

October 2002

# BUILDING SECURITY

## Security Responsibilities for Federally Owned and Leased Facilities



---

# Contents

---

---

Letter		1
	Results in Brief	2
	Background	5
	Most Agencies Reported Shared Security Responsibilities	13
	Eleven Agencies Reported that They Have Completed Security Assessments of Facilities	19
	A Variety of Security Forces and Technologies Are Used to Provide Building Security	21
	Funding of Security Needs	25
	Security Coordination Efforts among and within Agencies	28
	Agencies Identified Barriers to Securing Facilities	29
	Implications of the Creation of DHS on Agencies' Security Responsibilities	31
	Scope and Methodology	32
	Agency Comments and Our Evaluation	33

---

## Appendixes

<b>Appendix I:</b>	<b>Guidance Available to Help Agencies Address Security-Related Issues</b>	36
<b>Appendix II:</b>	<b>Federal Executive Branch Agencies with Some Level of Independent Authority to Acquire Real Property, Calendar Year 2000</b>	42
<b>Appendix III:</b>	<b>Definition of Security Levels I through V from DOJ's Vulnerability Assessment of Federal Facilities, June 28, 1995</b>	43
<b>Appendix IV:</b>	<b>Comments from the Administrative Office of the United States Courts</b>	45

---

## Tables

Table 1:	Status of Agencies' Security Assessments	20
Table 2:	Types of Security Forces Used by Agencies	21

---

## Figures

Figure 1:	Total Amount of Federally Owned and/or Leased Space by Category, as of September 30, 2000	6
Figure 2:	Agencies Building Security Responsibilities	18

---

**Abbreviations**

Agencies	federal departments, entities, and agencies
AIA	The American Institute of Architects
AOUSC	Administrative Office of the United States Courts
ASCE	American Society of Civil Engineers
ASHRAE	American Society of Heating, Refrigeration and Air Conditioning Engineers
ASIS	American Society of Industrial Security
BEP	Bureau of Engraving and Printing
BOMA	Building Owners and Managers Association
BPD	Bureau of Public Debt
CCTV	closed circuit television
CDC	Centers for Disease Control and Prevention
CIA	Central Intelligence Agency
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOT	Department of Transportation
Education	Department of Education
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FFC	Federal Facilities Council
FPS	Federal Protective Service
GPO	Government Printing Office
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
IFMA	International Facility Management Association
ISC	Interagency Security Committee
NASA	National Aeronautics and Space Administration
NCPC	National Capital Planning Commission
NIBS	National Institute of Building Sciences
OHS	Office of Homeland Security
SEC	Securities and Exchanges Commission

---

**Contents**

---

SSA	Social Security Administration
TISP	The Infrastructure Security Partnership
Treasury	Department of the Treasury
TSA	Transportation Security Administration
USACE	U. S. Army Corps of Engineers
USDA	Department of Agriculture
USMS	United States Marshals Service
USPS	United States Postal Service
VA	Department of Veterans Affairs



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

October 31, 2002

The Honorable Joseph I. Lieberman  
Chairman, Committee on Governmental Affairs  
United States Senate

The Honorable Robert F. Bennett  
United States Senate

In the wake of the events of September 11, 2001, you requested information regarding critical infrastructure protection within the federal government. This letter responds in part to your October 4, 2001, request for such information. As agreed with your offices, we prepared two products on physical infrastructure protection. Our September 2002 report<sup>1</sup> discussed the activities of the Interagency Security Committee (ISC), while this report discusses the responsibilities of 22 federal agencies for the protection of the federal buildings they own and/or occupy.

As agreed with your offices, the objectives of this second review were to determine (1) the roles and responsibilities that federal departments, entities, and agencies (agencies) have in providing security for office space they occupy; (2) whether security assessments of facilities had been completed; (3) the types of security forces and technologies used to secure and protect federal buildings; (4) funding for security operations; (5) the coordination of security efforts within and among agencies to improve or enhance building security; and (6) impediments that make it difficult to tighten security at federal buildings. We also agreed to provide the types and sources of security-related guidance that are available for agencies to use in addressing building security vulnerabilities. (See app. I for security-related guidance.) With the recent proposals to create a Department of Homeland Security (DHS), we briefly discuss the implications of the proposed department on agencies' security responsibilities.<sup>2</sup> Due to the broad scope and time frame of the review, the report does not assess whether agencies are making reasonable progress in improving building security, whether security funding has been adequate and spending

<sup>1</sup>U.S. General Accounting Office, *Building Security: Interagency Security Committee Has Had Limited Success in Fulfilling Its Responsibilities*, [GAO-02-1004](#) (Washington, D.C.: September 17, 2002).

<sup>2</sup>The President's proposal to Congress dated June 18, 2002, to create a Department of Homeland Security; H.R. 5005, 107<sup>th</sup> Cong. (2002); S. 2452, 107<sup>th</sup> Cong. (2002).

---

priorities appear to have been appropriate, whether new or revised security standards and/or protocols are needed, or whether security assessments have been done properly.

For the most part, we obtained information from the results of questions we sent to 22 federal agencies.<sup>3</sup> We selected 18 agencies because they were part of our ISC review, and these 2 assignments were done jointly. We selected the National Aeronautics and Space Administration (NASA) because of its large size; and we selected the Government Printing Office (GPO), Federal Communications Commission (FCC), and Securities and Exchange Commission (SEC) because of their small size. In addition to asking these agencies to respond to our questions, we asked them to provide documentation for such matters as authority to own or lease buildings and authority to have federal security forces. Twenty-one of the 22 agencies responded in writing, and the remaining agency answered the questions orally. We reviewed the responses and any supporting documentation provided, reviewed agency guidance on security, searched the Internet for other security guidance, and reviewed proposed DHS legislation. Although we received documentation for some areas, we did not independently verify the information provided by the agencies. We conducted our review between December 2001 and September 2002 in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from the 22 heads of the agencies included in our review. We received comments from 21 agencies. The Department of Commerce (DOC) did not provide comments on the report.

---

## Results in Brief

In May 1998, Presidential Decision Directive 63 was issued with the intent to eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructure. It makes every department and agency of the federal government responsible for protecting its own critical physical infrastructure. The ISC and all 22 of the agencies we reviewed have some role in providing security for office space, although the degree of involvement varied from agency to agency.

Other types of security responsibilities include performing security assessments, providing security funding, providing security forces and

---

<sup>3</sup>See table 1 in this report for a list of the agencies we included.

---

security technology, and coordination of security efforts among and within agencies. The ISC has overall responsibility for developing security policies and compliance with these policies for nonmilitary federal facilities. As we reported in September 2002, the ISC has had limited success in fulfilling its role. The General Services Administration (GSA) through its Federal Protective Service (FPS) has sole responsibility for protecting the buildings that it occupies to house its operations, and it also shares building security responsibilities with 19 of the other agencies included in the review that are tenants in GSA-owned or -leased buildings. Additionally, 18 of the agencies own or lease space directly and are responsible for the security of this space. Eleven of the 22 agencies stated that they had completed security assessments on all their facilities since 1995. Nine agencies reported that they were still doing security assessments on their buildings. Two agencies are located in GSA space only and GSA is responsible for the security assessments.

The agencies provide security using a combination of security forces and security technologies. Security forces are comprised of federal security forces<sup>4</sup> and contract security guards. Twelve of the 22 agencies reported using federal security forces to provide some of their physical security. For example, GSA, the Department of the Treasury (Treasury), and the U.S. Postal Service (USPS) have their own federal security forces. GSA through FPS provides integrated security and law enforcement services, including contract security guards and security technology to various facilities such as office buildings and courthouses that GSA owns, controls, or leases. Further, all 22 agencies provide some of their physical security using contract guards, either their own or GSA's. Examples of security technologies implemented by the agencies include closed circuit television (CCTV), X-ray machines, magnetometers, and window protection features.

The President initially allocated \$8.6 million of the \$40 billion from the Fiscal Year 2001 Emergency Supplemental Appropriations Act for Recovery from and Response to Terrorist Attacks on the United States (P.L. 107-38) to the Federal Buildings Fund, administered by GSA, to provide increased security for federal buildings. In the first quarter of fiscal year 2002, FPS received additional funding of \$98.5 million for security. However, the total amount of funds spent by the 22 agencies we reviewed dedicated to building security since the 1995 Oklahoma City bombing for

---

<sup>4</sup>We are defining federal security forces to be any federal employee who actually provides the physical security for a building.

---

fiscal years 1996 to 2001 was not readily available. The main coordination groups identified as providing coordination among agencies were the ISC, Office of Homeland Security (OHS), FPS, Federal Emergency Management Agency (FEMA), and the Federal Bureau of Investigation (FBI).

The impediments to improving security for federal buildings cited by the agencies in our review included difficulty getting lessors to allow federal agencies to implement strengthened security measures in their buildings, and insufficient funding and staff. For example, one agency reported that it had identified vulnerabilities at its facilities and appropriate security countermeasures that would minimize risk; however, without adequate funding it has limited ability to implement the countermeasures.

If DHS is created, it would have significant implications for agencies' security responsibilities.<sup>5</sup> According to proposals pending for the creation of DHS, responsibility for federal building security could be transferred from GSA and possibly other federal agencies to DHS; and DHS' responsibilities could vary, depending on the specific terms of the legislation enacted to create DHS. In our September 17, 2002, report, we suggested that Congress consider clarifying DHS' jurisdiction for federal building security as it deliberates on establishing the new department. In addition, GSA's and other federal entities' responsibilities for other facilities management functions would not be affected by the various pending legislative proposals. Still, the transfer of security responsibilities would separate security from other facility management functions, such as the siting, design, and construction of federal buildings, which play an important role in the provision of appropriate and effective security. However, as long as DHS is given some responsibility for security of facilities, an important responsibility that would need to be considered is integration between security and the other facility management functions.

For the most part, the agencies included in our review either concurred with the information included in a draft of this report, said they had no comments, or provided technical comments that we have reflected in this report, as appropriate. Additionally, the Administrative Office of the U.S. Courts (AOUSC) agreed with our concern about the possible expansiveness of DHS' mission as it could relate to federal building

---

<sup>5</sup>All current bills on the proposed creation of DHS would move FPS from GSA to DHS. In addition to providing security for GSA owned and occupied facilities, FPS also provides the secretariat for ISC.

---

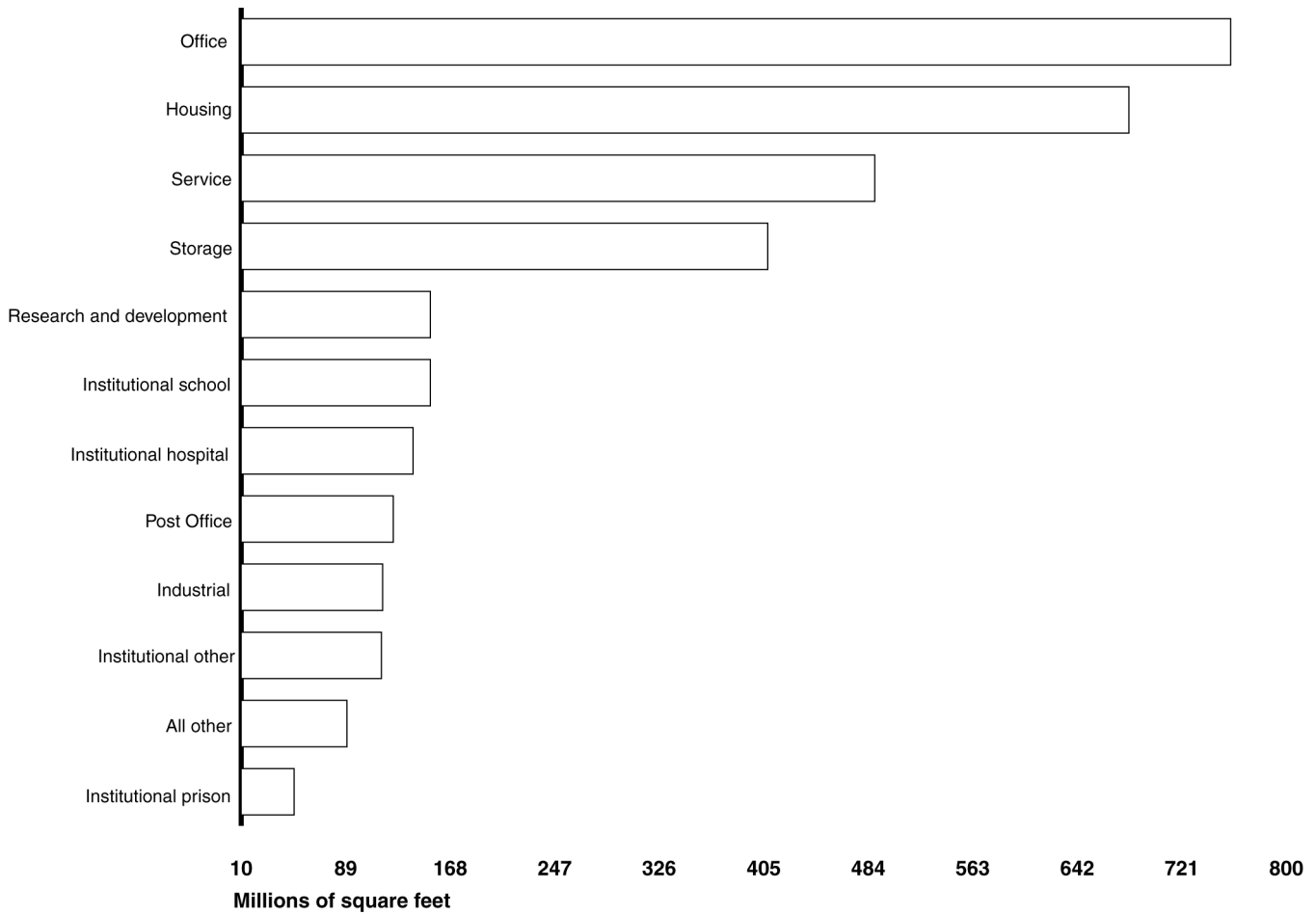
security. Further, the AOUSC expressed concern that the proposed legislation to create DHS does not specifically address the issue of delegations of authority from GSA to various agencies. AOUSC was concerned that these two issues could affect building security arrangements it and other agencies have in place. GSA agreed with the issues raised in the report and said it was developing guiding principles that would address many of these issues when DHS is established. At the same time, GSA said that it believed that the issues agencies have raised concerning their statutory or delegated security authority or law enforcement authorities outside of DHS need to be addressed in defining DHS' mission. We agree and believe that AOUSC's and GSA's concerns reinforce the suggestion we made to Congress in our September 17, 2002, report that it clarify DHS' jurisdiction for federal building security.

---

## Background

The federal government owns or leases more than 3.2 billion square feet of space in more than 500,000 buildings in the United States. This space is broken down into 12 building categories, including office, housing, and storage space. Office space is the largest category representing about 23 percent of the total, or about 758 million square feet. Figure 1 shows the approximate amount of space in each of the 12 categories.

**Figure 1: Total Amount of Federally Owned and/or Leased Space by Category, as of September 30, 2000**



Source: GSA's summary reports of real property owned and leased.

---

The three largest holders of owned and leased office space are GSA, with about 292 million square feet; the defense agencies with about 191 million square feet; and USPS, with about 190 million square feet.<sup>6</sup> In addition to these agencies, over 30 other executive branch agencies, 18 of which are discussed in this report, have some degree of authority to purchase, own, or lease office space or buildings. (See app. II for a listing of the agencies with such authority.)

Physical security for federal office buildings has been a governmentwide concern since the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma. One day after the bombing the President directed the Department of Justice (DOJ) to assess the vulnerability of federal office buildings. In June 1995, DOJ issued a report entitled *Vulnerability Assessment of Federal Facilities*.<sup>7</sup> The study designated security levels I through V into which federal office buildings could be categorized and identified minimum-security standards for each of the five security levels. (See app. III for the definitions of these security levels.) These standards covered perimeter, entry and interior security, and security planning. Fifty-two minimum standards were established with level I having 18 minimum standards and level V having 39 minimum standards. Examples of minimum standards include lighting with emergency power backup for all buildings (perimeter security); intrusion detection systems for building levels III through V (entry security); visitor control systems for building levels II through V (interior security); and standard armed and unarmed guard qualifications/training requirements in all buildings (security planning). In the June 28, 1995, presidential memorandum issuing the DOJ study, the President directed that security at each federal facility, where feasible, be upgraded to the minimum-security standards recommended by the DOJ study.

---

<sup>6</sup>The data on owned and leased space is taken from GSA reports *Summary Report of Real Property Owned, June 2001* and *Summary Report on Real Property Leased, June 2001*. The data in these reports are as of September 30, 2000. We issued a report, *Federal Real Property: Better Governmentwide Data Needed for Strategic Decisionmaking*, [GAO-02-342](#) (Washington, D.C.: April 2002), concerning the accuracy of the data in GSA's report *Summary Report of Real Property Owned*. However, it is the only source available for providing estimates of governmentwide ownership. GSA reported that it currently has about 300 million square feet of space.

<sup>7</sup>DOJ's study only covers office buildings and does not address facilities such as laboratories, nuclear facilities and facilities in foreign countries.

---

The DOJ study also recommended the establishment of the ISC, which was created in October 1995 by executive order. This committee was designed to enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States occupied by federal employees for nonmilitary activities and to provide a permanent body to address continuing governmentwide security for federal facilities.<sup>8</sup>

Prior to the DOJ study on vulnerability assessments, there were no formal governmentwide standards for security at federal buildings. However, in 1988, in response to a request from the 14 agencies that then comprised the Federal Construction Council (now called the Federal Facilities Council),<sup>9</sup> the Building Research Board of the National Research Council established a committee of experts to develop guidance for federal agencies to improve the security of persons, buildings, and information from terrorist attack. The report that was produced by this effort was directed primarily to the heads of the agencies that participated on the Federal Construction Council and, to a lesser extent, to the managers responsible for the individual facilities owned or occupied by these agencies.

In its report,<sup>10</sup> the committee offered the following recommendations to the federal agencies:

- An ongoing security program should be developed and implemented by agencies that own or lease federal office buildings.
- Top management should be responsible for security policy and implementation.
- Security strategies should be developed with a clear understanding and assessment of the threat.
- A formal means of threat communication should be established.

---

<sup>8</sup>GAO-02-1004.

<sup>9</sup>In 1988, the membership of the Federal Construction Council included the U.S. Air Force; U.S. Army; U.S. Navy; the Departments of Commerce, Energy, and State; GSA; NASA; the National Endowment of the Arts; the National Science Foundation; USPS; the U.S. Public Health Service; the Smithsonian Institution; and the Veterans Administration.

<sup>10</sup>Committee on the Protection of Federal Facilities Against Terrorism, Building Research Board, *Protection of Federal Office Buildings Against Terrorism* (National Academy Press, Washington, D.C.: 1988).

- 
- Every federal building should undergo a vulnerability analysis.
  - A base line or minimum level of protection should be established for each federal office building.
  - Temporary protective measures should be systematically reviewed.

The report included detailed guidelines for security management, threat assessment and vulnerability analysis, sites and buildings security, and a vulnerability checklist.

In June 1998, we testified on GSA's efforts to improve federal building security after the Oklahoma City bombing.<sup>11</sup> We reported that although GSA made progress implementing security upgrades in its buildings, it did not have the valid data needed to assess the extent to which completed upgrades had helped to increase security or reduce vulnerability to the greatest threats to federal office buildings. In October 1999, we again testified on GSA's efforts.<sup>12</sup> During that review, we found that the accuracy of GSA's security upgrade tracking system had improved and that almost all of its buildings had been evaluated for security needs. However, a review done in April and May 2000 exposed significant security vulnerability in access control at many government buildings,<sup>13</sup> and another review done in February and March 2002 exposed security vulnerability in access control at four federal office buildings.<sup>14</sup> Further, in September 2002, we reported that the ISC has had limited success in fulfilling its responsibilities.<sup>15</sup>

---

<sup>11</sup>U. S. General Accounting Office, *General Services Administration: Many Building Security Upgrades Made but Problems Have Hindered Program Implementation*, [GAO/T-GGD-98-141](#) (Washington, D.C.: June 4, 1998).

<sup>12</sup>U.S. General Accounting Office, *General Services Administration: Status of Efforts to Improve Management of Building Security Upgrade Program*, [GAO/T-GGD/OSI-00-19](#) (Washington, D.C.: October 7, 1999).

<sup>13</sup>U.S. General Accounting Office, *Security: Breaches at Federal Agencies and Airports*, [GAO/T-OSI-00-10](#) (Washington, D.C.: May 25, 2000).

<sup>14</sup>U.S. General Accounting Office, *Security: Security Breaches at Federal Buildings in Atlanta Georgia*, [GAO-02-668T](#) (Washington, D.C.: April 30, 2002).

<sup>15</sup>[GAO-02-1004](#).

---

The government's security assessment process is still evolving. GSA has adopted a risk management approach to assessing the security of its buildings. GAO has previously reported that for homeland security<sup>16</sup> and information systems security,<sup>17</sup> applying risk management principles can provide a sound foundation for effective security whether the assets are information, operations, people, or federal facilities. These principles, which have been followed by members of the intelligence and defense community for many years, can be reduced to five basic steps that help to determine responses to five essential questions. Because of the vast differences in types of federal facilities and the variety of risks associated with each of them, there is obviously no single approach to security that will work ideally for all buildings. Therefore, following these basic risk management steps are fundamental to determining security priorities and implementing appropriate solutions.<sup>18</sup> Following are the five basic steps in the risk management process:

- Identify assets—What am I protecting?
- Determine the threat—Who are my adversaries?
- Analyze the vulnerabilities—How am I vulnerable?
- Assess risk—What are my priorities?
- Apply countermeasures—What can I do?

However, deciding how much security is really needed is open to debate. In November 1999, the Symposium on Security and the Design of Public Buildings, jointly sponsored by GSA and the Department of State (DOS) in cooperation with the American Institute of Architects, began a national conversation on the balance between security and design in public

---

<sup>16</sup>U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, [GAO-02-208T](#) ((Washington, D.C.: October 31, 2001).

<sup>17</sup>U.S. General Accounting Office, *Information Security Management: Learning From Leading Agencies*, [GAO/AIMD-98-68](#) ((Washington, D.C.: May 1998).

<sup>18</sup>GSA uses a risk-assessment approach whereby threats and vulnerabilities are identified and corresponding security countermeasures are identified to either reduce or eliminate each threat and vulnerability.

---

buildings. Included in the symposium's summary report were the following remarks on the difficulty of resolving the security challenge:<sup>19</sup>

- “There are few, if any, easy answers to security concerns. Risks can be hard to quantify and statistics can be readily misused.”
- “The fact that security is most often addressed by bureaucracies, including such federal entities as the Department of State, GSA, the Department of Justice, the U.S. Marshals Service, the FBI, and many other agencies, adds to the complications related to this issue. Coordination among these agencies, each with its own interests, is difficult. Decision-making can be slow and ineffective in dealing with diverse circumstances and competing concerns. The budget process and the allocation of funds among people, training, and technology can be an imprecise and exhausting exercise. Policies can overlap and, at times, contradict one another.”
- “Security is also an arena full of contradictions and ironies. There are rigid rules and there are large exceptions. Even experts disagree about which solutions work and which do not. And there is a growing divide between those who champion openness and those that advocate security as their first priority.”
- “However clearly, when it comes to security, there are no universal solutions. We must listen to many voices and explore many options. We must be precautionary but also reasonable. Security is an issue that can atomize society so we must pursue it in ways that do not compromise our democratic values or our sense of community. Ultimately, we must find answers to this difficult challenge one building at a time.”

In recent years, the federal government's response to the threat of terrorism has profoundly affected Washington's historic urban design and streetscape. Street closures have disrupted local business activities and increased traffic congestion. The hastily erected jersey barriers, concrete planters, and guard huts that ring our buildings and line our streets mar the beauty of the Nation's Capital. In October 2000, the House and Senate Committees on Appropriations requested the National Capital Planning

---

<sup>19</sup>General Services Administration, *Balancing Security and Openness, A Thematic Summary of a Symposium on Security and the Design of Public Buildings*, November 30, 1999, Ronald Reagan Building and International Trade Center, Washington, D.C.

---

Commission (NCPC) to provide professional planning advice on federal security measures for the Capital. NCPC's goal or objective was to identify urban design solutions that would set a benchmark for security design throughout the Nation's Capital. In its initial report,<sup>20</sup> issued in October 2001, NCPC's Interagency Task Force outlined recommendations for an Urban Design and Security Plan that would promote the safety of those who live in, work in, and visit the Nation's Capital while preserving the openness and historic design that have made Washington an expression of American ideals and one of the world's most admired capital cities.

The plan is the result of a collaborative effort that included a wide range of viewpoints and expertise shared by staff of federal and city agencies; community groups; historic preservationists; nationally recognized urban designers and landscape architects; security experts, including the Secret Service and FBI; and members of the general public. It details how building perimeter security can be seamlessly integrated into consistent, welcoming streetscapes. It focuses exclusively on perimeter building security designed to protect employees, visitors, and federal functions and property from threats generated by unauthorized vehicles approaching or entering sensitive buildings. It does not address other kinds of security measures, such as building hardening (strengthening the exterior of buildings to protect against explosive blasts), operational procedures, or surveillance that individual agencies need to assess.

The plan responds to the alarming proliferation of unattractive, makeshift barriers that have gone up throughout the capital city with increasing frequency since the 9-11 terrorist attacks. It was motivated by several key issues which included providing appropriate levels of perimeter security; providing a seamless system of components that enhance the public realm and provide security; and giving priority to achieving aesthetic continuity along streets.

---

<sup>20</sup>The interagency task force included representatives from the Departments of the Interior, State, the Treasury, Defense, and Justice; GSA, the Central Intelligence Agency, FBI, Secret Service, National Park Service, Federal Highway Administration, the Architect of the Capitol, and Capitol Police; House Committee on Government Reform, Senate Committee on Governmental Affairs, various D.C. government agencies, and other interested parties.

---

The plan includes the following:

- A summary of the building perimeter security considerations that influence the conceptual streetscape designs proposed in the plan.
- Streetscape design concepts that incorporate security components. These conceptual designs illustrate how an array of landscape treatment and street furniture may be applied within various areas of the plan and are not intended as final designs.
- An implementation strategy for design, construction, funding, maintenance, and operations. The implementation program should ensure that work is completed according to the design intent and that improvements are maintained.

NCPC approved the plan on October 3, 2002. It will be forwarded to Congress and the White House for approval. In addition, the plan will be distributed to federal agencies as a guide for integrating security elements into current building perimeter security plans. NCPC believes that this plan can help set the standard for 21<sup>st</sup> Century security design—not only to be used in Washington, D.C., but throughout the nation.

---

## Most Agencies Reported Shared Security Responsibilities

Presidential Decision Directive 63 makes every department and agency of the federal government responsible for protecting its own critical infrastructure. As discussed in our September 2002 report,<sup>21</sup> the ISC was established to address continuing governmentwide security concerns, establish policies and standards for security in and protection of federal facilities and monitor agency compliance. Most of the agencies reported shared security responsibilities between the agency and GSA. Types of security responsibilities include performing security assessments, providing security funding, providing security forces and security technology, and coordinating security efforts among and within agencies.

In May 1998, Presidential Decision Directive 63 was issued with the intent to eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructure. Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy

---

<sup>21</sup>[GAO-02-1004](#).

---

and government. It makes every department and agency of the federal government responsible for protecting its own critical physical infrastructure. This would include the buildings that house critical cyber-based systems.

The ISC, which is chaired by the Administrator of GSA and includes 14 department-level agencies and other executive agencies and officials, has a role in facility security. It was created to provide a permanent body to address continuing governmentwide security concerns. It has three primary security responsibilities relating to the protection of federal facilities for nonmilitary activities: (1) establishing policies for security in and protection of federal facilities; (2) developing and evaluating security standards for federal facilities, including developing a strategy for ensuring compliance with such standards, and overseeing the implementation of appropriate security measures in federal facilities; and (3) taking such actions as may be necessary to enhance the quality and effectiveness of security and protection of federal facilities. In our September 2002 report on the ISC, we said that the ISC has had limited success in meeting its responsibilities. It has issued two official products, one on security design criteria and the other on minimum standards for building access procedures. Members identified factors affecting the ISC performance which included (1) the lack of consistent and aggressive leadership by GSA, (2) inadequate staff support and funding for the ISC, and (3) ISC's difficulty in making decisions. GSA, which chairs ISC, has acknowledged these factors, promised full support, and initiated efforts to address them.

All 22 of the agencies we reviewed have some role in providing security for office space; but for 20 of these agencies, building security involves both GSA and the agencies. Additionally, 18 of the agencies we reviewed own or lease space directly and are responsible for the security of this space. More specifically, security for space may be solely the responsibility of the agency, the responsibility of the agency working in conjunction with the GSA's FPS, or the responsibility of the agency working in conjunction with FPS and another agency. GSA through its FPS has responsibility for protecting the buildings that it occupies to house its operations and the other buildings it owns and leases.

For the agencies we reviewed, three factors determine their security role for office space: whether they have (1) the authority to own or lease real property, (2) assigned GSA space or delegated lease authority from GSA,

---

and (3) delegated security responsibility.<sup>22</sup> First, an agency may have direct authority to own or lease space, in which case it is the agency's responsibility to provide security. Second, if an agency is in GSA assigned space or in leased space obtained using GSA delegated leasing authority, it is GSA's responsibility to provide building security in cooperation with the agency.<sup>23</sup> Third, GSA can delegate security responsibility to an agency located in assigned space or leased space using its delegated leasing authority. In these cases, it is the agencies' responsibility to provide building security. For three agencies, the Department of Education (Education), GSA and SEC, only one factor applies. For 19 of the 22 agencies we reviewed, combinations of these factors apply.

Only the first factor applies to GSA and SEC. Each has direct authority to own and/or lease space and each provides its own security. SEC does not use GSA space. GSA provides no security for SEC. GSA has responsibility for the largest amount of owned and leased office space, approximately 292 million square feet in approximately 8,000 buildings, including space it uses for its own operations. As the government's landlord, GSA assigns space to multiple agencies throughout the government. It provides security for this space, through FPS, unless it has delegated this responsibility to a tenant agency. GSA provides contract guard services for access control to many of its buildings and security equipment for many of its buildings. In buildings with multiple federal tenants, GSA forms building security committees to work with it in determining the security needs of the agencies. Only the second factor applies to Education. Education occupies 35 buildings throughout the country that GSA owns or leases space. GSA is responsible for providing the building security for all the space occupied by Education.

The other 19 agencies involve some combination of two or three of the factors. For GPO and USPS factors one and two apply. GPO and USPS provide security for the properties they own or lease directly, and GSA provides security for the properties GSA controls and in which GPO or USPS is a tenant. For NASA, factors one and three apply. NASA provides

---

<sup>22</sup>If a component of an agency has authority to own or lease space directly, we identified the agency as having that authority. For example, the Food and Drug Administration, Department of Health and Human Services (HHS), has authority to own or lease buildings, so we identified the department as having that authority.

<sup>23</sup>Assigned space refers to the space agencies are given in GSA owned or leased space. This term is used because GSA owns the space or GSA has signed the lease for the space. GSA may delegate its leasing authority to an agency, in which case that agency signs the lease, not GSA.

---

security for the properties it owns or leases directly and has delegated security responsibility for the GSA space it occupies. Three agencies—the Department of Housing and Urban Development (HUD); the Federal Judiciary consisting of the U.S. District Courts and the U.S. Courts of Appeals; and the Social Security Administration (SSA)—combine factors two and three. For example, SSA is assigned space in 1,352 facilities<sup>24</sup> throughout the country and has been delegated security responsibility for only 8 of these facilities. SSA has limited security responsibilities for the other 1,344 facilities since GSA is primarily responsible for security at these buildings.

The Federal Judiciary is different from the other two agencies, in that security is provided through the U.S. Marshals Service (USMS) and GSA. The Judicial Conference Committee on Security and Facilities, supported by the AOUSC, analyzes security issues and develops security recommendations for consideration by the Judicial Conference, the federal judiciary’s policymaking body. AOUSC coordinates with the courts, USMS, and GSA to implement the judiciary’s security program. By law, USMS is responsible for providing security for the U.S. District Courts, U.S. Appeals Courts, and the Court of International Trade. It contracts for court security officers to assist with protection of federal judicial facilities. It also has received delegations of authority for building security from GSA. GSA through FPS assists the USMS in providing security for facilities that are primarily courthouses and provides the majority of security for courts located in multitenant buildings. For example, in multitenant federal buildings that house federal courts, FPS may provide contract guards for security screening, access control and perimeter roving patrols at the facility while USMS provides security for judicial space within the building. In facilities that are primarily courthouses the USMS provides security screening, access control, and security for all judicial areas while FPS may assist in providing perimeter-roving patrol and after hours coverage.<sup>25</sup>

The remaining 13 agencies combine all 3 factors. For example, the Department of Transportation (DOT) owns or directly leases approximately 18,000 buildings, representing approximately 60 million square feet of space nationwide for which it has security responsibility.

---

<sup>24</sup>These facilities may include other federal agencies.

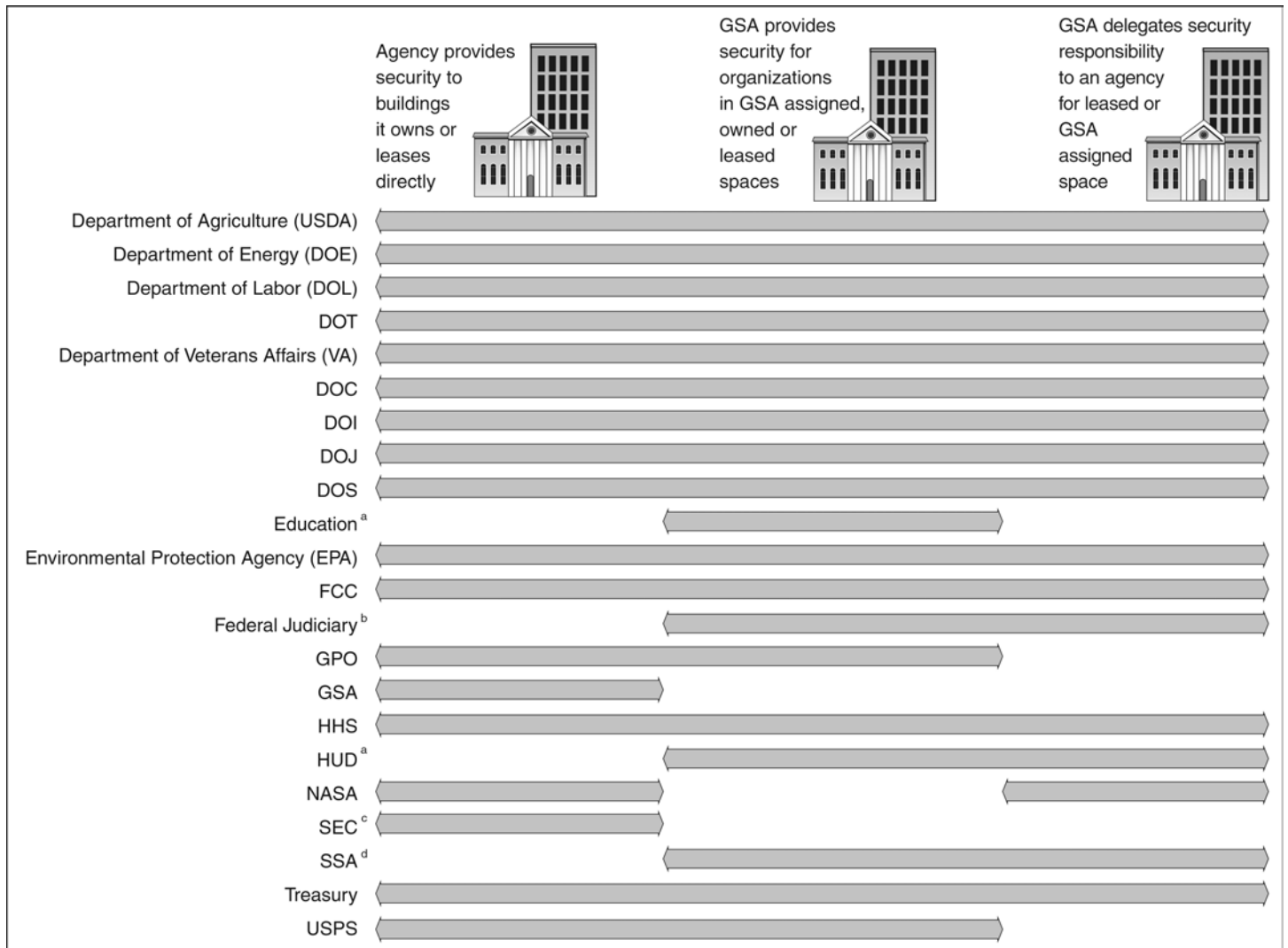
<sup>25</sup>For the Thurgood Marshall building, which houses the AOUSC and is owned by Architect of the Capitol office, guard service is provided through the Architect’s office.

---

GSA has assigned DOT approximately 8 million square feet of space in 400 buildings. GSA has primary security responsibility for 397 of these facilities. DOT has primary security responsibility for the other three buildings that are headquarters buildings, under a delegation of security authority from GSA.

Figure 2 shows a breakdown by agency of building security responsibilities.

**Figure 2: Agencies Building Security Responsibilities**



Note: If a component of an agency did any of the three things in figure 2, we reported the agency as a whole of doing them.

<sup>a</sup>Education does not currently own any buildings obtained from defaulted loans. However, Education does own 111 school buildings that are located on military bases. Education only owns the buildings, with the military owning the underlying land. Due to this unique arrangement, access to these buildings is already limited by the military base restrictions and requirements. The Department of Defense (DOD) operates 66 of the schools, as part of its Domestic Schools Operation. Local school districts use the remaining 45 buildings through long-standing permits to operate the buildings for the education of military dependent children. DOD and the local school districts are responsible for the day-to-day operations, including security, of all of these school facilities. Also, HUD owns buildings from such programs as the Federal Housing Administrations' Mortgage Insurance Program. If an

---

owner defaults on a loan for a property, the mortgage holder files a claim with HUD for the mortgage insurance; and when HUD pays the claim, it takes over ownership until it can auction the property. For this reason, we have identified neither of them as providing security to owned property.

<sup>b</sup>GSA delegates security to USMS for the Federal Judiciary.

<sup>c</sup>SEC has only leasing authority; it does not have authority to own real property.

<sup>d</sup>SSA stated that there is a dispute between GSA and SSA over the ownership of certain facilities bought with SSA trust fund money. SSA also provides security for these buildings. We cannot comment because this issue was outside the scope of our assignment.

Source: Responses from the 22 agencies.

In addition, for agencies we did not review, the U.S. Secret Service is responsible for the security of the White House and certain other executive buildings; the U.S. Capitol Police is responsible for security of the Capitol complex, including the Capitol and House and Senate Office buildings, but GSA provides security for congressional offices located in various states; and the Marshal of the Supreme Court and the Supreme Court Police provide security for the Supreme Court.

---

## Eleven Agencies Reported that They Have Completed Security Assessments of Facilities

GSA and the other agencies we reviewed reported having performed vulnerability, risk, or other security assessments of their buildings to varying degrees. Eleven of the 22 agencies stated that security assessments had been completed on all their facilities since 1995. Nine agencies reported that they were in the process of doing security assessments on their buildings. Two agencies are in only GSA space and GSA is responsible for the security assessments. Table 1 shows the agencies that reported having completed security assessments of their buildings and those that are still working on building security assessments.

**Table 1: Status of Agencies' Security Assessments**

Agencies	Agencies that reported having completed security assessments of all buildings since 1995	Agencies that reported being in the process of completing security assessments <sup>a</sup>
DOC	X	
DOE	X	
DOI		X
DOJ		X
DOL		X
DOS	X	
DOT	X	
Education	b	b
EPA		X
FCC	X	
Federal Judiciary	x <sup>c</sup>	
GPO		X
GSA		X
HHS		X
HUD	b	b
NASA	X	
SEC	X	
SSA	X	
Treasury		X
USDA		X
USPS	X	
VA	X	

Legend:

x represents status of agency assessments.

<sup>a</sup>If some agencies components did not respond to this question, we identified the agencies as being in the process of doing security assessments because we do not know the status of the other component(s).

<sup>b</sup>All of Education's and HUD's spaces are in GSA-assigned space. GSA is responsible for the security assessments of these spaces.

<sup>c</sup>USMS performs security surveys/assessments on a continuing basis.

Source: Responses from the 22 agencies.

According to an FPS official, GSA has performed risk assessments for all its owned properties, but has not completed all of its leased property assessments. GSA uses a process called regional threat assessment, which

identifies the threats, the vulnerabilities, the risks, and countermeasures needed for a building. The information is used to identify security needs, prioritize them, and seek funding for them based on regional prioritization. DOL, which reports being located in 573 buildings nationwide, has direct responsibility for physical security assessments in the 12 DOL-owned buildings. In addition to GSA's security reviews, agencies may perform their own security review of GSA space. Education and SSA report that they have done internal security assessments of their buildings, in addition to those done by GSA. Education reported doing assessments of 26 of 35 buildings, and SSA reported assessing all its buildings. SSA also reported that it is converting its security surveys to the risk assessment format used by GSA.

## A Variety of Security Forces and Technologies Are Used to Provide Building Security

Agencies use their own or contract security forces and technologies such as magnetometers and X-ray machines. Twelve of the 22 agencies reported using federal security forces to provide some of their physical security. All 22 agencies use contract guards to provide some or all of their physical security. SEC reported not using GSA to provide its security. Table 2 shows whether agencies use federal security forces, their own contract guards, or guards contracted by GSA.

**Table 2: Types of Security Forces Used by Agencies**

Agencies	Federal security forces <sup>a</sup>	Contract guards <sup>b</sup> (agency)	FPS <sup>c</sup>	Contract guards (GSA)
DOC	x	x	x	x
DOE	N/A	x	x	x
DOI	x	x	x	x
DOJ	x	x	x	x
DOL	N/A	x	x	x
DOS	N/A	x	x	x
DOT	x	x	x	x
Education	N/A	N/A	x	x
EPA	N/A	x	x	x
FCC	N/A	x	x	x
Federal Judiciary	x <sup>d</sup>	x <sup>d</sup>	x	x
GPO	x	N/A	x	x

(Continued From Previous Page)

Agencies	Federal security forces <sup>a</sup>	Contract guards <sup>b</sup> (agency)	FPS <sup>c</sup>	Contract guards (GSA)
GSA	x	x	x	x
HHS	x	x	x	x
HUD	N/A	x	x	x
NASA	N/A	x	x	N/A
SEC	N/A	x	N/A	N/A
SSA	N/A	x	x	x
Treasury	x	x	x	x
USDA	x	x	x	x
USPS	x	x	x	x
VA	x	x	x	x

Legend:

x represents security forces used by each agency.

Note: N/A represents nonapplicable.

<sup>a</sup>If any part of an agency had federal security forces, we reported the whole agency as having them.

<sup>b</sup>These contracts could be for properties owned or leased directly by the agencies or under delegated authority from GSA.

<sup>c</sup>FPS is only counted as a federal security force for GSA.

<sup>d</sup>USMS provides security and contracts for security guards to protect the Federal Judiciary.

Source: Responses from the 22 agencies.

The following are examples of types of security forces used to provide physical security for buildings by various agencies.

- For the Federal Judiciary, USMS provides the basic building security for courts using both federal security forces and contract court security officers. It contracts for court security officers to assist with protection of federal judicial facilities. It has also received delegations of authority for building security from GSA. GSA through FPS assists the USMS in providing security for facilities that are primarily courthouses and provides the majority of security for courts located in multitenant buildings. In facilities that are primarily courthouses, the USMS provides security screening, access control, and security for all judicial

---

areas while the FPS may assist in providing perimeter-roving patrol and after-hours coverage.<sup>26</sup>

- Various components of Treasury have different methods for providing security. For example, at the U.S. Mint, the U.S. Mint police have responsibility for providing the actual physical security for the buildings it owns. At the Bureau of Engraving and Printing (BEP), physical security is provided by the BEP police for two buildings in Washington, D.C., and one building in Fort Worth Texas. At the Bureau of Public Debt (BPD), the security branch oversees security and has delegated security authority from GSA. BPD contracts for security at its assigned space in Parkersburg, W.Va., but FPS provides security for the space it is assigned in Washington, D.C. At the Office of the Comptroller of the Currency, the property manager, as part of the leases, provides the guard services.
- NASA uses contract guard forces for the properties it independently leases. Its headquarters building is leased through GSA, but NASA has been delegated security responsibilities and uses contract guards to secure headquarters.
- USPS employs its security control officers and Postal Police to provide security for the properties it owns and leases. For the GSA owned or leased space assigned to USPS, GSA provides the contract guards if required.

Along with security forces, agencies use various technologies and procedures to secure their buildings. GSA or the agencies may provide these technologies or establish the procedures. The following is a list of technologies GSA identified as being implemented within various facilities it controls since fiscal year 1996 to meet the minimum standards set by the DOJ study on vulnerabilities.<sup>27</sup> GSA reported using the following technologies, depending on the building's security level, the results of each building's security assessment, and the requests made by individual building security committees in space occupied by multiple agencies:

---

<sup>26</sup>For the Thurgood Marshall building, which houses the AOUSC and other tenants and is owned by Architect of the Capitol, guard service is provided through the Architect's office.

<sup>27</sup>[GAO-02-481T](#).

- 
- CCTV,
  - X-rays machines,
  - magnetometers,
  - window protection features, and
  - exterior lighting and physical barriers.

GSA has also increased security since the September 11, 2001, terrorist attacks at various of its owned and leased facilities with the following equipment:

- bomb detection equipment and canines;
- protection for air intake for heating, ventilation and air conditioning systems; and
- under-vehicle inspection devices.

GSA has also implemented other nontechnological improvements, such as increasing the number of guards.

The other agencies reported having implemented or upgraded a wide variety of security enhancements since 1996. Some of the most commonly identified were the following:

- magnetometers,
- X-ray machines,
- physical access barriers,
- access control measures, and
- CCTV.

Examples of other security enhancements identified by the agencies included the following:

- explosive detection equipment including bomb detecting canines,

- 
- radiation detection equipment,
  - mail handling/anthrax testing,
  - emergency communication equipment,
  - window blast protection,
  - air intake protection,
  - restricted visitor entrances,
  - intrusion detection for rooftops,
  - radios for shuttle drivers, and
  - lockboxes for visiting police official's weapons.

Some agencies also reported implementing security-related procedures, such as directing employees to wear their identification badge at all times, providing visitor escorts, closing streets, and making identification checks outside the building.

---

## Funding of Security Needs

Following the September 2001 terrorist attacks, increased funding was appropriated for this purpose. Specifically, on September 18, 2001, the President signed the Fiscal Year 2001 Emergency Supplemental Appropriations Act, appropriating \$40 billion to respond to the terrorist attacks in the United States. The act provides funding to cover the physical protection of government facilities and employee security. On September 21, 2001, the President allocated \$8.6 million from this appropriation to the Federal Buildings Fund administered by GSA to provide increased security for federal buildings. In the first quarter of fiscal year 2002, FPS received additional funding of \$98.5 million for additional security for federal buildings. The President's fiscal year 2003 budget requests that \$367 million be made available from the Federal Buildings Fund to fund costs associated with implementing security improvements to federal buildings. The following are examples of other agencies included in the review that reported receiving supplemental funding for facility security:

- DOC received approximately \$3.6 million since September 11, 2001, for supplemental guard service and physical security upgrades;

- 
- DOL received an estimated \$5.8 million after September 11, 2001, for security enhancements to its headquarters building;
  - Federal Judiciary received \$85.3 million after September 11, 2001, of which \$65.2 million was for security and \$20.1 million was for mail handling facilities, emergency communications equipment for the courts, and window film for high threat trial locations; and
  - NASA received \$108.5 million after September 11, 2001, of which \$88.5 million was for security enhancements, human resources, and physical/technical counter measures, and \$20 million was for information technology security.

We asked the agencies included in our review to provide data to us on their funding for building security since the Oklahoma City bombing. However, the total amount of funds spent by the 22 agencies dedicated to building security for fiscal years 1996 to 2001 was not readily available. Although funding for building security is specifically identified in some agencies' budgets, such as GSA; this is not the case for others. Agencies varied in the extent to which they reported funding information. The reasons given by those reporting limited cost information included (1) security costs were funded partially by another agency, (2) security costs were part of the lease costs and not separately identified, and (3) security is not a separate line-item for agencies' funding. Further, agencies in GSA assigned space generally pay for basic security services and building specific security services through their rent payments to GSA. The following are examples of what agencies reported and may or may not represent all their security expenditures.<sup>28</sup>

- FPS obligated approximately \$1.3 billion for security for fiscal years 1996 to 2001. Its fiscal year 2002 budget was \$362.1 million, of which about \$207 million was for contract guard services. Additionally in fiscal year 2002, GSA was slated to spend over \$300 million more from its reimbursable program<sup>29</sup> for contract guard services, according to a FPS official. This total of over \$500 million for contract guard services was to fund approximately 7,300 contract guards.

---

<sup>28</sup>Some of the money reported may be duplicative because we could not determine whether all costs were paid directly to the provider by the agencies or through rent payments to GSA.

<sup>29</sup>The reimbursable program provides security funding from the rents paid by agencies assigned space in GSA-owned or -leased buildings; the rent includes a building specific charge for contract guards.

- 
- In fiscal years 1999 to 2001, Federal Judiciary paid \$71.6 million for security through its rent payments to GSA. The Federal Judiciary and the USMS also obligated another approximately \$577.1 million from the Court Security Appropriation. For fiscal year 2002, the Federal Judiciary expected to pay \$36.7 million for security through its rent payments to GSA. Also, in fiscal year 2002, the Federal Judiciary received an appropriation and emergency supplemental for court security officers, court security inspectors, and security systems and equipment, and transferred \$280.5 million to the USMS to administer the Judicial Security Facilities Program.<sup>30</sup> Through its own appropriation, the USMS also received \$24.1 million in funding for construction; security, including guard contracts and security equipment; and furniture to handle serious security deficiencies in federal courthouses related to prisoner handling and the protection of judges, judicial employees, the public and the Marshals.
  - For fiscal years 1996 to 2001, Education paid GSA approximately \$7.7 million in security related expenses. In fiscal year 2002, Education expected to expend approximately \$2.0 million in security related expenses, of which about \$1.9 million was for guard costs.
  - For fiscal years 1996 to 2001, EPA identified security costs of \$55.0 million, of which \$38.6 million were for guard costs. It estimated additional security costs paid through rent to be \$13.9 million for this period.
  - FCC pays basic security costs through its rent to GSA and reported GSA delegated security authority for a guard contract valued at \$2.1 million.
  - For fiscal years 1996 to 2001, HHS reported security obligations of \$209.4 million, including guard costs of \$113.1. In fiscal year 2002, it expected to spend \$102.8 million, of which \$40.1 million is for contract guard costs.
  - For fiscal years 1996 to 2001, DOL reported obligating approximately \$27 million for guard contracts. In fiscal year 2002, it expected to spend \$4.5 million. It pays additional security costs for its GSA space through rent.

---

<sup>30</sup>This includes \$63.3 million of the \$85.3 million supplemental previously discussed.

- 
- For fiscal year 2002, SEC reported costs of \$2.2 million for guard services in New York City, New York and Washington, D.C.; \$1.4 million for security upgrades at both sites; and \$19 million for security features in the new SEC building under construction in Washington, D.C.
  - For fiscal years 1997 to 2001, SSA reported estimated security costs of \$125.9 million, of which \$76.7 million was for guard contracts. For fiscal year 2002, it reported estimated security costs were \$26.5 million, of which \$21.0 million was for guard contracts.
  - For fiscal years 1996 to 2001, DOS reported estimated security costs as approximately \$126.6 million for domestic security, of which about \$95.2 million was for guard costs. For fiscal year 2002, it reported estimated security costs of \$42.4 million.

---

## Security Coordination Efforts among and within Agencies

Security efforts are coordinated among and within agencies in a variety of ways. For instance ISC, OHS, FPS, FBI, and FEMA are organizations that facilitate coordination among agencies. Specifically,

- ISC oversees coordination and cooperation among federal agencies and provides a forum for agencies to discuss security topics of common interest.
- OHS through Homeland Security Presidential Directive 3 established the protection alert levels, which color-code alert levels into 5 colors: green = low/normal; blue = guarded; yellow = elevated; orange = high; and red = severe. OHS mandated that each executive branch agency employ the color-coded system with its respective security alert level program.
- In response to the OHS directive, FPS developed a color-coded alert system for all GSA-owned and -leased facilities under its control. FPS can declare nationwide or regional alerts for its facilities. For example, a regional alert could be used for sensitive trials in a region. Each FPS alert level has a set of corresponding actions to be implemented as deemed appropriate based on the threat and personnel available. FPS also has building security committees in its joint tenant buildings that can share local security information.
- FBI conducts a weekly terrorism briefing that agencies can attend.

- 
- FEMA has a national warning system to which an agency can be linked.

Other agencies through which security information can be shared are the Physical Security Working Group operating under the Department of Defense (DOD) and the Central Intelligence Agency, the Protective Forces Working Group, and the Security Working Group established by the Federal Real Property Council to share information and experiences on building security. Another example of coordination among agencies is the “C” Street Southwest working group whose members include Education, HHS, FEMA, Voice of America, and the Small Business Administration, and is chaired by a FPS officer. The group was formed to discuss common security problems and discuss evacuation planning for the area in which they are all located.

The agencies identified various internal coordination efforts. For example,

- USDA has established an Office of Physical Security as a central point of contact for USDA agencies concerning security questions. It is also developing a Security Steering Board to bring all parts of USDA together to make collaborative decisions that will affect security throughout USDA.
- DOC’s Office of Security’s Counterintelligence Unit reviews, evaluates, and disseminates applicable security information to its offices.
- HHS has a Departmental Physical Security Work Group whose purpose is to disseminate physical security and related information and develop minimum physical security standards for office and special space such as laboratories; staff also coordinate with each other.
- Treasury has the Treasury Threat Advisory Group that meets periodically to discuss and share intelligence within the agencies.

---

## Agencies Identified Barriers to Securing Facilities

The agencies identified various problems in providing adequate security for their facilities. Sixteen of the 22 agencies identified leased space as a problem, and 13 of the 22 agencies identified resources, including funding and/or people as a problem. Other problems were less frequently cited.

Leased space was identified as a problem because agencies reported having difficulty getting the lessor to allow security countermeasures in buildings that are not fully occupied by federal employees. This situation sometimes arises when the federal tenants share the building with private

---

tenants and the lessor does not want to inconvenience the private tenants. For example, the judiciary is often assigned space by GSA in a portion of a nonfederal office building. In such cases, security screening may be provided only at the entrance to the judiciary's assigned space, not at the building entrance. Therefore, weapons and/or hazardous materials can be brought into a building housing judicial officials. Even for buildings that are fully occupied by federal employees, leasing can cause a problem.

Resources, both funding and/or staffing, were also identified by 13 agencies as a problem. Agencies indicated that with the increased security requirements and the need for upgrades, funding shortfalls might delay the timely implementation of security requirements and upgrades. For example, DOT reported that it knows what vulnerabilities exist at its facilities and believes it has identified appropriate security countermeasures that would minimize risk; however, without adequate funding it is limited in its ability to implement the countermeasures. Also, since the creation of the Transportation Security Administration (TSA), FPS, BEP police, and the U.S. Mint police have reported losing police to TSA. BEP also said that it was having difficulty replacing the officers it had lost.

Agencies also identified other problems in implementing or strengthening security, such as the historical nature of a facility, poor quality of contract guards, employee resistance to security measures, location of a facility, and dealing with local governments. Concerning the quality of guards, GSA has developed a standard guard contract with enhanced requirements such as the amount of training for the guards. It is replacing the old contracts as they expire with the new one. A FPS official said that FPS is about half way through the process. DOL identified an example of dealing with local government. A tunnel for an interstate passes directly under its headquarters building. It has submitted a written request to the local jurisdiction to limit the tunnel to cars and small trucks to minimize the security risk, but the request is still under consideration by the local jurisdiction. Also, an official from one of the Treasury bureaus pointed out that control of streets, alleys, traffic patterns, means of entering and exiting buildings, and local zoning decisions also impact security.

---

---

## Implications of the Creation of DHS on Agencies' Security Responsibilities

The creation of a DHS would have significant implications on security responsibilities for GSA and the agencies we reviewed. The security responsibility for the facilities controlled by GSA could shift to DHS, and DHS might be assigned security responsibility for facilities owned, occupied, or secured by the federal government, including any agency, instrumentality, or wholly owned or mixed-ownership government corporation.

The President's DHS proposal as well as the DHS bills pending in the Congress would move FPS from GSA to DHS. The President's proposal and S. 2452 did not specifically address whether DHS' security responsibilities for facilities would include more than just buildings that are GSA owned or occupied. However, H.R. 5005, as passed by the House of Representatives, provides that the DHS Secretary shall protect buildings and grounds and persons on those properties that are owned, occupied, or secured by the federal government, including any agency, instrumentality, or wholly owned or mixed-ownership government corporation. This could include facilities housing DOD, Congress, and the Judiciary. This could include as many as 500,000 buildings. Thus, if such a provision were included in the final legislation, DHS would have significant authority and responsibility for federally owned and leased facilities. Under H.R. 5005, the DHS secretary would have direct authority and responsibility for security governmentwide. Moreover, the DHS Secretary, in consultation with the GSA Administrator, could issue and enforce policies and standards governmentwide. The specific language of the final legislation creating DHS and how it addresses this issue would obviously affect agencies' security responsibilities. In our September 17, 2002, report, we suggested two factors for Congress to consider in deciding which security-related functions DHS should be responsible for providing. These factors were the need for integrating the security functions with the day-to-day management of facility and the challenge that would be associated with providing day-to-day security for all federally owned, occupied, or secured facilities.

However, as long as DHS is given some responsibility for security of facilities, an important responsibility that would need to be considered is integration between security and the facility management functions. Under DHS proposals, DHS would be responsible for property security, but GSA and other agencies with authority to own or acquire space would retain their responsibilities for such functions as choosing facility locations and building design and operation. In addition, agencies will still need to ensure that each property adequately and effectively supports the mission of the

---

occupying agencies or other government entity and that any security systems, procedures, or devices implemented at a facility do not materially hamper the ability of the entity to carry out its mission effectively. DHS would need a way to ensure that building security and other facility management functions such as the siting, design, and construction of federal buildings, which play an important role in the provision of appropriate and effective security, are integrated.<sup>31</sup>

---

## Scope and Methodology

To address our first six objectives which were to determine (1) the roles and responsibilities that federal agencies have in providing security for owned and leased office space they occupy; (2) whether security assessments of facilities have been completed; (3) the types of security forces and technologies being used to secure and protect federal buildings; (4) funding for security operations; (5) the coordination of security efforts between and among agencies to improve or enhance building security; and (6) impediments that make it difficult to tighten security at federal buildings—we provided the agencies with a set of questions to answer. In addition to asking these agencies to respond to our questions, we asked them to provide documentation for such matters as authority to own or lease buildings and authority to have federal security forces. We selected 18 agencies because they were part of our ISC review, and these two assignments were done jointly. We selected NASA because of its large size, and we selected GPO, FCC, and SEC because of their small size. Twenty-one of the agencies responded in writing and one provided information orally. Some of the agencies stated that some of the information was not centralized so that they could not answer the questions in our time frame, and financial information on security is generally not tracked separately from other accounts so they could not provide some or all of the information on security funding. Some of the agencies did not answer certain questions, and for other agencies that sought responses from their various components, some components did not respond with the information requested. Although we reviewed the documentation agencies provided, we did not independently verify the information. We also agreed to provide the types and sources of security-related guidance that are available for agencies to use in addressing building security vulnerabilities

---

<sup>31</sup>See U.S. General Accounting Office *Building Security: Interagency Security Committee Has Had Limited Success in Fulfilling Its Responsibilities*, [GAO-02-1004](#) (Washington, D.C.: September 17, 2002) for additional information.

---

they identify; we reviewed agencies guidance on security they provided and searched the Internet for other security guidance.

To determine the implications of the creation of DHS on building security responsibilities, we reviewed the President's proposal to create DHS, proposed legislation that would create DHS, the Office of Homeland Security's July 2002 National Strategy, Executive Order 13267, and our July 2001 report on security protection for executive branch officials. We also discussed this issue with representatives from OMB, GSA, and OHS.

We conducted our review between December 2001 and September 2002 in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from the 22 agencies that supplied information.

---

## Agency Comments and Our Evaluation

We requested comments on a draft of this report from the appropriate officials at the 22 agencies participating in our review. We received written responses on our draft report from officials in AOUSC, DOE, HUD, and from SSA's Commissioner. Although all four agencies concurred with the information in the report, AOUSC and SSA provided additional comments.

AOUSC agreed with the issues we raised concerning the DHS legislation and is concerned about the impact of the proposed legislation on the judicial branch and other organizations. Further, its response pointed out that an amendment by Senator Lieberman to H.R. 5005, which would transfer FPS from GSA to DHS, could impinge upon current judiciary security arrangements. Also, the judiciary is concerned because under such a transfer the legislation does not address delegation of security authority from GSA to other agencies and this could impact GSA's delegation of security authority to the USMS for judicial building security. It is concerned that DHS might assume certain authorities for judicial security that now reside with the USMS. The judiciary believes that Congress probably did not intend for DHS to impinge upon current authorities, be they statutory or delegated to USMS. (See app. IV.) The judiciary also provided technical comments that have been included in the report, as appropriate. SSA suggested that we note in the report a dispute between it and GSA over the ownership of certain facilities bought with SSA trust fund money, which we have done.

We received oral or E-mail responses on our draft report from program officials or our liaisons in 17 agencies. USDA, GSA, and VA concurred with

---

the information in the report. USDA provided a technical change, which has been added to this report, and pointed out that it has many special-use facilities that were not addressed in DOJ's 1995 report on building security. USDA also said that it endorses GSA's risk-based approach to building security in that the approach in DOJ's report is too limiting given USDA's mix of facilities. GSA pointed out that FPS is proceeding in its planning for the transition to DHS with the understanding that the mission and function of FPS will continue to be the same in DHS. According to GSA, FPS is working with GSA's Public Buildings Service in developing guiding principles that will form the basis of their relationship after the transition and address the issues raised in this report. GSA also pointed out that the concerns a number of agencies raised about their statutory or delegated security authority for building protection if DHS should be established are valid and need to be addressed in defining DHS' mission. DOI, DOJ, DOL, DOS, DOT, EPA, Education, FCC, GPO, HHS, NASA, SEC, Treasury, and USPS had no comments. DOJ, DOT, EPA, Education, FCC, GPO, HHS, and SEC provided technical comments, which have been included in this report, as appropriate. DOC did not provide comments on this report.

We believe that the issues raised by AOUSC and GSA regarding agencies' statutory or delegated security authorities under the proposed DHS legislation reinforce the suggestion we made in our September 17, 2002, report to you that Congress clarify DHS' jurisdiction with respect to federal building security as it deliberates establishing the new department.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 7 days from the report date. At that time, we are sending copies of this letter to the Ranking Minority Member of the Senate Committee on Governmental Affairs, other appropriate congressional committees, to the heads of the agencies that participated in our review and other interested organizations. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO web site at <http://www.gao.gov>.

---

If you or your staff have any questions about this report, please contact Ron King or me on (202) 512-2834. Major contributors to this report include Ron King, Tom Keightley, Lisa Wright-Solomon, John Vocino, Shirley Bates, and Mike Yacura.

A handwritten signature in black ink, appearing to read "Bernard L. Ungar". The signature is written in a cursive style with a large, sweeping initial 'B'.

Bernard L. Ungar  
Director, Physical Infrastructure Issues

# Guidance Available to Help Agencies Address Security-Related Issues

Many agencies have developed guidance to help building owners and facility managers in addressing issues related to building security and terrorist attacks, as well as security needs and disaster response plans for events such as fire, natural disasters, and bomb threats. To identify and compile the following list, we reviewed agencies guidance on security they provided and searched the Internet for other security guidance.

The following list is not all inclusive. Available guidance is usually updated regularly as additional agencies and evolving technologies identify new protective recommendations.

Agencies	Reference or Link	Description
American Society of Civil Engineers (ASCE)	<a href="http://ascestore.aip.org">http://ascestore.aip.org</a> <i>Vulnerability and Protection of Infrastructure Systems: The State of the Art</i>	An ASCE 2002 publication that discusses the risk, vulnerability, and protection of civil infrastructures. It includes analysis of damage and failure of constructed facilities under fires; analysis of blast damage to the Murrah Federal Building; protection of civil infrastructure facilities from damage from bomb blasts; analysis of infrastructure risk from a systems perspective; and methodological advances in disaster response planning.
American Society of Heating, Refrigeration and Air Conditioning Engineers (ASHRAE)	<a href="http://www.ashrae.org/">http://www.ashrae.org/</a> <i>Risk Management Guidance for Health and Safety under Extraordinary Incidents</i>	Report prepared by the ASHRAE Presidential Study Group on Health and Safety under Extraordinary Incidents that provides recommendations for owners and managers of existing buildings.
American Society for Industrial Security (ASIS)	<a href="http://www.asisonline.org/">http://www.asisonline.org/</a>	Locates security specialists and provides the <i>Crises Response Resources</i> link to find information related to terrorism and building security.
Building Owners and Managers Association (BOMA)	<a href="http://www.boma.org/emergency/">http://www.boma.org/emergency/</a> <a href="http://www.boma.org/pubs/bomamp.html">http://www.boma.org/pubs/bomamp.html</a> <i>How to Design and Manage Your Preventive Maintenance Program</i>	Information on emergency planning and security assessments. Recommendations to effectively manage and maintain a building's systems. (Information for purchasing only).
Centers for Disease Control and Prevention (CDC)	<a href="http://www.cdc.gov/">http://www.cdc.gov/</a> <i>Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks, May 2002</i> <i>Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response</i>	Health guidance for chemical, biological, or radiological (CBR) agents. Document identifies actions that a building owner or manager can implement without undue delay to enhance occupant protection from and airborne CBR attack. Recommendations of the CDC Strategic Planning Workgroup
Central Intelligence Agency (CIA)	<a href="http://www.cia.gov/cia/publications/cbr-handbook/cbr-book.html">http://www.cia.gov/cia/publications/cbr-handbook/cbr-book.html</a> <i>Chemical, Biological, Radiological Incident Handbook</i>	Unclassified document describing potential CBR events, recognizing potential CBR events, differences between agents, common symptoms, and information for making preliminary assessments when a CBR release is suspected.

**Appendix I**  
**Guidance Available to Help Agencies Address**  
**Security-Related Issues**

(Continued From Previous Page)

Agencies	Reference or Link	Description
Federal Facilities Council (FFC)	<a href="http://www4.nas.edu/cets/ffc.nsf/web/chemical">http://www4.nas.edu/cets/ffc.nsf/web/chemical</a> and biological threats to buildings/OpenDocument	Online notes and presentations from FFC seminar on chemical and biological threats to buildings.
International Facility Management Association (IFMA)	<a href="http://www.ifma.org/">http://www.ifma.org/</a>	Information on security-related training courses.
Lawrence Berkeley National Laboratory	<a href="http://securebuildings.lbl.gov">http://securebuildings.lbl.gov</a>	Web site with advice for safeguarding buildings against chemical or biological attack.
National Capital Planning Commission (NCPC)	www.ncpc.gov  <i>Designing for Security in the Nation's Capital</i> , October 2001	In recent years, there has been an increasing concern about the hodge-podge of solutions that have no aesthetic continuity or urbanistic integrity as each federal agency responds to its own individual security needs. This report addresses the need for a comprehensive urban design plan that provides adequate security while at the same time enhances the unique character of the Nation's Capital.
	<i>The National Capital Urban Design and Security Plan</i> , October 2002	The plan offers an urban design framework that focuses exclusively on perimeter building security designed to protect employees, visitors, and federal functions and property from threats generated by unauthorized vehicles approaching or entering sensitive buildings. It does not address other kinds of security measures, such as building hardening, operational procedures, or surveillance. It deals with security in the context of a citywide program of streetscape enhancement and public realm beautification, rather than a separate or redundant system of components whose only purpose is security.
National Institute of Building Sciences (NIBS)	www.wbdg.org  <i>Whole Building Design Guide</i>	Internet site featuring security-related design information.
National Research Council	<a href="http://nap.edu/openbook/N1000265/html/R1.html">http://nap.edu/openbook/N1000265/html/R1.html</a>  <i>Protection of Federal Office Buildings Against Terrorism</i> , National Academy Press, 1988	Report includes security guidelines for buildings and sites, as well as guidelines for security management. Also includes guidelines for scaling back or removing security measures when they are no longer needed.
Occupational Safety and Health Administration (OSHA)	<a href="http://www.osha.gov/bioterrorism/anthrax/matrix">http://www.osha.gov/bioterrorism/anthrax/matrix</a>  <i>Workplace Risk Pyramid</i>	OSHA developed a risk reduction matrix to offer basic advice and suggest protective measures that it believes will reduce the risk of exposure to bacillus anthracis (anthrax) in light of current concerns about the presence of anthrax spores in the workplace. The workplace risk pyramid has three zones—Red (confirmed anthrax spore contamination); Yellow (possible contamination); and Green (unlikely contamination). The level of risk in any particular workplace is based upon specific factors which are outlined on the website.

**Appendix I**  
**Guidance Available to Help Agencies Address**  
**Security-Related Issues**

(Continued From Previous Page)

Agencies	Reference or Link	Description
Sandia National Laboratories	<a href="http://www.sandia.gov/capabilities/homeland-security/index.html">http://www.sandia.gov/capabilities/homeland-security/index.html</a>	<p>A resource for information on a variety of counter-terrorism and homeland security technologies research and development such as,</p> <ul style="list-style-type: none"> <li>• risk assessment methodology and computer applications for federal buildings;</li> <li>• explosives detection technology for vehicle inspections;</li> <li>• research to evaluate the feasibility of developing a glass material that can be used effectively in blast environments to reduce injuries to building occupants;</li> <li>• tools for assessing vulnerability of buildings to chemical and biological attacks; and</li> <li>• advanced modeling and simulation capabilities and expertise for analyzing critical infrastructures, their interdependencies, vulnerabilities, and system complexities.</li> </ul>
The American Institute of Architects (AIA)	<a href="http://www.aia.org">http://www.aia.org</a>	A resource center that offers architects and others, up-to-date, in-depth material on building security issues.
	<i>Building Security Through Design</i>	A primer on how security needs in buildings are defined and describes concepts and strategies for shaping design responses, among other issues.
The Infrastructure Security Partnership (TISP)	<a href="http://www.tisp.org">www.tisp.org</a>	<p>An association of public and private sector agencies that collaborate on issues related to the security of the nation's built environment. Its purpose is to act as a national asset facilitating dialogue on domestic infrastructure security and offering sources of technical support and sources for comment on public policy related to the security of the nation's built environment leveraging members' collective technical expertise and research and development capabilities. Its objectives are to</p> <ul style="list-style-type: none"> <li>• promote joint efforts to improve antiterrorism and asset protection methods/techniques;</li> <li>• promote the participation of all interested agencies and ensure effective communication between all participating entities, from the national to the state and local level;</li> <li>• cooperate in identifying and disseminating security data and information;</li> <li>• promote effective and efficient transfer of infrastructure knowledge from research to codes, standards, public policy and general practice;</li> <li>• encourage synergy between agencies to react quickly and positively to issues of significance;</li> <li>• promote effective professional relationships to further the advancement of the infrastructure industry;</li> <li>• encourage and support the development of a methodology for assessing vulnerabilities;</li> <li>• encourage the establishment of protocols related to the sensitivity of information generated and distributed by the Partnership; and</li> <li>• consider the consequences of antiterrorism and asset protection measures on occupants of facilities and emergency responders.</li> </ul>

**Appendix I**  
**Guidance Available to Help Agencies Address**  
**Security-Related Issues**

(Continued From Previous Page)

Agencies	Reference or Link	Description
U.S. Army Corps of Engineers (USACE)	<a href="http://buildingprotection.subcom.army.mil/basic/">http://buildingprotection.subcom.army.mil/basic/</a>  Technical Instruction 853-01, Oct. 2001 (Draft) <i>Protecting Buildings and Their Occupants from Airborne Hazards</i>	Document presents a variety of ways to protect building occupants from airborne hazards—to prevent, protect against, and reduce the effects of outdoor and indoor releases of hazardous materials. It contains guidance for building managers, designers, and security planners on how to minimize the potential effects of hazardous materials released in accidents, malicious acts, or natural phenomena.
U.S. Environmental Protection Agency (EPA)	<a href="http://www.epa.gov/iaq/largebldgs/baqtoc.html">http://www.epa.gov/iaq/largebldgs/baqtoc.html</a>  <i>Building Air Quality: A Guide for Building Owners and Facility Managers</i>  <a href="http://www.epa.gov/iaq/schools/">http://www.epa.gov/iaq/schools/</a>  Indoor Air Quality (IAQ) Tools for Schools Kit	Provides procedures and checklists for developing a building profile and performing preventive maintenance in commercial buildings.  Provides procedures and checklists for developing a building profile and performing preventive maintenance in schools.
U. S. Fire Administration	<a href="http://www.usfa.fema.gov/cipc">www.usfa.fema.gov/cipc</a>  <i>The Critical Infrastructure Protection Process – Job Aid</i>	Document provides a model process or template for the systematic protection of critical infrastructure.

**Appendix I**  
**Guidance Available to Help Agencies Address**  
**Security-Related Issues**

(Continued From Previous Page)

Agencies	Reference or Link	Description
U. S. General Services Administration (GSA)	<a href="http://hydra.gsa.gov/pbs/pc/facilitiesstandards/">http://hydra.gsa.gov/pbs/pc/facilitiesstandards/</a>  <i>Facility Standards for the Public Buildings Service (PBS-P100) (rev. Nov. 2000)</i>	Establishes design standards and criteria for new buildings, major and minor alterations, and work in historic structures for the Public Buildings Service. Chapter 8 of the document focuses specifically on security design.
	<i>Balancing Security and Openness (PBS)</i>	A thematic summary of a Symposium on Security and the Design of Public Buildings.
	<i>Occupant Emergency Program Guide (FPS), March 2002</i>	A publication providing a step-by-step guide to assist federal agencies in meeting the Federal Management Regulations occupant emergency program requirements.
	<i>Making Federal Buildings Safe (FPS)</i>	Document provides tips and guidance. Topics covered include how to handle suspicious and possibly contaminated mail; actions for a telephone threat; actions for a chemical/biological threat; actions for a bomb threat; and what to do if faced with a gun, knife, or weapon threat.
	<a href="http://www.gsa.gov/mailpolicy">http://www.gsa.gov/mailpolicy</a> <i>Mail Center Manager's Security Guide – Second Edition</i>	This guide was developed to assist federal mail center managers with keeping mail center safe and secure. The guide includes <ul style="list-style-type: none"> <li>• elements of a mail center security plan,</li> <li>• descriptions of those elements,</li> <li>• tips for training and communications,</li> <li>• suggestions on creating and reviewing security procedures,</li> <li>• list of resources, and</li> <li>• a security checklist.</li> </ul>
	<i>July 2002 GSA Advisory on Managing Anthrax Threats in D.C.-Area Mail Centers</i>	GSA offers these guidelines as standard operating procedures for dealing with potential anthrax contamination specifically in the Washington, D.C. area. These guidelines should be implemented to the extent that a worksite-specific assessment shows they are appropriate. They include guidance on threat assessment, incident response, detection equipment and routine sampling, and planning and communications.
	July 19, 2002, Memorandum for Federal Mail Managers and First Responders to Federal Mail Centers	This is a memorandum from the Executive Office of the President, Office of Science and Technology Policy. It addresses the purchase of anthrax detection technologies. It advises agencies to cease issuing any new procurement requests, task orders, purchase orders, or contracts for the purchase of new equipment or services that may detect, sample, test or filter air for bacillus anthracis (anthrax) as the method for assaying suspicious mail, or for routine environmental sampling of mail rooms since many of the commercially available have been shown to give a significant number of false positive readings, which could cause unnecessary medical intervention with its own risk.

---

**Appendix I**  
**Guidance Available to Help Agencies Address**  
**Security-Related Issues**

---

(Continued From Previous Page)

<b>Agencies</b>	<b>Reference or Link</b>	<b>Description</b>
U. S. Postal Inspection Service	<a href="http://www.usps.com/postalinspectors/is-pubs.htm">http://www.usps.com/postalinspectors/is-pubs.htm</a>  <i>Mail Center Security Guidelines, Publication 166, September 2002</i>	This guide provides general advice and recommends protective measures to help assess, prevent, and respond to threats from weapons of mass destruction (chemical; biological, including anthrax bacteria; and radiological), and mail bombs and bomb threats, as well as mail center theft.

---

Source: GAO.

# Federal Executive Branch Agencies with Some Level of Independent Authority to Acquire Real Property, Calendar Year 2000

---

This information is from *Facilities Location: Agencies Should Pay More Attention to Cost and Rural Development Act*. ([GAO-01-805](#), July 31, 2001).

Agency for International Development  
American Battle Monuments Commission  
Appalachian Regional Commission  
Bonneville Power Administration  
Central Intelligence Agency  
Department of Agriculture  
Department of Commerce  
Department of Defense  
Department of Education  
Department of Energy  
Department of Health and Human Services  
Department of Housing and Urban Development  
Department of the Interior  
Department of Justice  
Department of Labor  
Department of State  
Department of Transportation  
Department of the Treasury  
Department of Veterans Affairs  
Environmental Protection Agency  
Federal Emergency Management Agency  
General Services Administration  
National Aeronautics and Space Administration  
National Archives and Record Administration  
National Science Foundation  
National Transportation Safety Board  
Panama Canal Commission  
Pennsylvania Avenue Development Corporation  
Securities and Exchange Commission  
Smithsonian Institution  
Tennessee Valley Authority  
Broadcasting Board of Governors  
U.S. Parole Commission  
U.S. Postal Service  
U.S. Sentencing Commission  
U.S. Trade Representative

# Definition of Security Levels I through V from DOJ's Vulnerability Assessment of Federal Facilities, June 28, 1995

---

## **Level I**

A level I facility has 10 or fewer federal employees. In addition, the facility likely has 2,500 or less square feet of office space and a low volume of public contact or contact with only a small segment of the population. A typical level I facility is a small storefront-type operation, such as a military recruiting office.

## **Level II**

A level II facility has between 11 and 150 federal employees. In addition, the facility likely has from 2,500 to 80,000 square feet; a moderate volume of public contact; and federal activities that are routine in nature, similar to commercial activities. A typical level II building is the Social Security Administration Office in El Dorado, Colorado.

## **Level III**

A level III facility has between 151 and 450 federal employees. In addition, the facility likely has from 80,000 to 150,000 square feet and a moderate to high volume of public contact. Tenant agencies may include law enforcement agencies, courts<sup>32</sup> and related agencies and functions, and government records and archives. A typical level III building is the Pension building, a multitenant, historical building between 4th and 5th Streets on F Street, N.W., Washington, D.C.

## **Level IV**

A level IV facility has over 450 federal employees. In addition, the facility likely has more than 150,000 square feet; high volume of public contact; and tenant agencies that may include high-risk law enforcement and intelligence agencies, courts, judicial offices, and highly sensitive government records. A typical level IV building is the Department of Justice Building on Constitution Avenue in Washington, D.C.<sup>33</sup>

---

<sup>32</sup>This is the definition included in the DOJ study. However, all courts have been identified as being level IV.

<sup>33</sup>This is the definition included in the DOJ study. However, the DOJ Building on Constitution Avenue in Washington, D.C. has been identified as being level V.

---

**Appendix III**  
**Definition of Security Levels I through V from**  
**DOJ's Vulnerability Assessment of Federal**  
**Facilities, June 28, 1995**

---

**Level V**

A level V facility is a building such as the Pentagon or CIA Headquarters that contains mission functions critical to national security. A level V facility is similar to a level IV facility in terms of number of employees and square footage.

# Comments from the Administrative Office of the United States Courts



LEONIDAS RALPH MECHAM  
Director

ADMINISTRATIVE OFFICE OF THE  
UNITED STATES COURTS

CLARENCE A. LEE, JR.  
Associate Director

WASHINGTON, D.C. 20544

October 21, 2002

Mr. Bernard L. Ungar  
Director, Physical Infrastructure Issues  
U.S. General Accounting Office  
441 G Street, N.W.  
Washington, D.C. 20548

Dear Mr. Ungar:

The Administrative Office of the U.S. Courts (AO) appreciates the opportunity to comment on the draft report entitled *Building Security: Security Responsibility for Federally Owned and Leased Facilities*. The AO has one substantive comment; the enclosure to this letter provides several technical corrections.

The AO agrees with the issues that the GAO raises regarding the Department of Homeland Security (DHS) legislation. The AO shares the concern of the GAO that H.R. 5005, as written, could impact upon the security arrangements of the Judicial Branch and other organizations. Likewise, the amendment by Senator Lieberman to H.R. 5005 which the Senate has been considering could impinge upon the current security arrangements for the judiciary. The delegation of authority for court security from the General Services Administration to the United States Marshals Service would not necessarily be maintained under this legislation.

The judiciary also agrees with the views expressed by the Department of State on the prior GAO report (GAO-02-1004) regarding the need for the DHS legislation to address delegations of security authority from GSA to other agencies. Without clarification, DHS might assume certain authorities for judicial security that now reside with the United States Marshals Service. The judiciary believes that it is probably not the intent of Congress for the DHS to impinge upon the current authorities, be they statutory or delegated to the Marshals Service.

It is fortunate that the GAO has raised this timely and important issue.

Sincerely,

A handwritten signature in cursive script, appearing to read "Clarence Lee, Jr.", written in black ink.

Clarence A. Lee, Jr.  
Associate Director

Enclosure

---

A TRADITION OF SERVICE TO THE FEDERAL JUDICIARY

---

## GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site ([www.gao.gov](http://www.gao.gov)) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to [www.gao.gov](http://www.gao.gov) and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

---

## Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office  
441 G Street NW, Room LM  
Washington, D.C. 20548

To order by Phone:   Voice: (202) 512-6000  
                                  TDD: (202) 512-2537  
                                  Fax: (202) 512-6061

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Public Affairs

Jeff Nelligan, managing director, [NelliganJ@gao.gov](mailto:NelliganJ@gao.gov) (202) 512-4800  
U.S. General Accounting Office, 441 G Street NW, Room 7149  
Washington, D.C. 20548

---

**United States  
General Accounting Office  
Washington, D.C. 20548-0001**

**Presorted Standard  
Postage & Fees Paid  
GAO  
Permit No. GI00**

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

**Address Service Requested**

---

