA currently has approximately 325 million pages of textual records awaiting declassification review.¹ NARA's declassification division reviewed approximately 43 million and 40 million pages in fiscal years 1991 and 1992, respectively. NARA received about 17 million and 11 million pages needing declassification review in those same years. Additionally, NARA has some classified nontextual records such as microfilm, maps, and photographs that are awaiting declassification review. NARA officials stated that the percentage of records being accessioned that need declassification review has grown from 10 percent to 40 percent.

In fiscal year 1992, the State Department spent \$4.3 million, primarily on personnel salaries for the systematic processing and review of classified documents 30 years old, as well as for researcher-initiated reviews of contemporary documents. The total amount includes \$200,000 paid to NARA for personnel to help declassify State Department records.

Destruction of Classified Materials

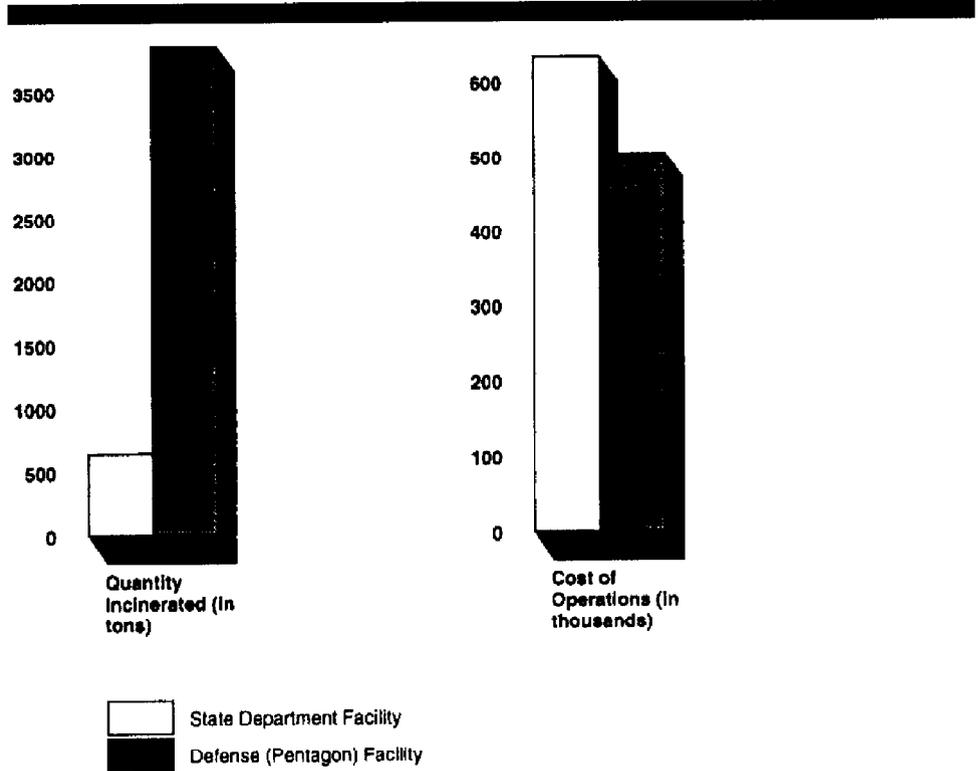
As U.S. government agencies and offices determine that classified information is no longer needed, the materials are destroyed by one or more of the following methods: shredding, pulverizing, incinerating, and recycling. The destruction is often carried out in many different locations along with other functions. For example, an individual office might use a shredder to destroy classified information along with other data that is considered sensitive. For the most part, the applicable costs are not accumulated.

In the Washington, D.C., area, both the Defense and State Departments also operate centralized destruction facilities at a combined total annual cost of more than \$1 million. The costs of operating each facility and the quantities of materials destroyed are shown in figure V.1.

¹Not all records awaiting declassification review are actually classified. For example, in fiscal year 1992, of the 40 million pages reviewed, 6.5 million pages were actually classified.

Appendix V
Central Storage, Declassification, and
Destruction

Figure V.1: Destruction Costs and
Quantities for Fiscal Year 1992



Source: State Department and DOD.

In fiscal year 1992, the State Department spent \$633,500 to destroy classified materials at its facility serving the Washington, D.C. metropolitan area. This cost included contract personnel, overtime, and materials. In fiscal year 1992, DOD similarly spent \$502,700 to operate its Pentagon destruction facility which included the salaries of DOD employees, maintenance, and utilities. Additionally, this site was used to destroy 25 tons of Privacy Act materials in 1992. In fiscal year 1992, the Pentagon facility destroyed 3,830 tons of classified material and the State facility destroyed 640 tons. According to a State Department official, its incineration facility costs more to operate than the Pentagon's because it is more labor-intensive and is staffed by contractors.

Objective, Scope, and Methodology

The former Chairman, House Government Operations Subcommittee on Information, Justice, Transportation, and Agriculture, requested us to review the costs involved in protecting national security information. As agreed with subcommittee staff, our objective was to determine, to the extent practical, annual cost information pertaining to classified information safeguards at selected levels and areas of the government. We also acquired information regarding DOD efforts being undertaken to standardize and reduce these costs.

We obtained annual fiscal year 1990-92 cost data for major life cycle cost elements involved with classifying and protecting national security information at two levels. First, we attempted to obtain aggregate cost data at the highest level available—either governmentwide or at individual agencies or departments we reviewed. We obtained information and interviewed officials on these costs from the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; OPM; DIS; the General Services Administration; NSA; the FBI; and NARA. We also reviewed pertinent agency regulations and other executive orders related to these areas.

Second, we conducted case studies of two defense agencies—ARPA and DMA—and the Department of State in Washington, D.C., to collect their costs associated with classifying information and protecting classified information. We selected ARPA and DMA, because we believed that major costs could be more readily obtained at these smaller defense agencies. The State Department was chosen because the Information Security Oversight Office reported that State led all government agencies in the origination of classified information with 38 percent of all original classification decisions in fiscal year 1992. We also visited one overseas post where we collected cost data and interviewed embassy officials.

Data for major cost elements were not always available at the same level for the agencies we reviewed. However, during our review, we obtained agency studies or reports that provided data for several cost elements at the agencywide level. One report we obtained late in our review and frequently cite for DOD-wide costs is a September 1992 report by the Institute for Defense Analysis for the Deputy Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Counterintelligence and Security Countermeasures. The report examined fiscal year 1991 resources expended by DOD components and the military services in the areas of counterintelligence, physical security, security and investigative activities, industrial security, personnel security,

communications security, and computer security. DOD officials advised us that the Institute's estimates, while indicative of security costs in DOD, are not primarily based on budget or program data and should not be used for budgeting or programming purposes.

We did not independently verify data obtained on governmentwide costs, Institute for Defense Analysis estimates of DOD costs, or those costs associated with our case studies. Additionally, we did not obtain information on Department of Energy costs with classifying and protecting information associated with the Atomic Energy Act or cost data on industrial security costs to the government. The Central Intelligence Agency would not provide us with cost information.

Except as noted above, we conducted our review in accordance with generally accepted government auditing standards.

Major Contributors to This Report

**National Security and
International Affairs
Division, Washington,
D.C.**

Stewart Tomlinson, Assistant Director
Jason Fong, Evaluator-in-Charge
Hynek Kalkus, Evaluator
Auturo Holguín, Evaluator

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are \$2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

**U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015**

or visit:

**Room 1000
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC**

**Orders may also be placed by calling (202) 512-6000
or by using fax number (301) 258-4066.**

**United States
General Accounting Office
Washington, D.C. 20548**

**Official Business
Penalty for Private Use \$300**

**First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100**
