United States General Accounting Office

GAO

Report to the Committee on Government Reform and the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House of Representatives

December 2003

INFORMATION SECURITY

Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies

GAO-04-157

GAO
Accountability•Integrity•Reliability

Highlights

Highlights of GAO-04-157, a report to the House Committee on Government Reform and the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Why GAO Did This Study

The federal government is increasingly using online applications to provide access to information and services and to conduct internal business operations. In light of this trend, strong security assurances are needed to properly safeguard sensitive, personal, and financial data, in part by ensuring that the identities of those who use such applications are appropriately authenticated. When fully and properly implemented, public key infrastructure (PKI) offers many of these assurances. In 2001, GAO reported that the federal government faces a number of challenges in deploying PKI technology (GAO-01-277). GAO was requested to follow up this work by (1) determining the status of federal PKI activities, including initiatives planned or under way at 24 major federal departments and agencies, as well as the status and planned activities of the Federal Bridge Certification Authority (FBCA) and Access Certificates for Electronic Services (ACES) programs, and (2) identifying challenges encountered by the 24 agencies in implementing PKI initiatives since the 2001 report was issued.

In commenting on a draft of this report, GSA and OMB officials generally agreed with its content and conclusions. Technical comments provided by OMB have been addressed as appropriate.

www.gao.gov/cgi-bin/getrpt?GAO-04-157.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

December 2003

INFORMATION SECURITY

Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies

What GAO Found

PKI and its associated hardware, software, policies, and people can provide greater security assurances than simpler means of authenticating identity, such as passwords. In pursuit of these benefits, 20 of the 24 agencies reported that they are undertaking a total of 89 PKI initiatives. The 89 initiatives are at various stages of development, and collectively they represent a significant investment, estimated at about $1 billion. In addition, the governmentwide FBCA and ACES programs continue to promote the adoption and implementation of PKI, but these programs have seen mixed progress and results. The level of participation in the FBCA, which provides a means to link independent agency PKIs into a broader network, is the same as in 2001—four agencies have been certified as meeting technical and security requirements to interconnect through the network. Additional organizations are planning to participate in the future, including four federal agencies and some nonfederal organizations, such as the state of Illinois, the Canadian government, and educational consortiums. Similarly, the ACES program, which offers agencies various PKI services through a General Services Administration (GSA) contract, has seen lower than expected participation by federal agencies. GSA plans to revise the pricing structure associated with the ACES program to encourage participation.

PKI implementation continues to pose major challenges for agencies, which are shown in the table. Many of these challenges are similar to those identified in GAO's 2001 report. In that report, GAO recommended that the Office of Management and Budget (OMB), working with other key federal entities, take action to address these challenges, including establishing a governmentwide framework of policy and technical guidance and a program plan for the federal PKI. GAO also recommended that OMB take steps to ensure that agencies adhere to federal PKI guidance. OMB has not yet fully addressed the recommendations related to the construction of a PKI policy framework, but it issued a policy memorandum in July 2003 that lays out steps for consolidating investments related to authentication and identity management processes across government.

Challenges to Implementation of PKI

Challenge	Description
Policy and guidance	These are lacking or ill-defined in a number of areas, including both technical standards and legal issues.
Funding	Besides the high costs associated with the technology, cost models are lacking that would aid budgeting, and cost is increased when systems must be designed to accommodate the uncertainty associated with undefined standards.
Interoperability	Integrating PKI systems with other systems (such as network, security, and operating systems) often requires significant changes or even replacement of existing systems.
Training and administration	Training is required for personnel to use and manage PKI, and basic PKI requirements and processes impose significant administrative burdens.

Source: GAO.

Contents

Abbreviations

ACES	Access Certificates for Electronic Services
FBCA	Federal Bridge Certification Authority
GSA	General Services Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PKI	public key infrastructure

GAO

Accountability ⋆ Integrity ⋆ Reliability

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

December 15, 2003

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

The Honorable Adam H. Putnam
Chairman, Subcommittee on Technology, Information Policy,
  Intergovernmental Relations and the Census
Committee on Government Reform
House of Representatives

Increasingly, the federal government is using the World Wide Web and other Internet-based applications to provide online public access to information and services as well as to improve internal business operations. To properly conduct communications and transactions with the government over the Internet may require security assurances that go beyond simple security measures—such as passwords—to properly safeguard sensitive, personal, and financial data. Public key infrastructure (PKI)[1] offers many of the security assurances that, when fully and properly implemented, can protect online communications and transactions. In 2001, we reported that the federal government must address a number of challenges before PKI technology can be effectively deployed, including providing well-defined PKI policies and guidance; addressing funding constraints; ensuring interoperability; and managing training and administrative problems.[2] This report responds to your request that we (1) determine the status of federal PKI activities, including initiatives planned or under way at 24 major federal departments and agencies,[3] as well as the status and planned activities of the Federal Bridge Certification Authority (FBCA) and Access Certificates for Electronic Services (ACES) programs, and (2) identify

[1] PKI is a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances—including confidentiality, data integrity, authentication, and nonrepudiation—that are important in protecting sensitive communications and transactions.

[2] U.S. General Accounting Office, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: Feb. 26, 2001).

[3] Major federal departments and agencies included the 24 organizations subject to the Chief Financial Officers Act at the time we began our review; these do not include the newly established Department of Homeland Security.

challenges encountered by these 24 agencies in implementing PKI initiatives since our 2001 report was issued.

To address these objectives, we conducted a structured query at 24 major federal departments and agencies to obtain up-to-date information on PKI initiatives planned or under way across government since 2001, including information on the costs associated with PKI projects, the number of certificates issued, and other details on project-related issues. As part of the query, we obtained information on key challenges to implementing and deploying PKI technology. We also interviewed key officials responsible for or involved in the FBCA and ACES programs to obtain information on the status of PKI activities. In addition, we conducted follow-up discussions with selected agency officials to verify or clarify their responses to the query as needed. All 24 agencies responded to our query. We did not independently verify the information provided by agencies. Our evaluation work was completed between November 2002 and July 2003 in accordance with generally accepted government auditing standards.

On September 12, 2003, we provided your staff with a briefing on the results of our study. The slides from that briefing[4] are included as appendix I to this report. The purpose of this report is to provide you with the published briefing slides.

In summary, we found that of the 24 agencies involved in our query, 20 are pursuing a total of 89 PKI initiatives. The 89 initiatives are at various stages of development, and collectively they represent a significant investment, estimated at about $1 billion. In addition, the governmentwide FBCA and ACES programs continue to promote the adoption and implementation of PKI, but these programs have seen mixed progress and results. The level of participation in the FBCA, which provides a means to link independent agency PKIs into a broader network, is the same as in 2001—four agencies are certified to operate through the network. Additional agencies are planning to participate in the future, as well as nonfederal organizations, such as the state of Illinois, the Canadian government, and educational consortiums. Similarly, the ACES program, which offers agencies various PKI services through a General Services Administration (GSA) contract, has garnered lower than expected participation among federal agencies.

[4] We have amended the briefing as of November 25, 2003, to include technical corrections and clarifications.

GSA plans to revise the pricing structure associated with the ACES program to improve participation levels.

PKI implementation continues to pose major challenges for agencies, and many of these challenges are similar to those identified in our 2001 report. The challenges identified by agencies involved in our query fell into the following general categories:

- *Policy and guidance.* These are lacking or ill-defined in a number of areas, including both technical standards and legal issues.

- *Funding.* Besides the high costs associated with the technology, cost models are lacking that would aid budgeting, and cost is increased when systems must be designed to accommodate the uncertainty associated with undefined standards.

- *Interoperability.* Integrating PKI systems with other systems (such as network, security, and operating systems) often requires significant changes or even replacement of existing systems.

- *Training and administration.* Training is required for personnel to use and manage PKI, and basic PKI requirements and processes impose significant administrative burdens.

In 2001, we recommended that the Office of Management and Budget (OMB)—working with other key federal entities, such as the Chief Information Officers (CIO) Council and the National Institute of Standards and Technology (NIST)—take action to address the PKI implementation challenges that we had identified, including establishing a governmentwide framework of policy and technical guidance and a program plan for the federal PKI. We also recommended that OMB take steps to ensure that agencies adhere to federal PKI guidance.

OMB has not yet fully addressed our recommendations related to the construction of a framework of policy and technical guidance for PKI, but it issued a policy memorandum in July 2003 that lays out steps for consolidating investments related to authentication and identity management processes across government, including a timetable for consolidation of agency investments in identity credentials and PKI services. Shared service providers were to be selected to manage credentials and PKI services by December 2003, and agencies are expected to migrate to these services by 2005.

We received oral comments on a draft of this report from GSA's Associate Administrator, Office of Governmentwide Policy, and from officials of OMB's Office of Information and Regulatory Affairs and its Office of General Counsel. Both GSA and OMB generally agreed with the content and conclusions in the draft report. Technical comments provided by OMB have been addressed as appropriate.

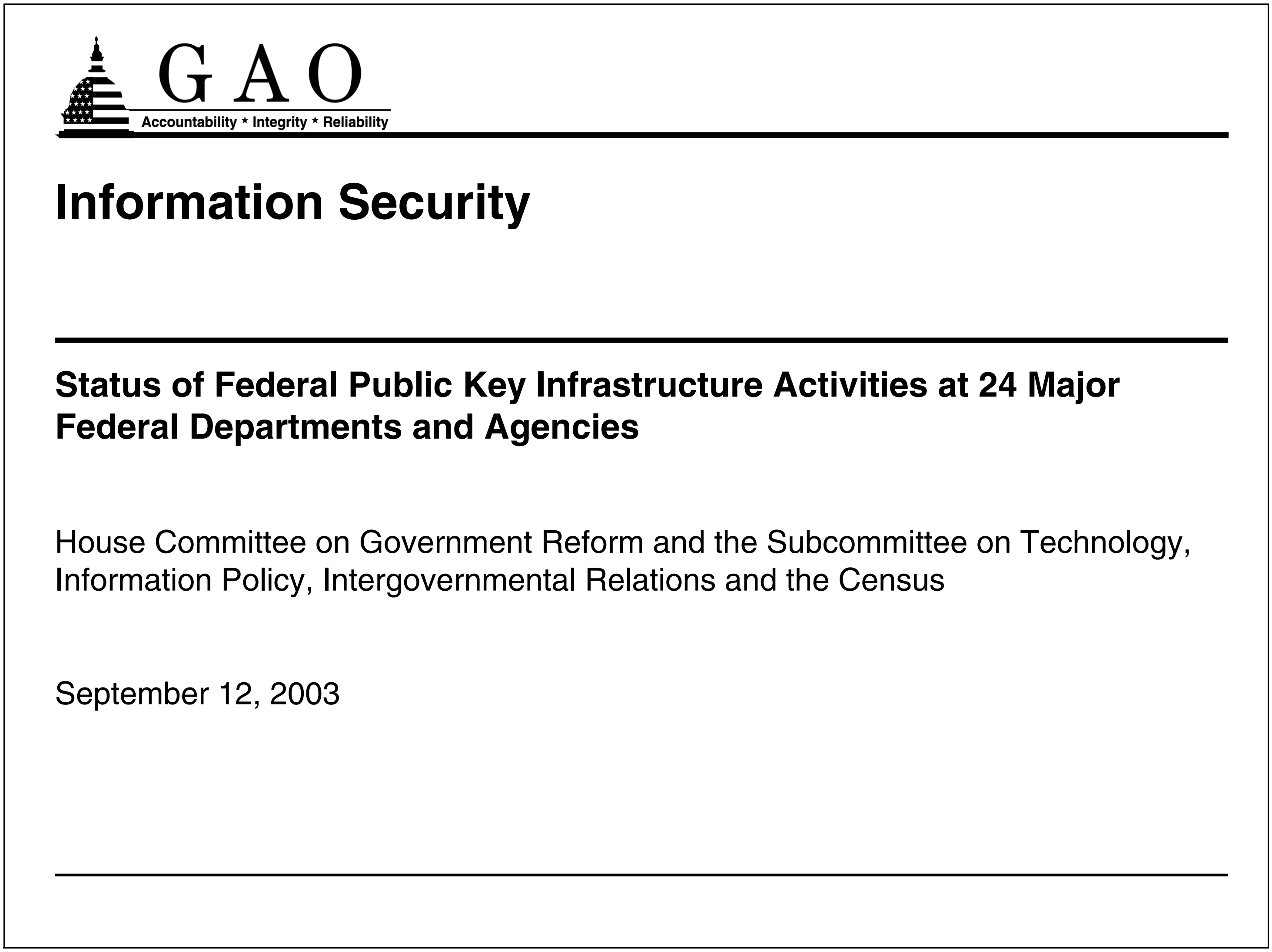
As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this letter. At that time, we will send copies of this report to the Ranking Minority Member, House Committee on Government Reform; the Ranking Minority Member, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform; and other interested congressional committees. We will also send copies to the Director of OMB and the Administrator of GSA. Copies will be made available to others upon request. In addition, this report will be available at no charge on the GAO Web site at www.gao.gov.

If you have any questions concerning this report, please call me at (202) 512-6240 or send e-mail to koontzl@gao.gov. Other major contributors to this report included Theresa Canjar, Barbara Collier, John de Ferrari, Vijay D'Souza, Steven Law, and Yvonne Vigil.

Linda D Koontz

Linda D. Koontz
Director, Information Management Issues

Status of Federal Public Key Infrastructure Activities at 24 Major Federal Departments and Agencies



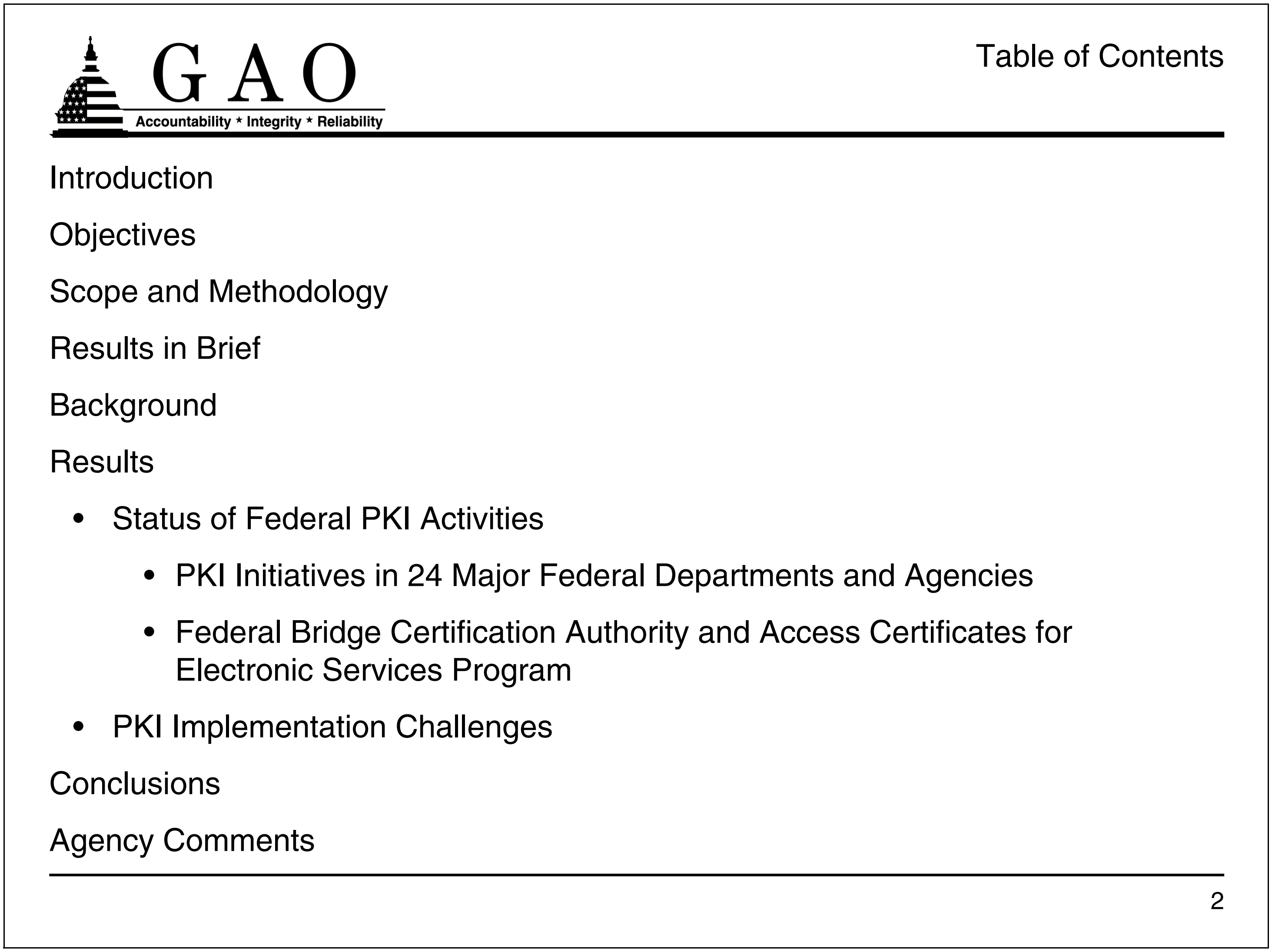
GAO Accountability * Integrity * Reliability

Information Security

Status of Federal Public Key Infrastructure Activities at 24 Major Federal Departments and Agencies

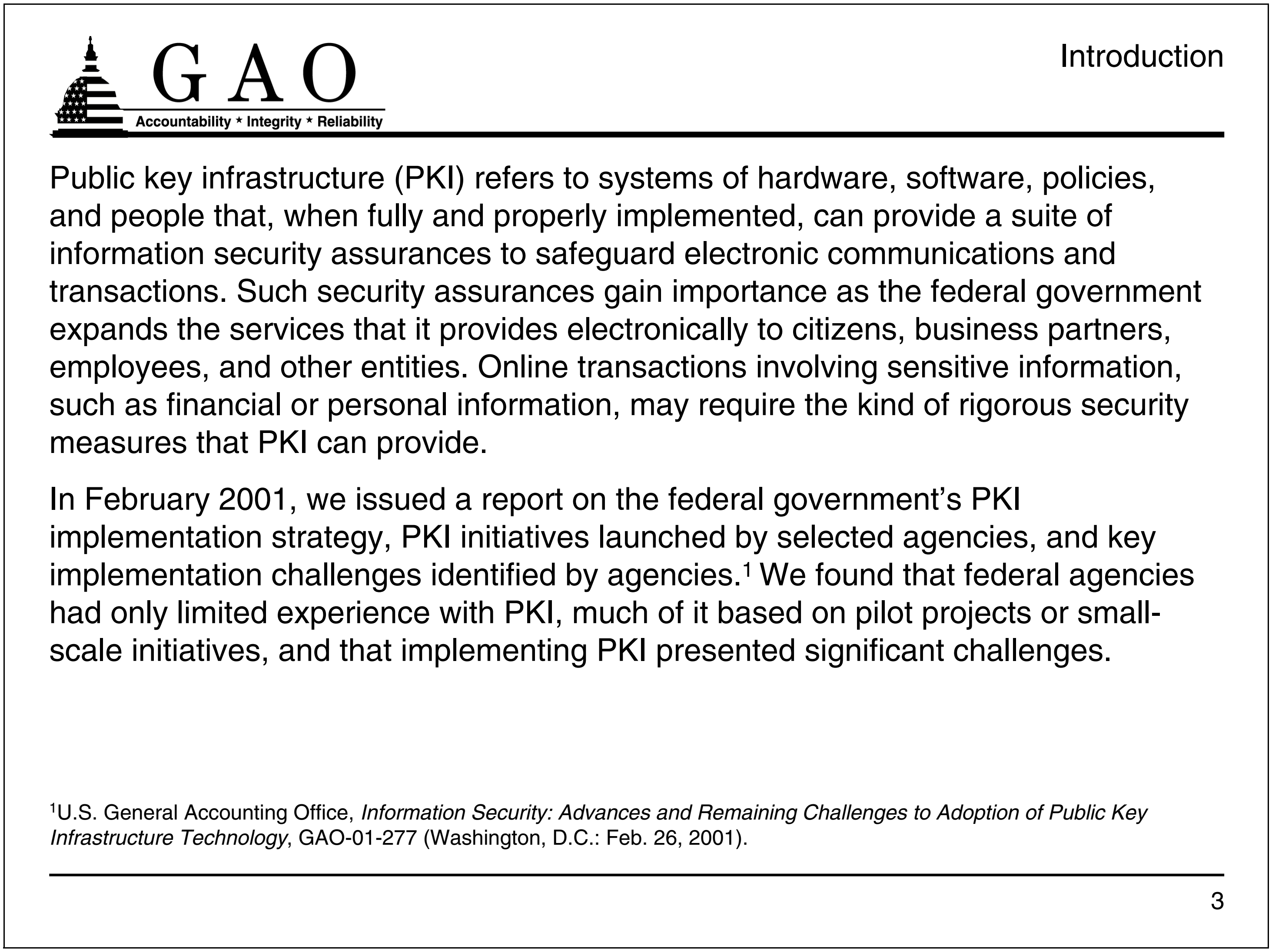
House Committee on Government Reform and the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

September 12, 2003



GAO
Accountability * Integrity * Reliability

Table of Contents



Introduction

Public key infrastructure (PKI) refers to systems of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances to safeguard electronic communications and transactions. Such security assurances gain importance as the federal government expands the services that it provides electronically to citizens, business partners, employees, and other entities. Online transactions involving sensitive information, such as financial or personal information, may require the kind of rigorous security measures that PKI can provide.

In February 2001, we issued a report on the federal government's PKI implementation strategy, PKI initiatives launched by selected agencies, and key implementation challenges identified by agencies.[1] We found that federal agencies had only limited experience with PKI, much of it based on pilot projects or small-scale initiatives, and that implementing PKI presented significant challenges.

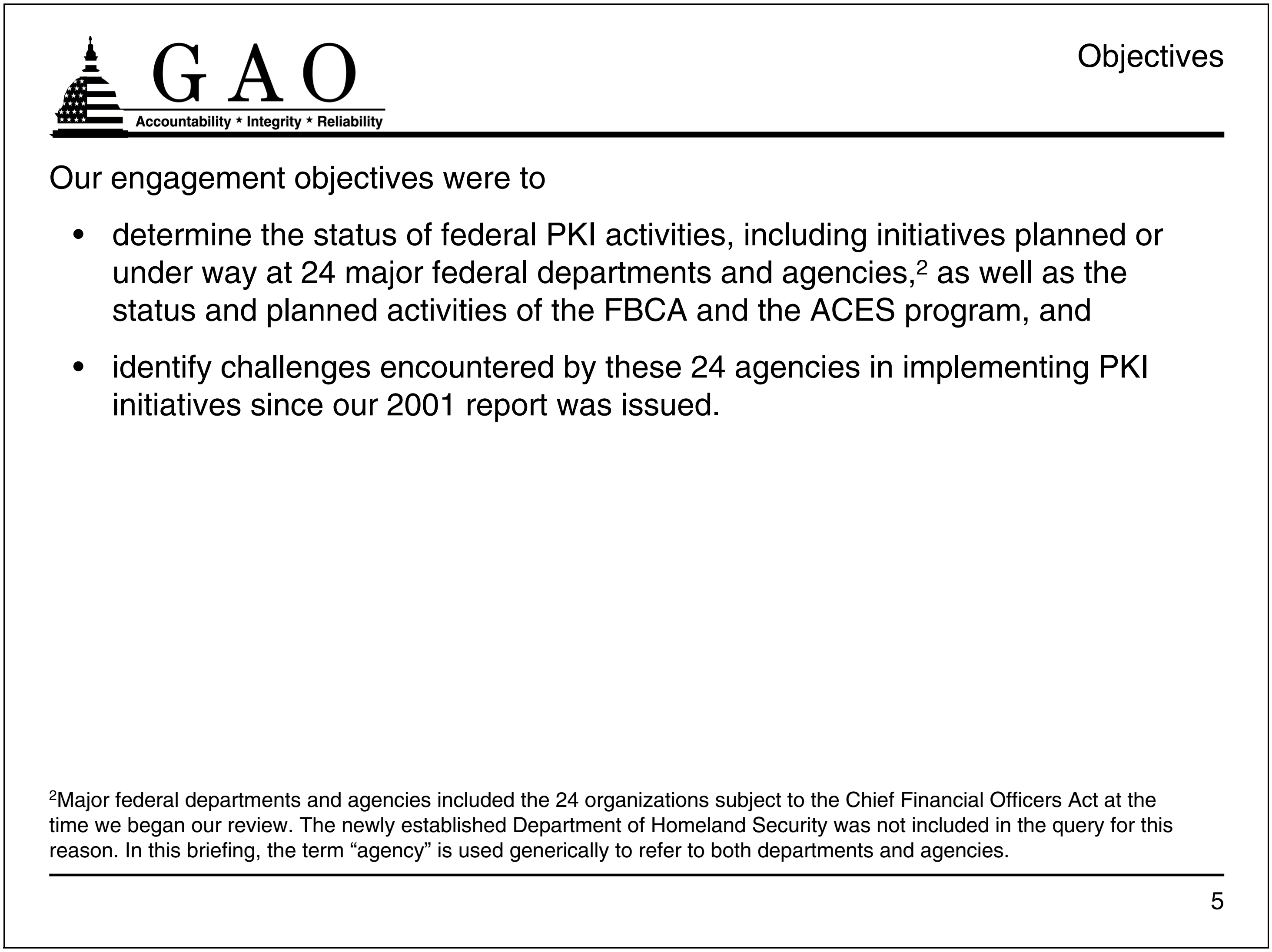
[1] U.S. General Accounting Office, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: Feb. 26, 2001).

GAO
Accountability * Integrity * Reliability

Introduction

Many federal agencies are now pursuing PKI initiatives, and two organizations have established major governmentwide initiatives to promote PKI technology:

- The Federal PKI Steering Committee established the Federal Bridge Certification Authority (FBCA) to connect agency PKIs in support of a broader, governmentwide PKI network.
- The General Services Administration (GSA) developed its Access Certificates for Electronic Services (ACES) program to assist agencies in procuring PKI technology and services and to facilitate adoption of the technology for government transactions made directly with the public.

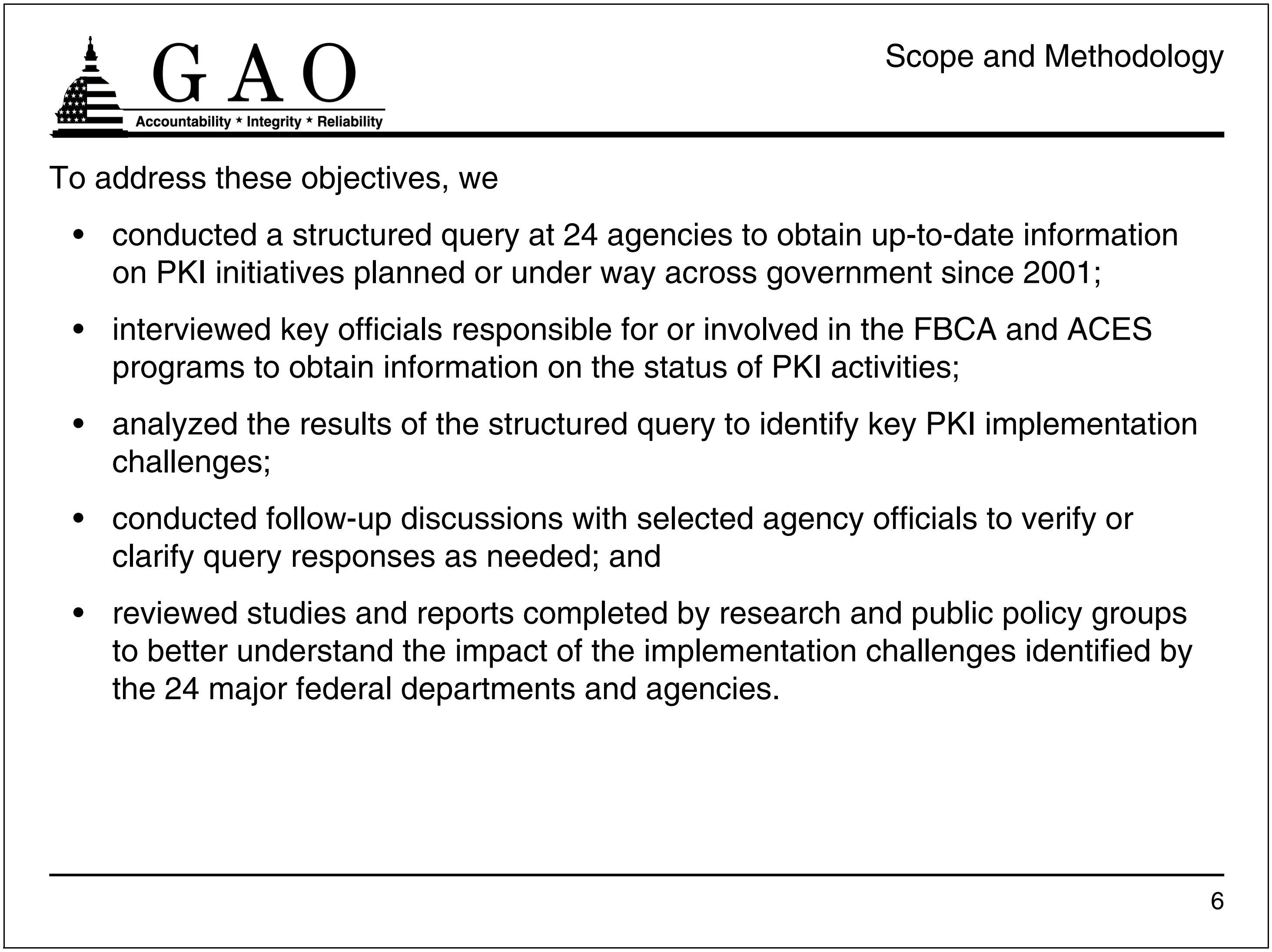


Objectives

Our engagement objectives were to

- determine the status of federal PKI activities, including initiatives planned or under way at 24 major federal departments and agencies,[2] as well as the status and planned activities of the FBCA and the ACES program, and
- identify challenges encountered by these 24 agencies in implementing PKI initiatives since our 2001 report was issued.

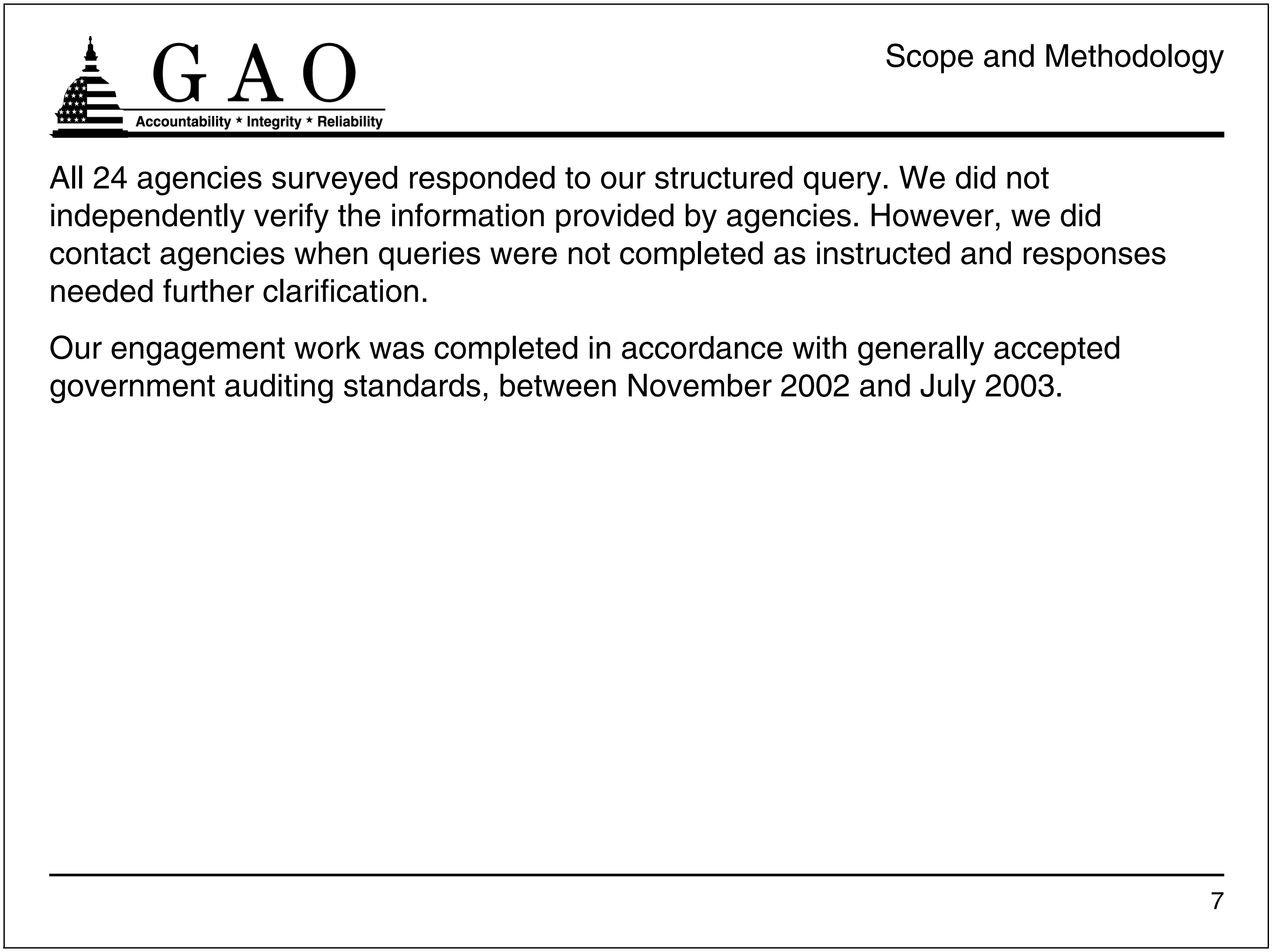
[2] Major federal departments and agencies included the 24 organizations subject to the Chief Financial Officers Act at the time we began our review. The newly established Department of Homeland Security was not included in the query for this reason. In this briefing, the term "agency" is used generically to refer to both departments and agencies.



Scope and Methodology

To address these objectives, we

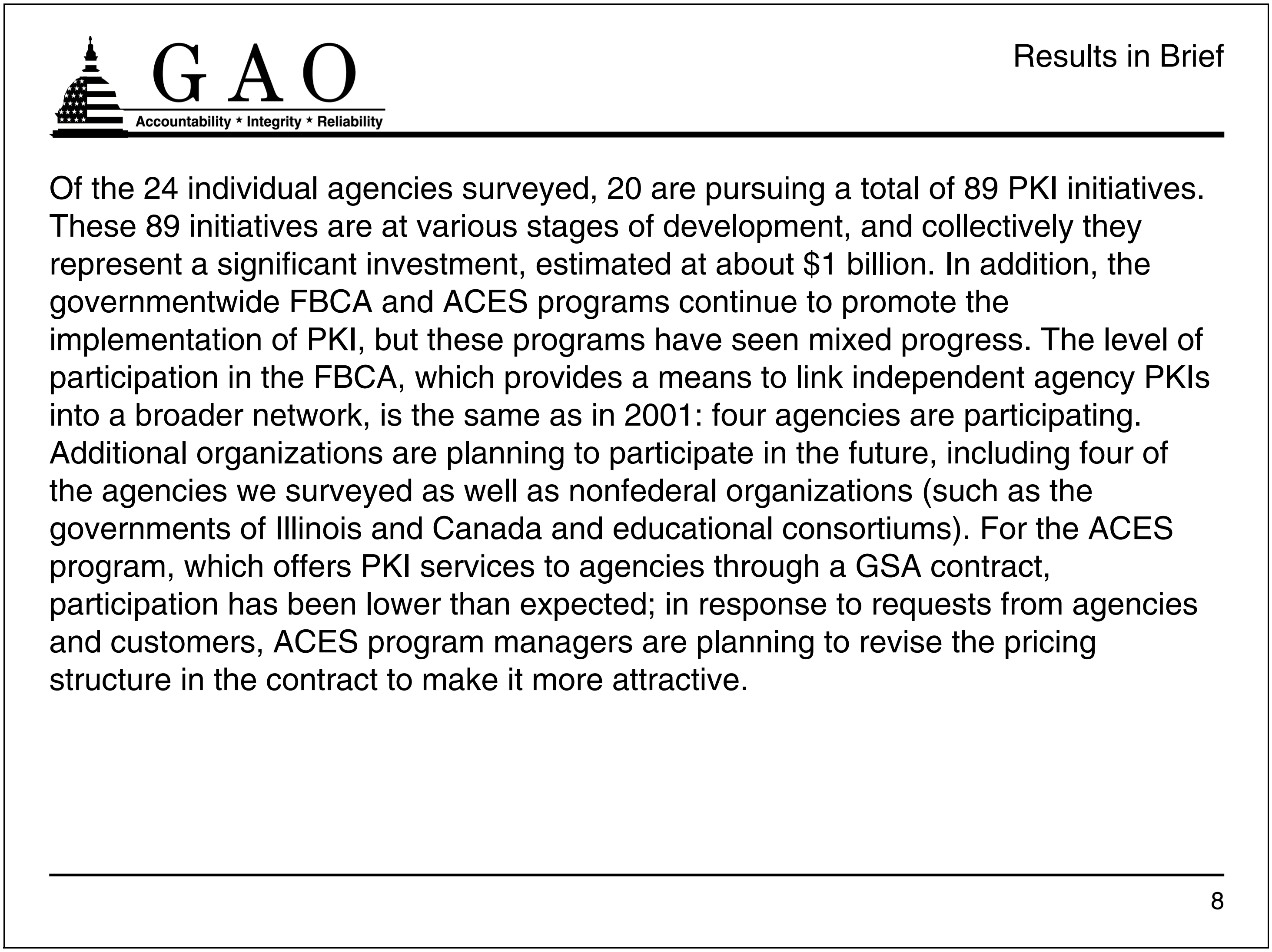
- conducted a structured query at 24 agencies to obtain up-to-date information on PKI initiatives planned or under way across government since 2001;
- interviewed key officials responsible for or involved in the FBCA and ACES programs to obtain information on the status of PKI activities;
- analyzed the results of the structured query to identify key PKI implementation challenges;
- conducted follow-up discussions with selected agency officials to verify or clarify query responses as needed; and
- reviewed studies and reports completed by research and public policy groups to better understand the impact of the implementation challenges identified by the 24 major federal departments and agencies.



Scope and Methodology

All 24 agencies surveyed responded to our structured query. We did not independently verify the information provided by agencies. However, we did contact agencies when queries were not completed as instructed and responses needed further clarification.

Our engagement work was completed in accordance with generally accepted government auditing standards, between November 2002 and July 2003.

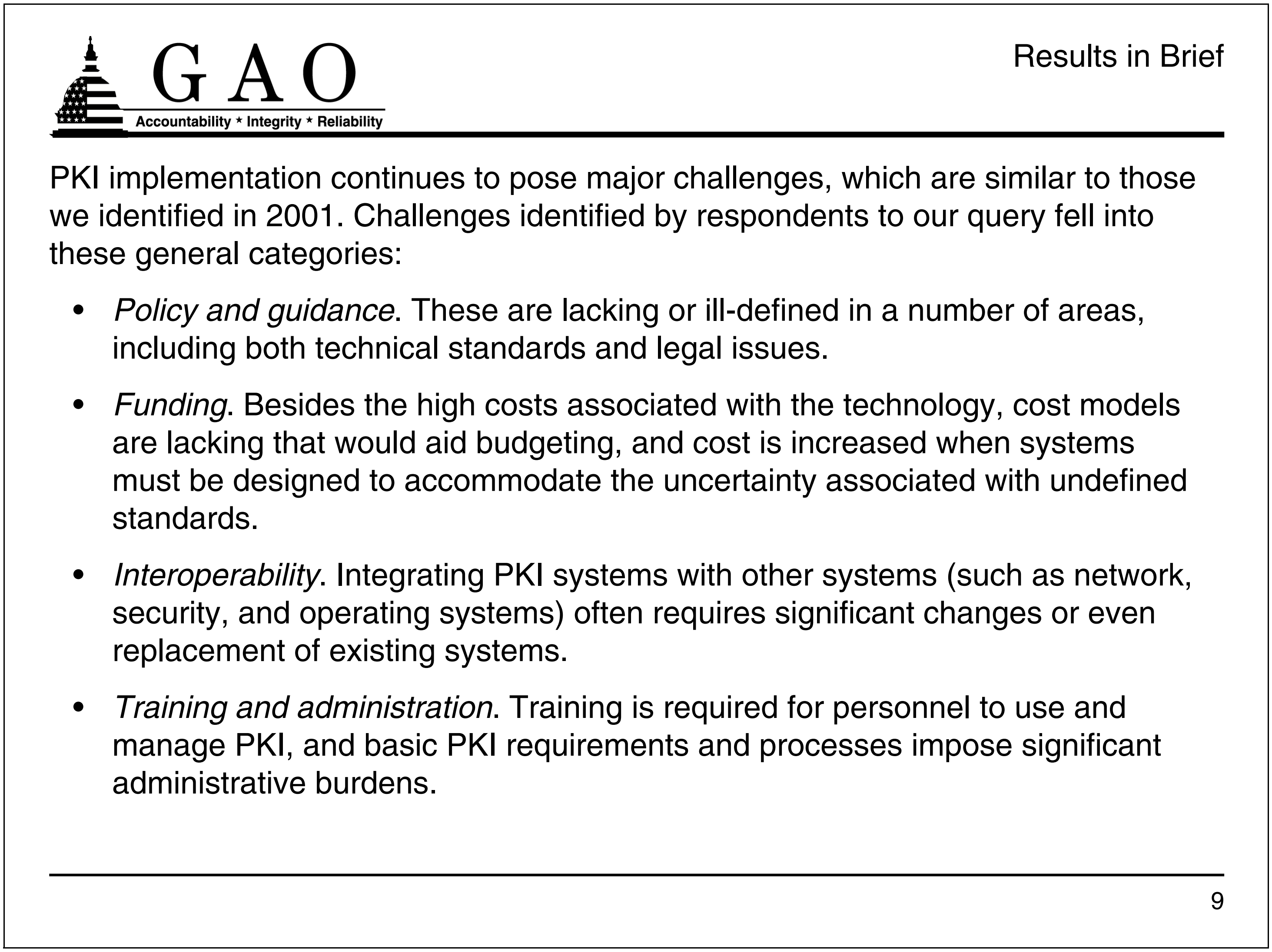


GAO
Accountability * Integrity * Reliability

Results in Brief

Of the 24 individual agencies surveyed, 20 are pursuing a total of 89 PKI initiatives. These 89 initiatives are at various stages of development, and collectively they represent a significant investment, estimated at about $1 billion. In addition, the governmentwide FBCA and ACES programs continue to promote the implementation of PKI, but these programs have seen mixed progress. The level of participation in the FBCA, which provides a means to link independent agency PKIs into a broader network, is the same as in 2001: four agencies are participating. Additional organizations are planning to participate in the future, including four of the agencies we surveyed as well as nonfederal organizations (such as the governments of Illinois and Canada and educational consortiums). For the ACES program, which offers PKI services to agencies through a GSA contract, participation has been lower than expected; in response to requests from agencies and customers, ACES program managers are planning to revise the pricing structure in the contract to make it more attractive.

8

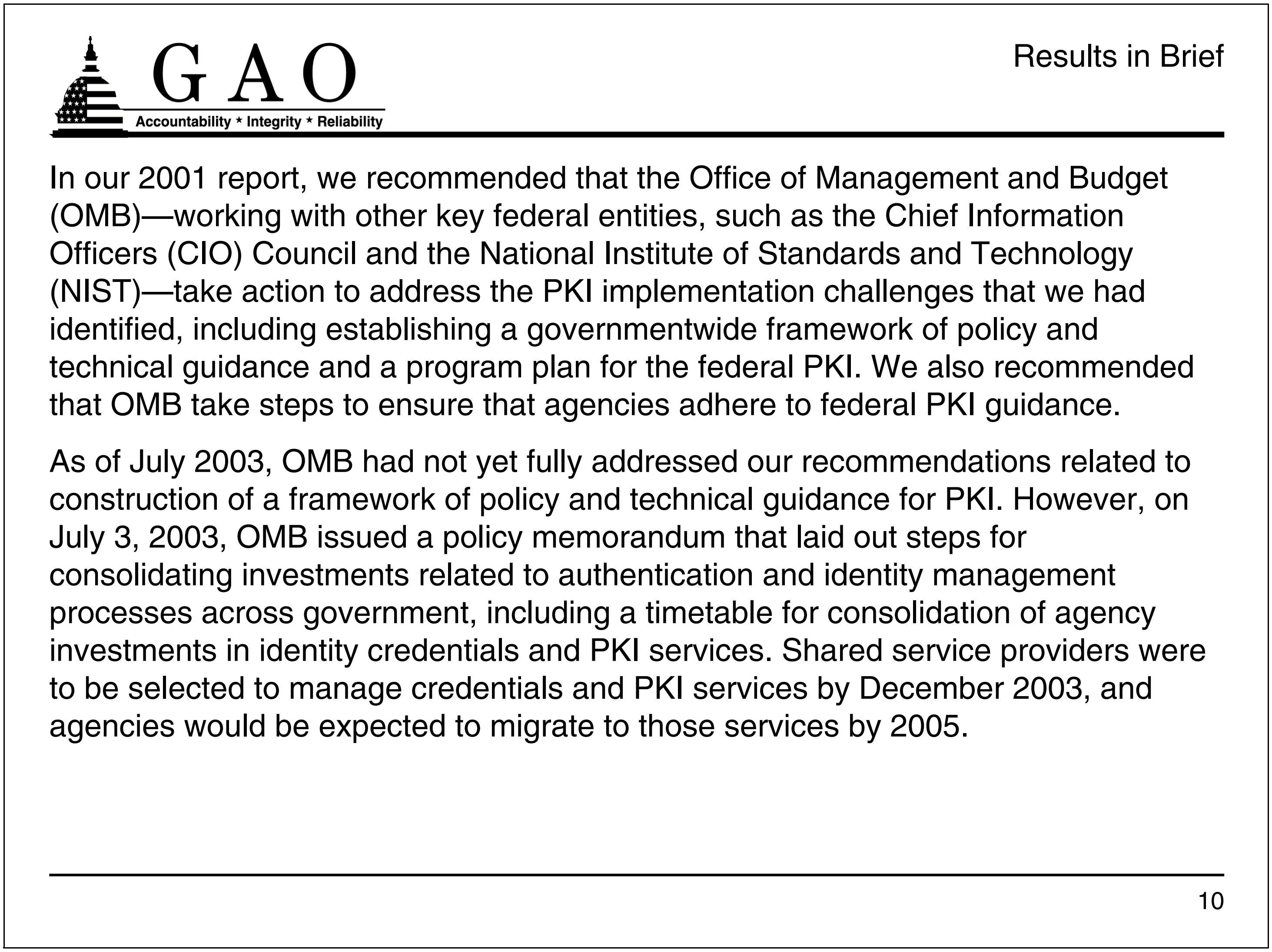


Results in Brief

PKI implementation continues to pose major challenges, which are similar to those we identified in 2001. Challenges identified by respondents to our query fell into these general categories:

- *Policy and guidance*. These are lacking or ill-defined in a number of areas, including both technical standards and legal issues.
- *Funding*. Besides the high costs associated with the technology, cost models are lacking that would aid budgeting, and cost is increased when systems must be designed to accommodate the uncertainty associated with undefined standards.
- *Interoperability*. Integrating PKI systems with other systems (such as network, security, and operating systems) often requires significant changes or even replacement of existing systems.
- *Training and administration*. Training is required for personnel to use and manage PKI, and basic PKI requirements and processes impose significant administrative burdens.

9

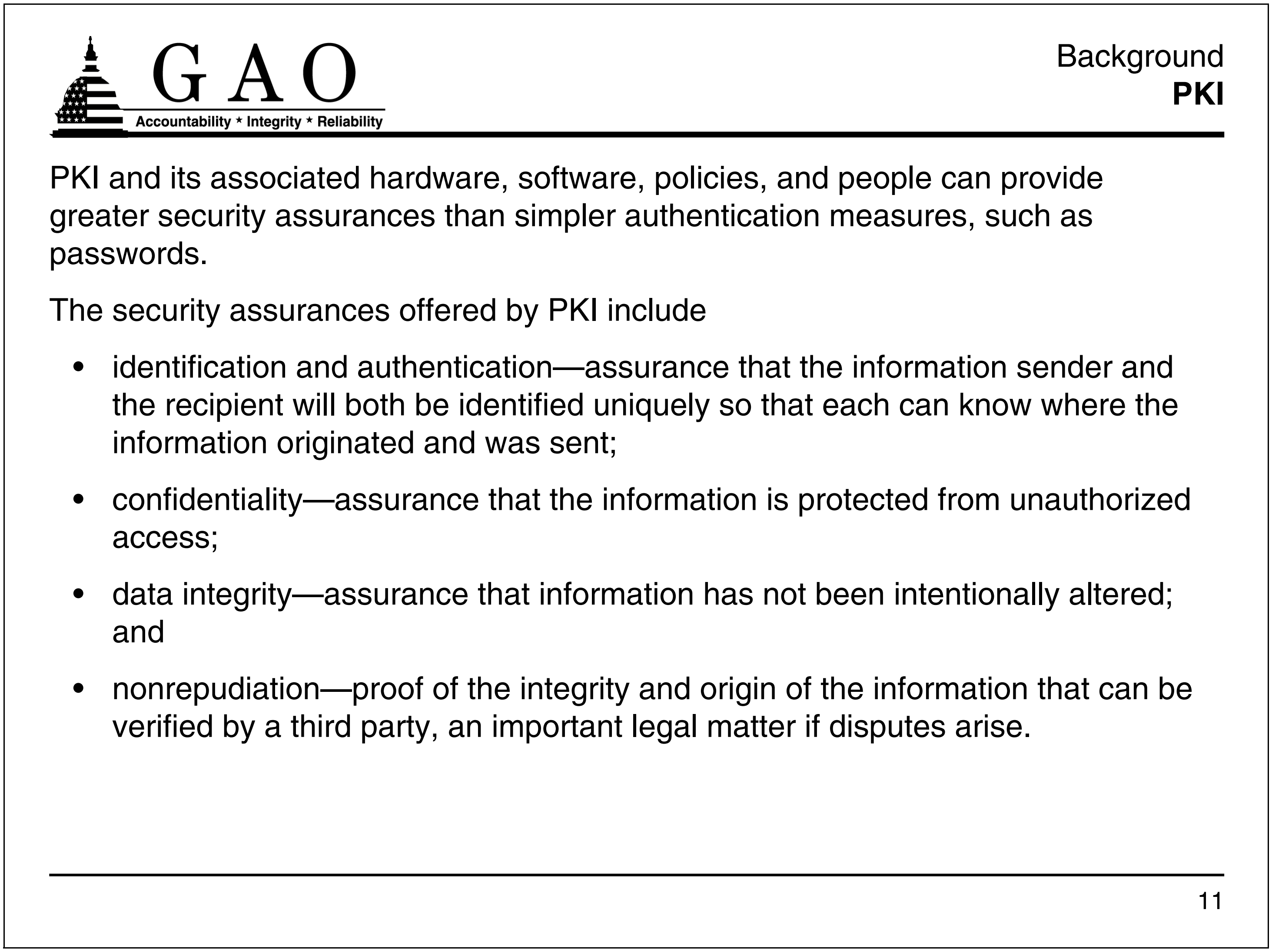


GAO
Accountability * Integrity * Reliability

Results in Brief

In our 2001 report, we recommended that the Office of Management and Budget (OMB)—working with other key federal entities, such as the Chief Information Officers (CIO) Council and the National Institute of Standards and Technology (NIST)—take action to address the PKI implementation challenges that we had identified, including establishing a governmentwide framework of policy and technical guidance and a program plan for the federal PKI. We also recommended that OMB take steps to ensure that agencies adhere to federal PKI guidance.

As of July 2003, OMB had not yet fully addressed our recommendations related to construction of a framework of policy and technical guidance for PKI. However, on July 3, 2003, OMB issued a policy memorandum that laid out steps for consolidating investments related to authentication and identity management processes across government, including a timetable for consolidation of agency investments in identity credentials and PKI services. Shared service providers were to be selected to manage credentials and PKI services by December 2003, and agencies would be expected to migrate to those services by 2005.



Background
PKI

PKI and its associated hardware, software, policies, and people can provide greater security assurances than simpler authentication measures, such as passwords.

The security assurances offered by PKI include

- identification and authentication—assurance that the information sender and the recipient will both be identified uniquely so that each can know where the information originated and was sent;
- confidentiality—assurance that the information is protected from unauthorized access;
- data integrity—assurance that information has not been intentionally altered; and
- nonrepudiation—proof of the integrity and origin of the information that can be verified by a third party, an important legal matter if disputes arise.

GAO
Accountability * Integrity * Reliability

Background
PKI

PKI systems are based on encryption that requires each user to have two different keys: a *public key* and a *private key*. Public keys are easily accessible and enable information to be encrypted. However, only the owner of the associated private key can decrypt the information. Both public and private keys may be generated on a hardware token—such as a smart card—or on a user's computer, as well as provided to the user by a third party.[3]

A *digital certificate* is an electronic credential that guarantees the association between a public key and an individual or specific entity (such as a server). These certificates, which consist of a person or entity's name, public key, and certain other identifying information, are stored in a *directory* or other database. Directories may be publicly available repositories kept on servers that act like telephone books for users to look up others' public keys.

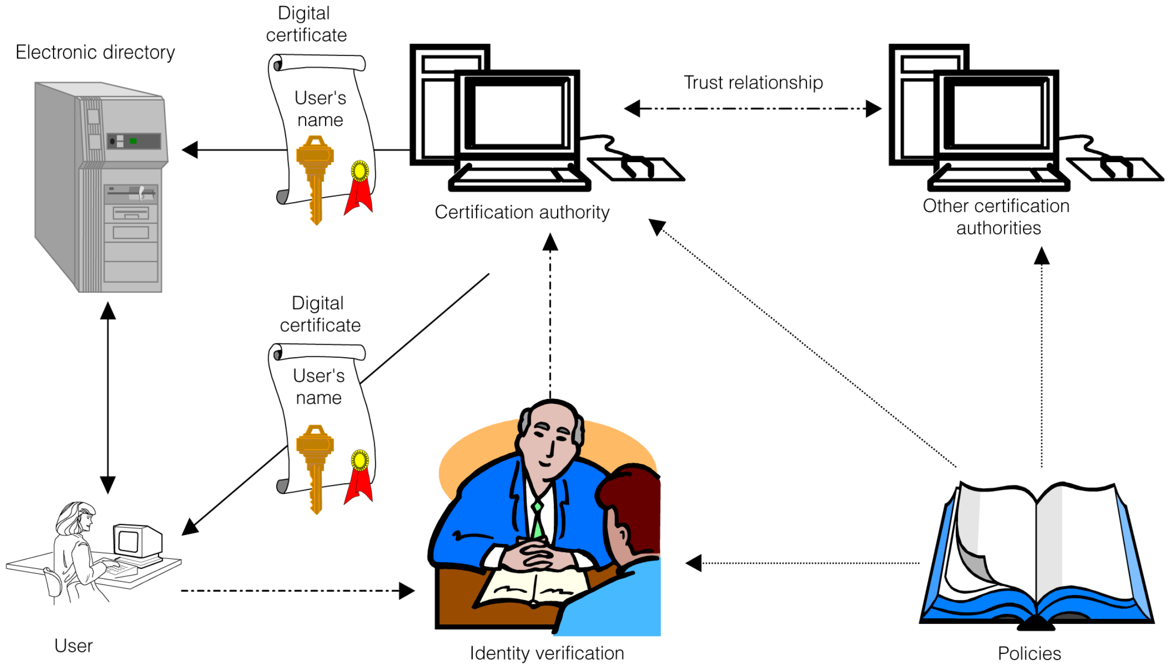
Digital certificates are created by a trusted third party called a *certification authority*, which digitally signs the certificate, thus providing assurance that the public key contained in the certificate does indeed belong to the individual named in the certificate. A certification authority is responsible for managing digital certificates.

[3] For more information on smart cards, see U.S. General Accounting Office, *Electronic Government: Progress In Promoting Adoption of Smart Card Technology*, GAO-03-144 (Washington, D.C.: Jan. 3, 2003).

GAO
Accountability * Integrity * Reliability

Background
PKI

The following figure depicts how PKI technology can be applied to authenticate individual users involved in on-line communications or transactions.



Source: GAO.

13

GAO
Accountability * Integrity * Reliability

Background
Governmentwide Efforts

Federal Bridge Certification Authority (FBCA). Because a number of federal PKI initiatives were established independently, each of which had developed certification authorities, the Federal PKI Steering Committee—a committee of the federal CIO Council—determined that a mechanism was required to link individual PKIs into a single federal structure. The mechanism chosen was a certification authority that would act as a bridge among the disparate agency PKIs. In operation since 2001, the FBCA was designed to be able to accommodate both federal and nonfederal certification authorities, including state and local government agencies and the private sector.

GAO
Accountability * Integrity * Reliability

Background
Governmentwide Efforts

The Federal PKI Steering Committee also established the Federal PKI Policy Authority to facilitate agency participation in the FBCA project and to address policy-related issues associated with PKI implementation. The Policy Authority is also responsible for overseeing and coordinating agency involvement with the bridge authority and for correlating and reconciling the varying trust levels that agencies have for their different PKI initiatives with FBCA standards. This includes reconciling differences in polices related to the generation, distribution, renewal, revocation, and suspension of digital certificates.

Since June 2000, the Federal PKI Policy Authority has conducted monthly meetings with federal agencies and other stakeholders to establish by-laws, procedures, and guidelines for the FBCA. For example, the Policy Authority established the certificate policy for the FBCA—which defines five different assurance levels for certificates—in 2002. Other educational materials also have been developed for organizations interested in the FBCA.

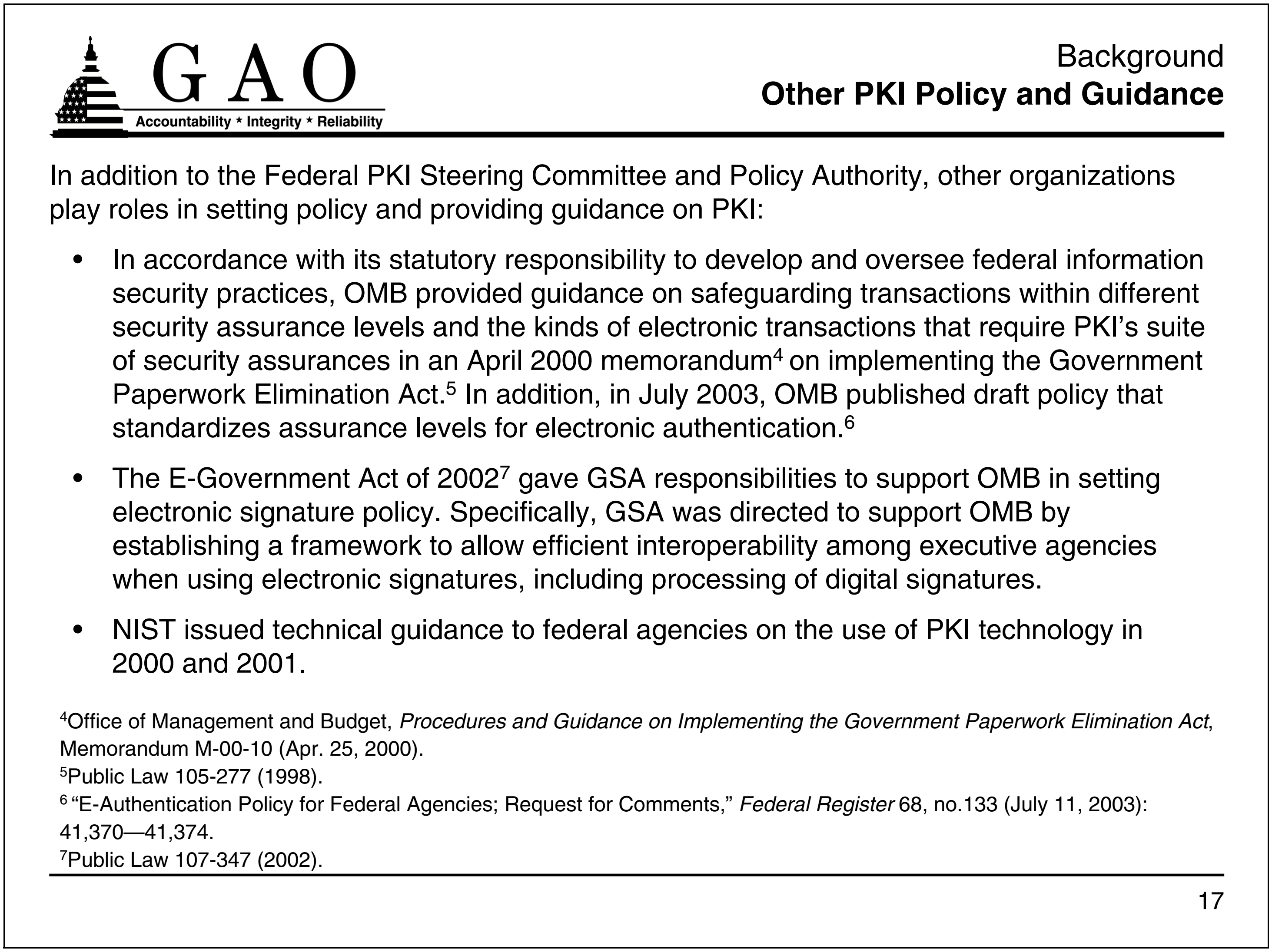
GAO
Accountability * Integrity * Reliability

Background
Governmentwide Efforts

Access Certificates for Electronic Services (ACES). GSA established its ACES program to provide a standardized contracting vehicle that federal agencies could use to obtain various PKI elements “off the shelf” from commercial vendors. A primary function of the program is to make certificates available for agencies to issue to individual citizens who wish to access and submit sensitive information. As originally designed, contract providers would charge participating agencies an issuance fee for each certificate as well as a transaction fee each time a certificate was used. In order to jump-start the use of ACES certificates, GSA arranged with its contractors to waive the issuance fee for the first 500,000 certificates issued beginning in June 2000.

In 2001, we reported that the ACES program was being used only to a limited extent: two agencies—the Federal Emergency Management Agency and the Social Security Administration—had taken advantage of the services offered by GSA’s three contract vendors.

16

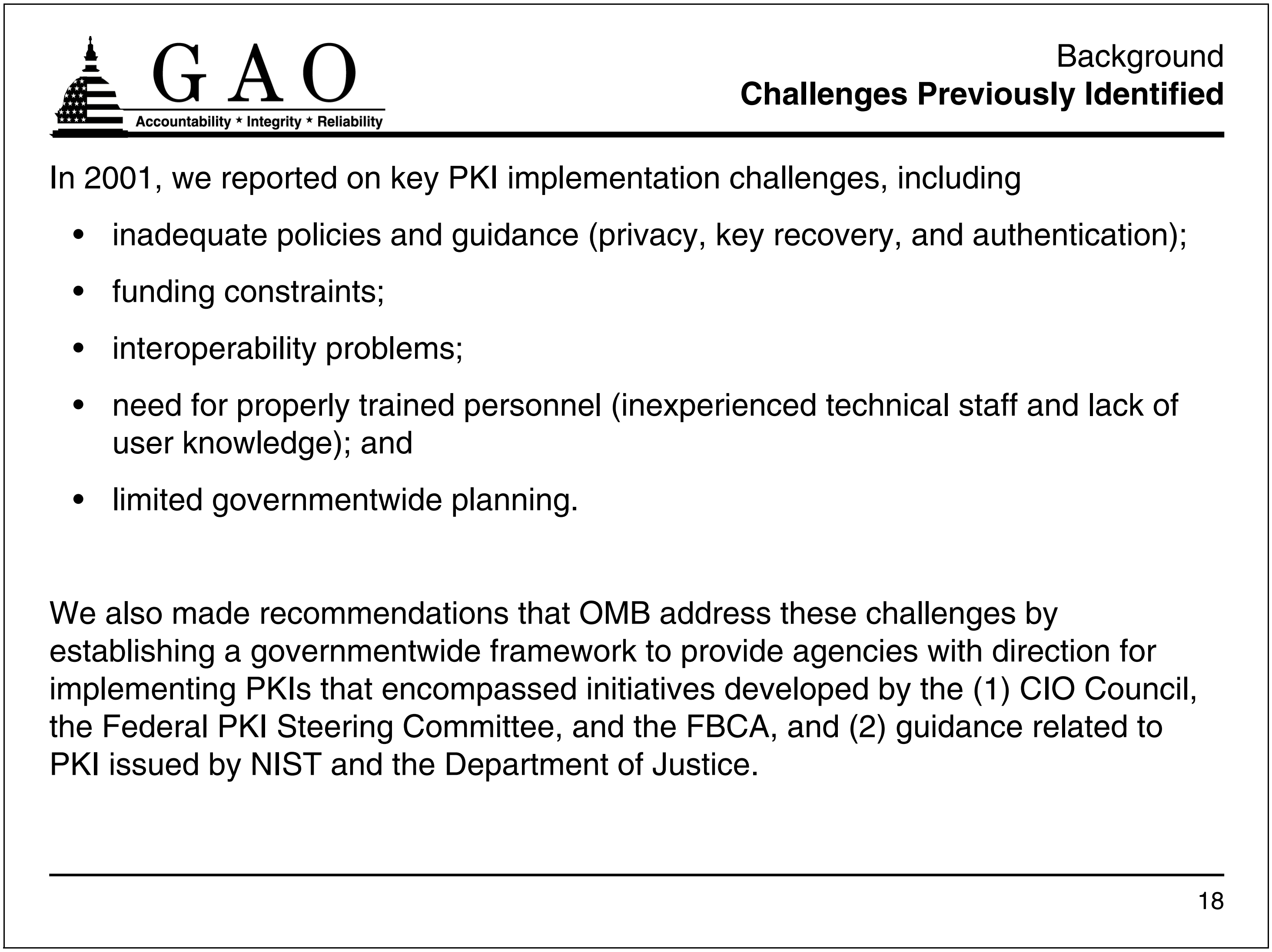


Background
Other PKI Policy and Guidance

In addition to the Federal PKI Steering Committee and Policy Authority, other organizations play roles in setting policy and providing guidance on PKI:

- In accordance with its statutory responsibility to develop and oversee federal information security practices, OMB provided guidance on safeguarding transactions within different security assurance levels and the kinds of electronic transactions that require PKI's suite of security assurances in an April 2000 memorandum[4] on implementing the Government Paperwork Elimination Act.[5] In addition, in July 2003, OMB published draft policy that standardizes assurance levels for electronic authentication.[6]
- The E-Government Act of 2002[7] gave GSA responsibilities to support OMB in setting electronic signature policy. Specifically, GSA was directed to support OMB by establishing a framework to allow efficient interoperability among executive agencies when using electronic signatures, including processing of digital signatures.
- NIST issued technical guidance to federal agencies on the use of PKI technology in 2000 and 2001.

[4] Office of Management and Budget, *Procedures and Guidance on Implementing the Government Paperwork Elimination Act*, Memorandum M-00-10 (Apr. 25, 2000).
[5] Public Law 105-277 (1998).
[6] "E-Authentication Policy for Federal Agencies; Request for Comments," *Federal Register* 68, no.133 (July 11, 2003): 41,370—41,374.
[7] Public Law 107-347 (2002).



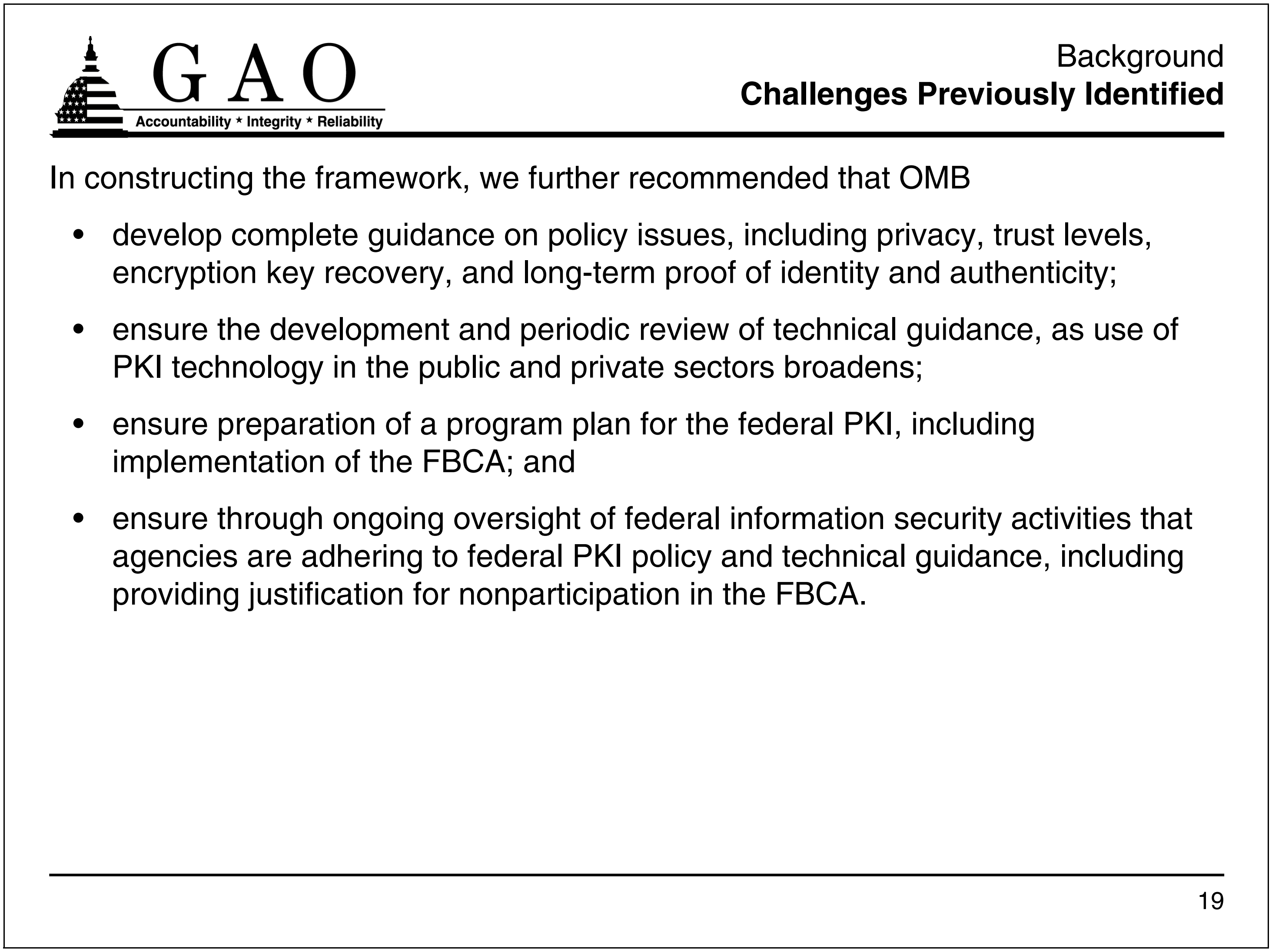
GAO
Accountability * Integrity * Reliability

Background
Challenges Previously Identified

In 2001, we reported on key PKI implementation challenges, including

- inadequate policies and guidance (privacy, key recovery, and authentication);
- funding constraints;
- interoperability problems;
- need for properly trained personnel (inexperienced technical staff and lack of user knowledge); and
- limited governmentwide planning.

We also made recommendations that OMB address these challenges by establishing a governmentwide framework to provide agencies with direction for implementing PKIs that encompassed initiatives developed by the (1) CIO Council, the Federal PKI Steering Committee, and the FBCA, and (2) guidance related to PKI issued by NIST and the Department of Justice.

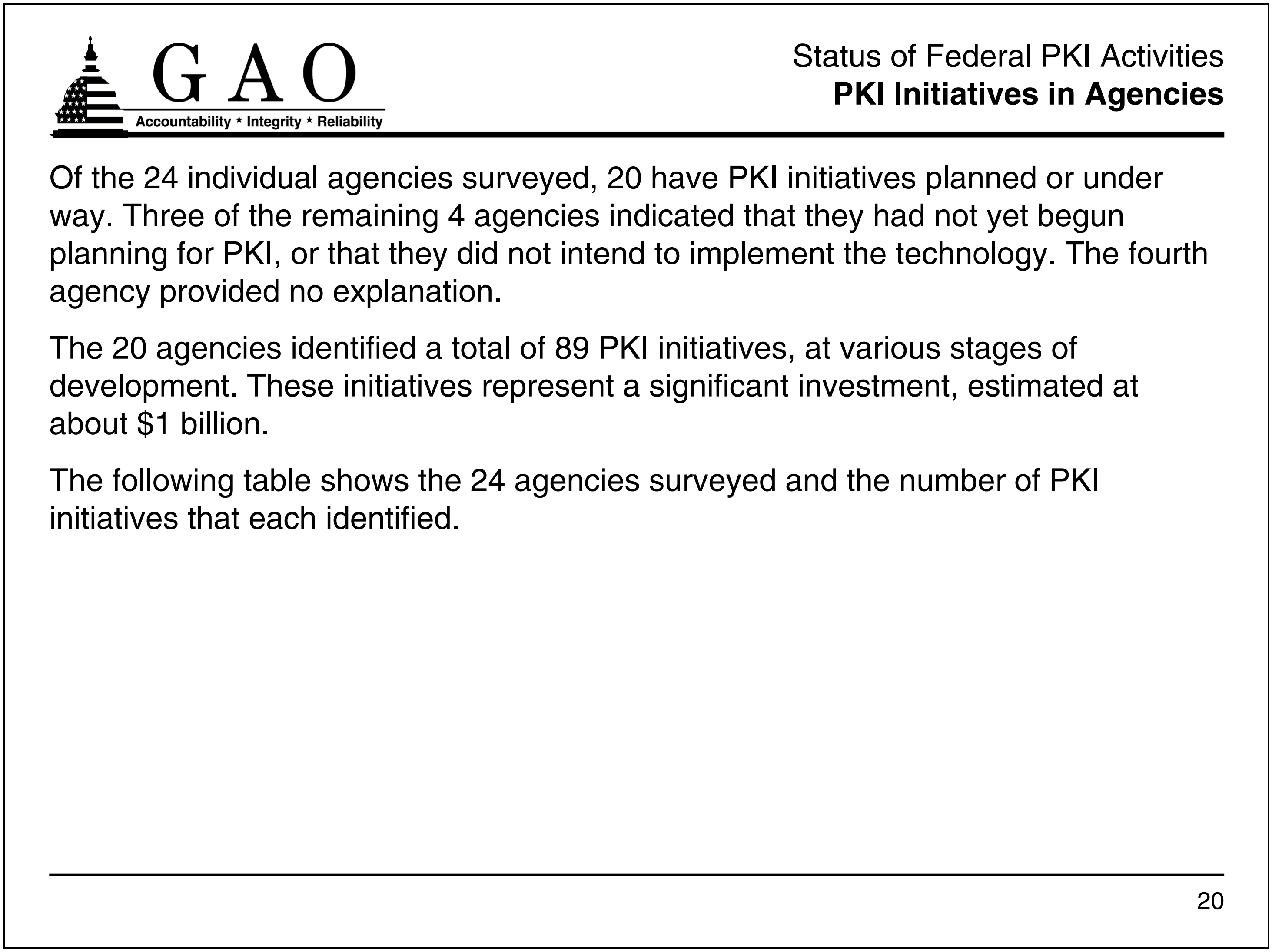


GAO
Accountability * Integrity * Reliability

Background
Challenges Previously Identified

In constructing the framework, we further recommended that OMB

- develop complete guidance on policy issues, including privacy, trust levels, encryption key recovery, and long-term proof of identity and authenticity;
- ensure the development and periodic review of technical guidance, as use of PKI technology in the public and private sectors broadens;
- ensure preparation of a program plan for the federal PKI, including implementation of the FBCA; and
- ensure through ongoing oversight of federal information security activities that agencies are adhering to federal PKI policy and technical guidance, including providing justification for nonparticipation in the FBCA.



GAO
Accountability * Integrity * Reliability

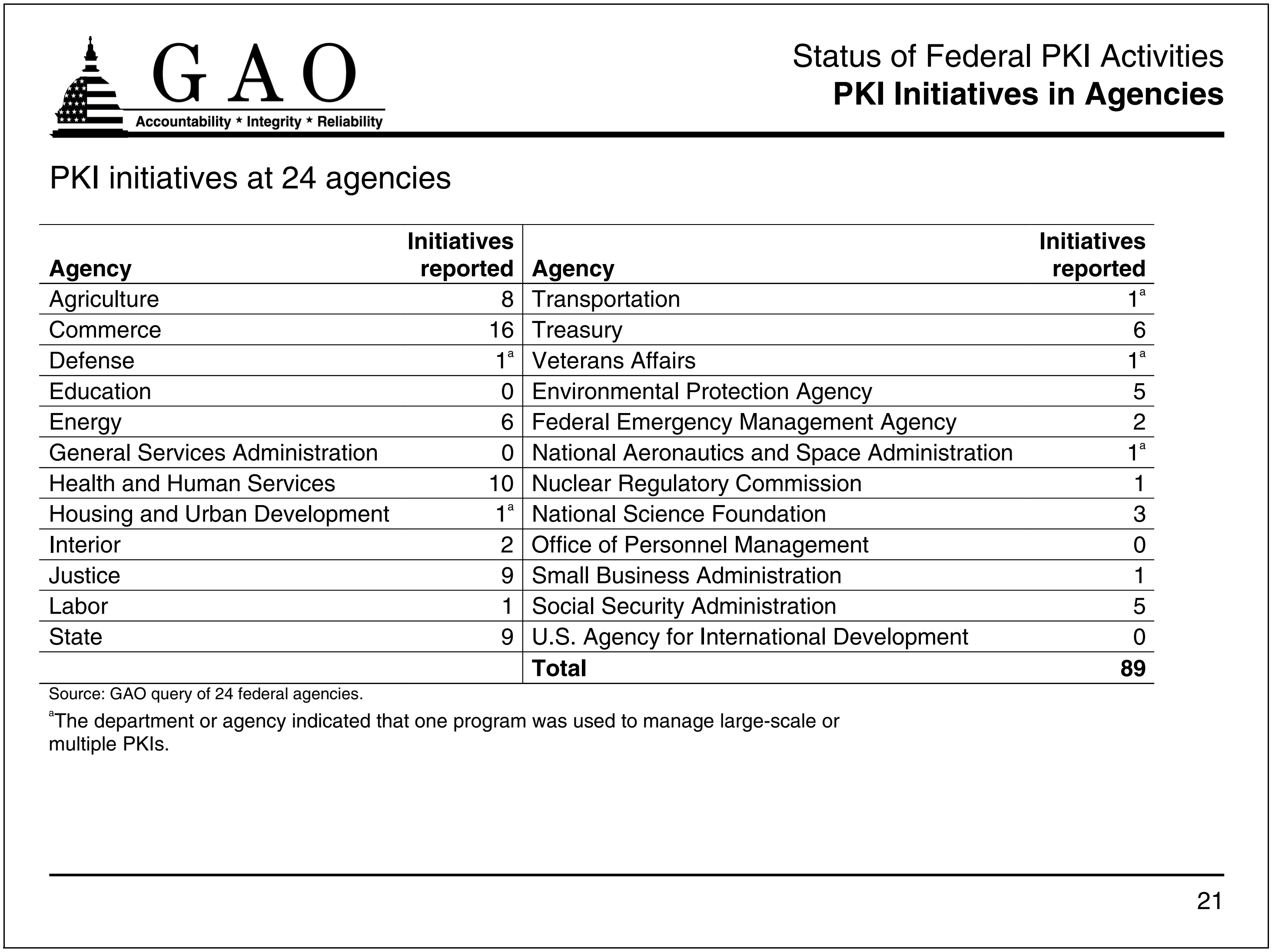
Status of Federal PKI Activities

PKI Initiatives in Agencies

Of the 24 individual agencies surveyed, 20 have PKI initiatives planned or under way. Three of the remaining 4 agencies indicated that they had not yet begun planning for PKI, or that they did not intend to implement the technology. The fourth agency provided no explanation.

The 20 agencies identified a total of 89 PKI initiatives, at various stages of development. These initiatives represent a significant investment, estimated at about $1 billion.

The following table shows the 24 agencies surveyed and the number of PKI initiatives that each identified.



GAO
Accountability * Integrity * Reliability

Status of Federal PKI Activities
PKI Initiatives in Agencies

PKI initiatives at 24 agencies

Agency	**Initiatives reported**	**Agency**	**Initiatives reported**
Agriculture	8	Transportation	1[a]
Commerce	16	Treasury	6
Defense	1[a]	Veterans Affairs	1[a]
Education	0	Environmental Protection Agency	5
Energy	6	Federal Emergency Management Agency	2
General Services Administration	0	National Aeronautics and Space Administration	1[a]
Health and Human Services	10	Nuclear Regulatory Commission	1
Housing and Urban Development	1[a]	National Science Foundation	3
Interior	2	Office of Personnel Management	0
Justice	9	Small Business Administration	1
Labor	1	Social Security Administration	5
State	9	U.S. Agency for International Development	0
		Total	**89**

Source: GAO query of 24 federal agencies.

[a] The department or agency indicated that one program was used to manage large-scale or multiple PKIs.

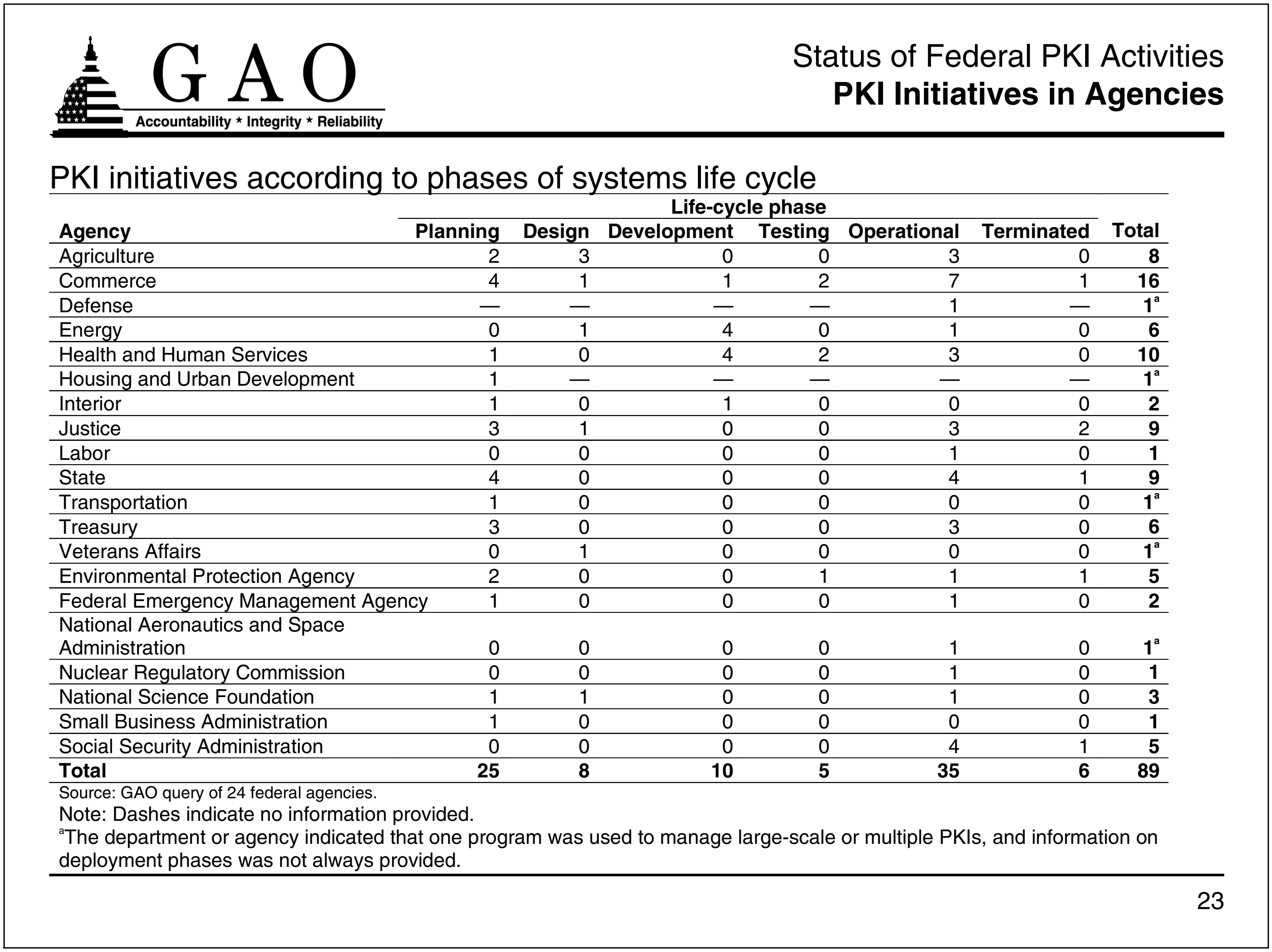
21

Status of Federal PKI Activities
PKI Initiatives in Agencies

The following table categorizes the 89 reported PKI initiatives according to their system development life-cycle phases, which are commonly used by both public and private sector organizations to monitor the progress of technology initiatives. These phases include

- planning,
- design,
- development,
- testing, and
- operations.

Agencies reported ongoing PKI initiatives in each of these phases. Thirty-five (39 percent) were operational. In addition, 6 of the 89 initiatives were reported to have been terminated.



Status of Federal PKI Activities
PKI Initiatives in Agencies

PKI initiatives according to phases of systems life cycle

	Life-cycle phase						
Agency	**Planning**	**Design**	**Development**	**Testing**	**Operational**	**Terminated**	**Total**
Agriculture	2	3	0	0	3	0	**8**
Commerce	4	1	1	2	7	1	**16**
Defense	—	—	—	—	1	—	**1**[a]
Energy	0	1	4	0	1	0	**6**
Health and Human Services	1	0	4	2	3	0	**10**
Housing and Urban Development	1	—	—	—	—	—	**1**[a]
Interior	1	0	1	0	0	0	**2**
Justice	3	1	0	0	3	2	**9**
Labor	0	0	0	0	1	0	**1**
State	4	0	0	0	4	1	**9**
Transportation	1	0	0	0	0	0	**1**[a]
Treasury	3	0	0	0	3	0	**6**
Veterans Affairs	0	1	0	0	0	0	**1**[a]
Environmental Protection Agency	2	0	0	1	1	1	**5**
Federal Emergency Management Agency	1	0	0	0	1	0	**2**
National Aeronautics and Space Administration	0	0	0	0	1	0	**1**[a]
Nuclear Regulatory Commission	0	0	0	0	1	0	**1**
National Science Foundation	1	1	0	0	1	0	**3**
Small Business Administration	1	0	0	0	0	0	**1**
Social Security Administration	0	0	0	0	4	1	**5**
Total	**25**	**8**	**10**	**5**	**35**	**6**	**89**

Source: GAO query of 24 federal agencies.

Note: Dashes indicate no information provided.

[a] The department or agency indicated that one program was used to manage large-scale or multiple PKIs, and information on deployment phases was not always provided.

23

Status of Federal PKI Activities
PKI Initiatives in Agencies

Five agencies reported terminating a total of six PKI initiatives between 1998 and 2002. The six initiatives had progressed to various life-cycle phases before being terminated, and expenditures for them varied. For four of the six projects, an estimated total of about $956,000 was expended. Costs were not reported for the other two projects.

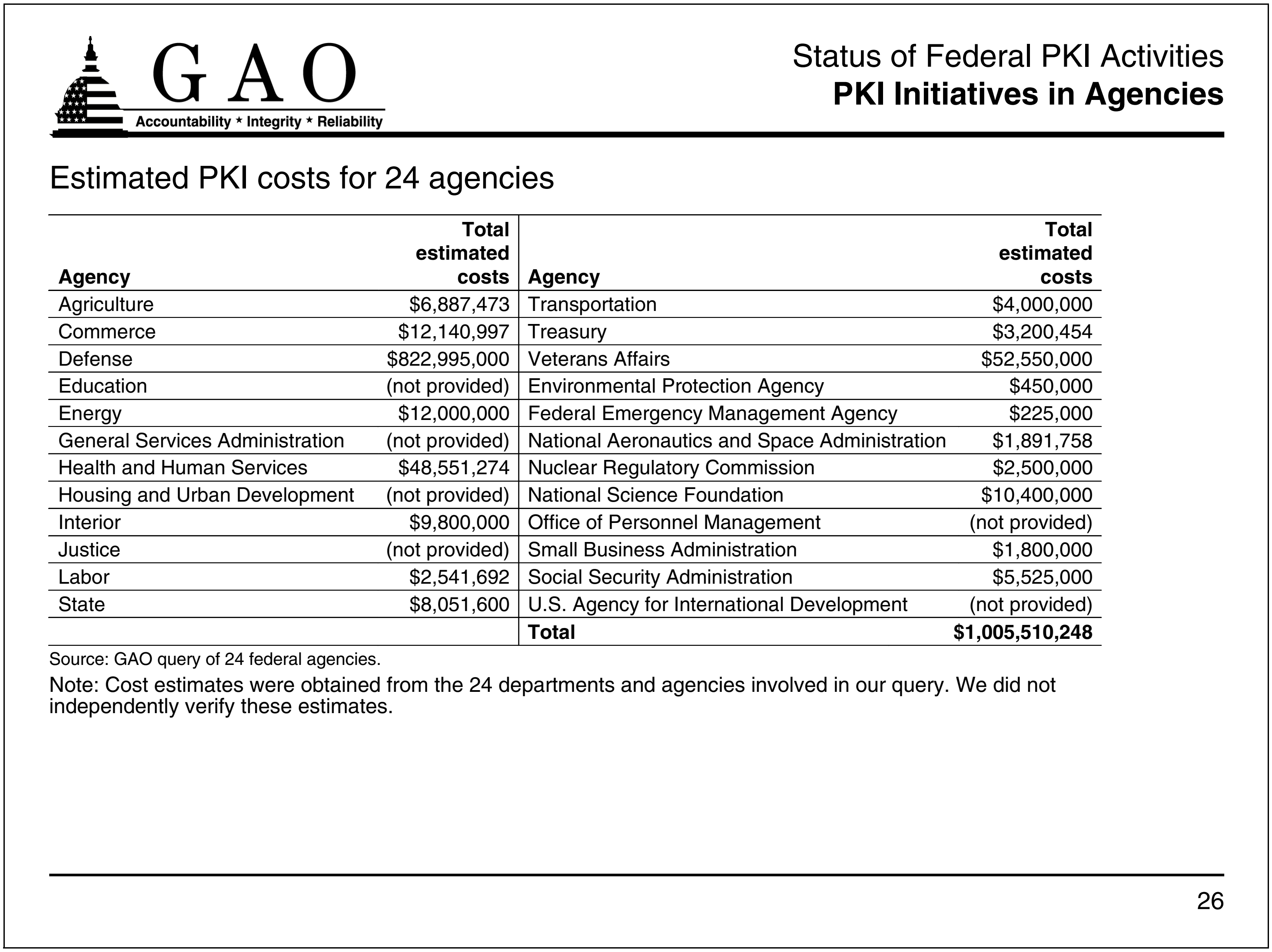
Three agencies reported that they terminated their PKI initiatives because of the lack of funding or the expense of the technology. One agency canceled its project as a result of technical problems. Another agency’s project was a limited pilot study and not expected to go beyond the pilot phase. The remaining project provided no explanation for canceling the initiative.

Status of Federal PKI Activities

PKI Initiatives in Agencies

Investments in the 89 PKI initiatives varied from agency to agency. Some of this variation arises because the initiatives are at varying points in their life cycles, as shown in the previous table.

The following table summarizes department or agency estimates of the total costs associated with the 89 PKI initiatives. These estimates were based on the total costs associated with completing multiple PKIs over various years, and time frames varied among agencies.



GAO
Accountability * Integrity * Reliability

Status of Federal PKI Activities
PKI Initiatives in Agencies

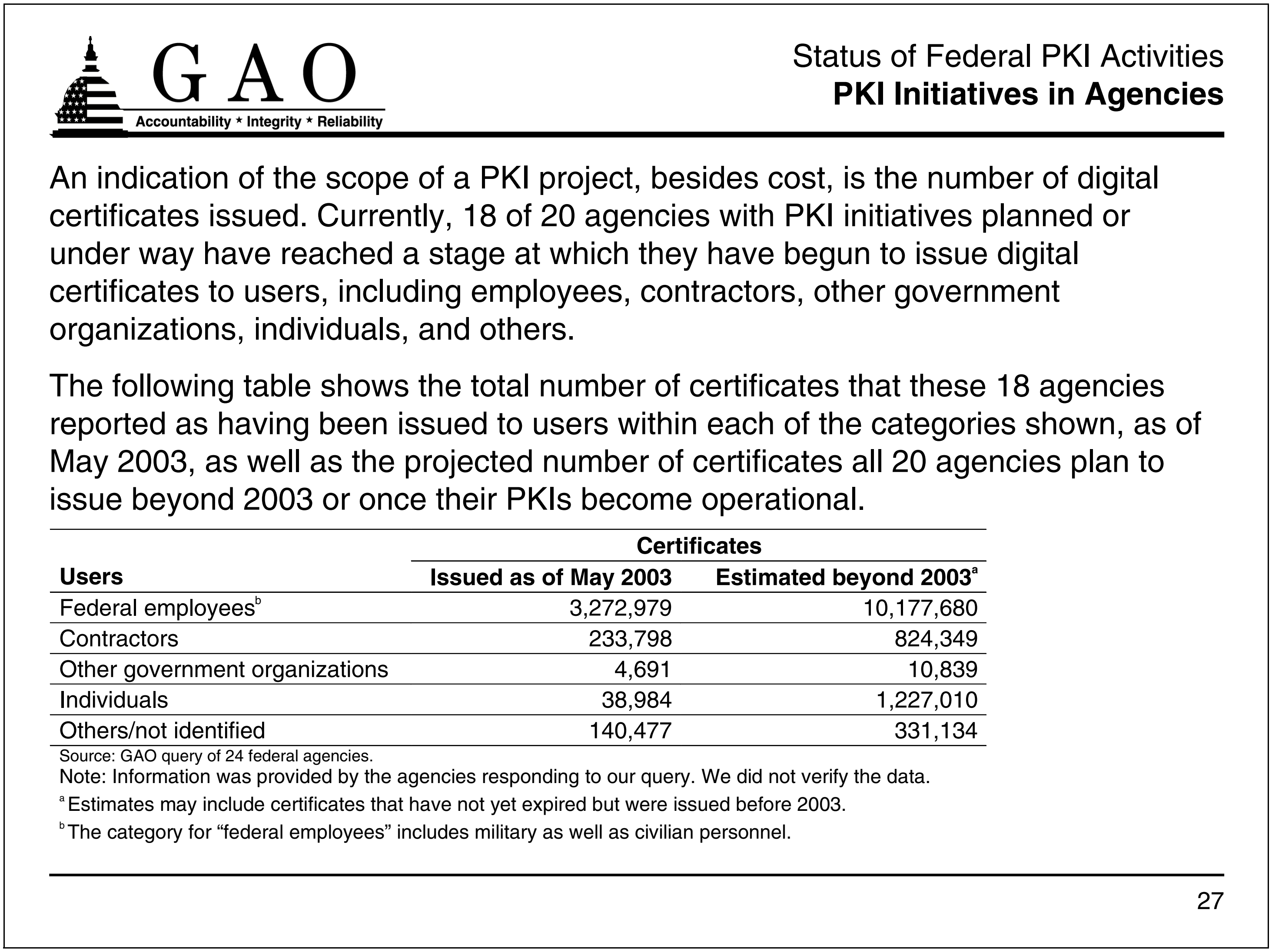
Estimated PKI costs for 24 agencies

Agency	Total estimated costs	Agency	Total estimated costs
Agriculture	$6,887,473	Transportation	$4,000,000
Commerce	$12,140,997	Treasury	$3,200,454
Defense	$822,995,000	Veterans Affairs	$52,550,000
Education	(not provided)	Environmental Protection Agency	$450,000
Energy	$12,000,000	Federal Emergency Management Agency	$225,000
General Services Administration	(not provided)	National Aeronautics and Space Administration	$1,891,758
Health and Human Services	$48,551,274	Nuclear Regulatory Commission	$2,500,000
Housing and Urban Development	(not provided)	National Science Foundation	$10,400,000
Interior	$9,800,000	Office of Personnel Management	(not provided)
Justice	(not provided)	Small Business Administration	$1,800,000
Labor	$2,541,692	Social Security Administration	$5,525,000
State	$8,051,600	U.S. Agency for International Development	(not provided)
		Total	**$1,005,510,248**

Source: GAO query of 24 federal agencies.

Note: Cost estimates were obtained from the 24 departments and agencies involved in our query. We did not independently verify these estimates.

26



Status of Federal PKI Activities

PKI Initiatives in Agencies

An indication of the scope of a PKI project, besides cost, is the number of digital certificates issued. Currently, 18 of 20 agencies with PKI initiatives planned or under way have reached a stage at which they have begun to issue digital certificates to users, including employees, contractors, other government organizations, individuals, and others.

The following table shows the total number of certificates that these 18 agencies reported as having been issued to users within each of the categories shown, as of May 2003, as well as the projected number of certificates all 20 agencies plan to issue beyond 2003 or once their PKIs become operational.

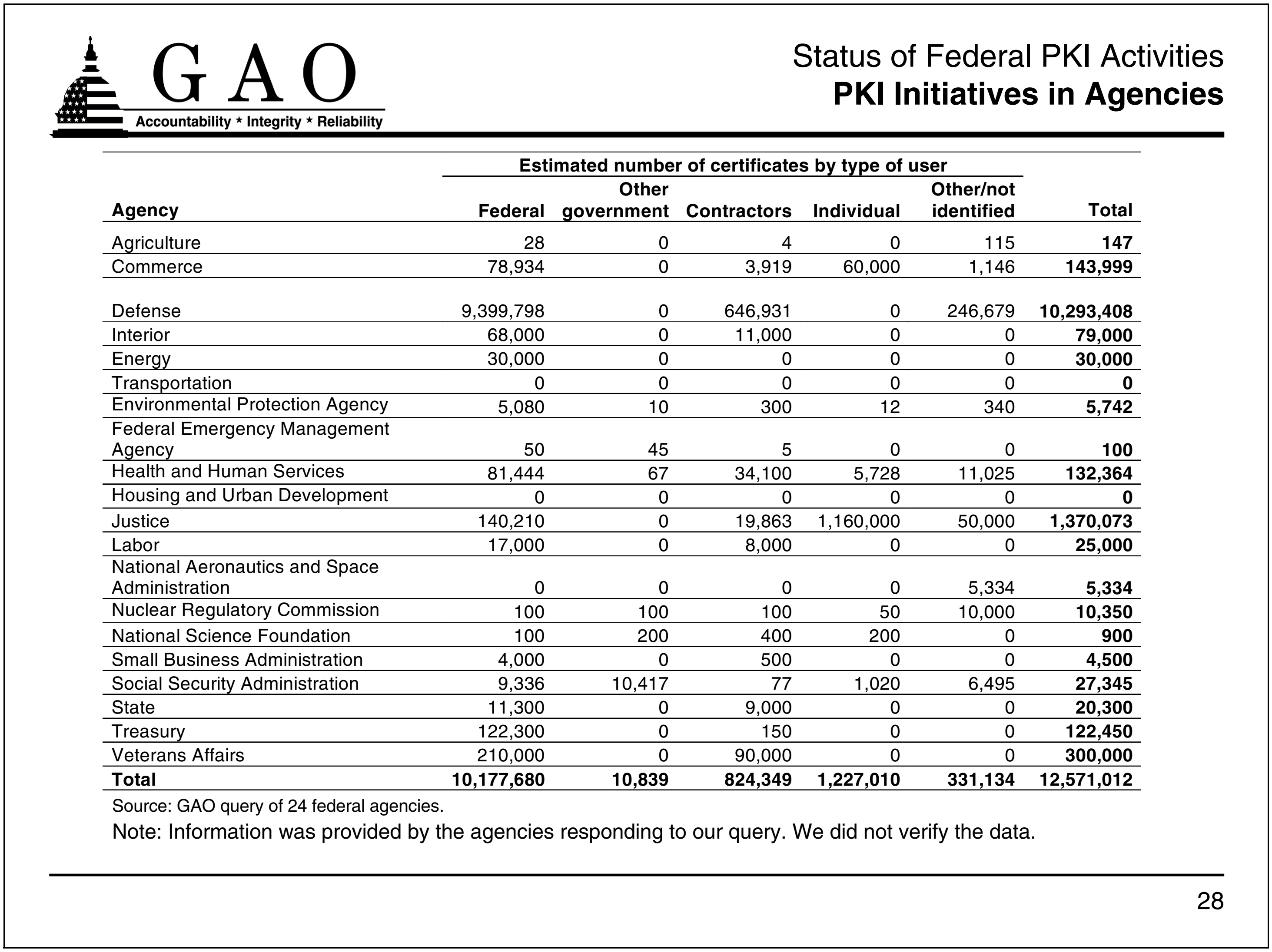
	Certificates	
Users	**Issued as of May 2003**	**Estimated beyond 2003[a]**
Federal employees[b]	3,272,979	10,177,680
Contractors	233,798	824,349
Other government organizations	4,691	10,839
Individuals	38,984	1,227,010
Others/not identified	140,477	331,134

Source: GAO query of 24 federal agencies.

Note: Information was provided by the agencies responding to our query. We did not verify the data.

[a] Estimates may include certificates that have not yet expired but were issued before 2003.

[b] The category for “federal employees” includes military as well as civilian personnel.



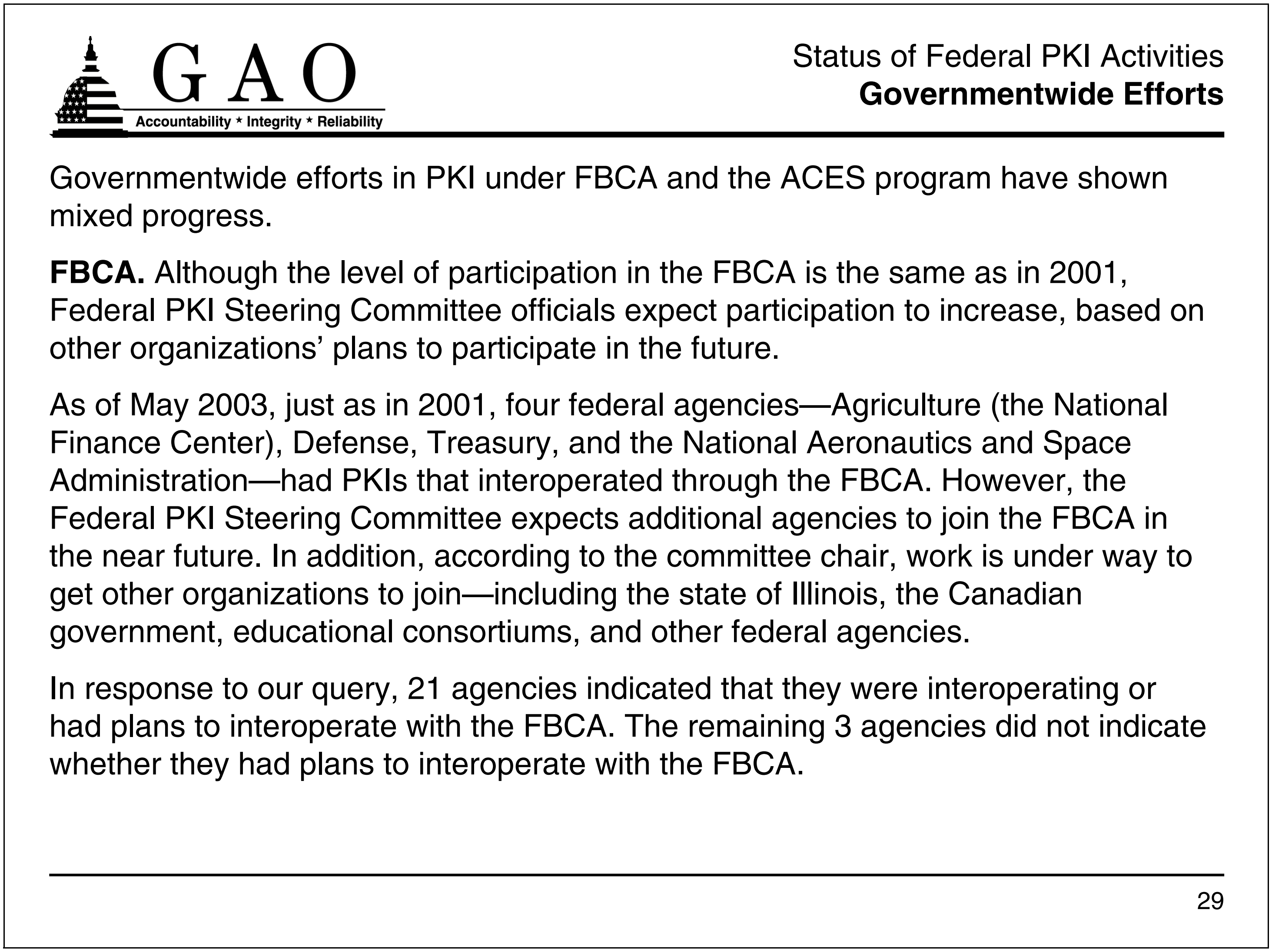
G A O
Accountability * Integrity * Reliability

Status of Federal PKI Activities
PKI Initiatives in Agencies

	Estimated number of certificates by type of user					
Agency	**Federal**	**Other government**	**Contractors**	**Individual**	**Other/not identified**	**Total**
Agriculture	28	0	4	0	115	**147**
Commerce	78,934	0	3,919	60,000	1,146	**143,999**
Defense	9,399,798	0	646,931	0	246,679	**10,293,408**
Interior	68,000	0	11,000	0	0	**79,000**
Energy	30,000	0	0	0	0	**30,000**
Transportation	0	0	0	0	0	**0**
Environmental Protection Agency	5,080	10	300	12	340	**5,742**
Federal Emergency Management Agency	50	45	5	0	0	**100**
Health and Human Services	81,444	67	34,100	5,728	11,025	**132,364**
Housing and Urban Development	0	0	0	0	0	**0**
Justice	140,210	0	19,863	1,160,000	50,000	**1,370,073**
Labor	17,000	0	8,000	0	0	**25,000**
National Aeronautics and Space Administration	0	0	0	0	5,334	**5,334**
Nuclear Regulatory Commission	100	100	100	50	10,000	**10,350**
National Science Foundation	100	200	400	200	0	**900**
Small Business Administration	4,000	0	500	0	0	**4,500**
Social Security Administration	9,336	10,417	77	1,020	6,495	**27,345**
State	11,300	0	9,000	0	0	**20,300**
Treasury	122,300	0	150	0	0	**122,450**
Veterans Affairs	210,000	0	90,000	0	0	**300,000**
Total	**10,177,680**	**10,839**	**824,349**	**1,227,010**	**331,134**	**12,571,012**

Source: GAO query of 24 federal agencies.

Note: Information was provided by the agencies responding to our query. We did not verify the data.



Status of Federal PKI Activities
Governmentwide Efforts

Governmentwide efforts in PKI under FBCA and the ACES program have shown mixed progress.

FBCA. Although the level of participation in the FBCA is the same as in 2001, Federal PKI Steering Committee officials expect participation to increase, based on other organizations' plans to participate in the future.

As of May 2003, just as in 2001, four federal agencies—Agriculture (the National Finance Center), Defense, Treasury, and the National Aeronautics and Space Administration—had PKIs that interoperated through the FBCA. However, the Federal PKI Steering Committee expects additional agencies to join the FBCA in the near future. In addition, according to the committee chair, work is under way to get other organizations to join—including the state of Illinois, the Canadian government, educational consortiums, and other federal agencies.

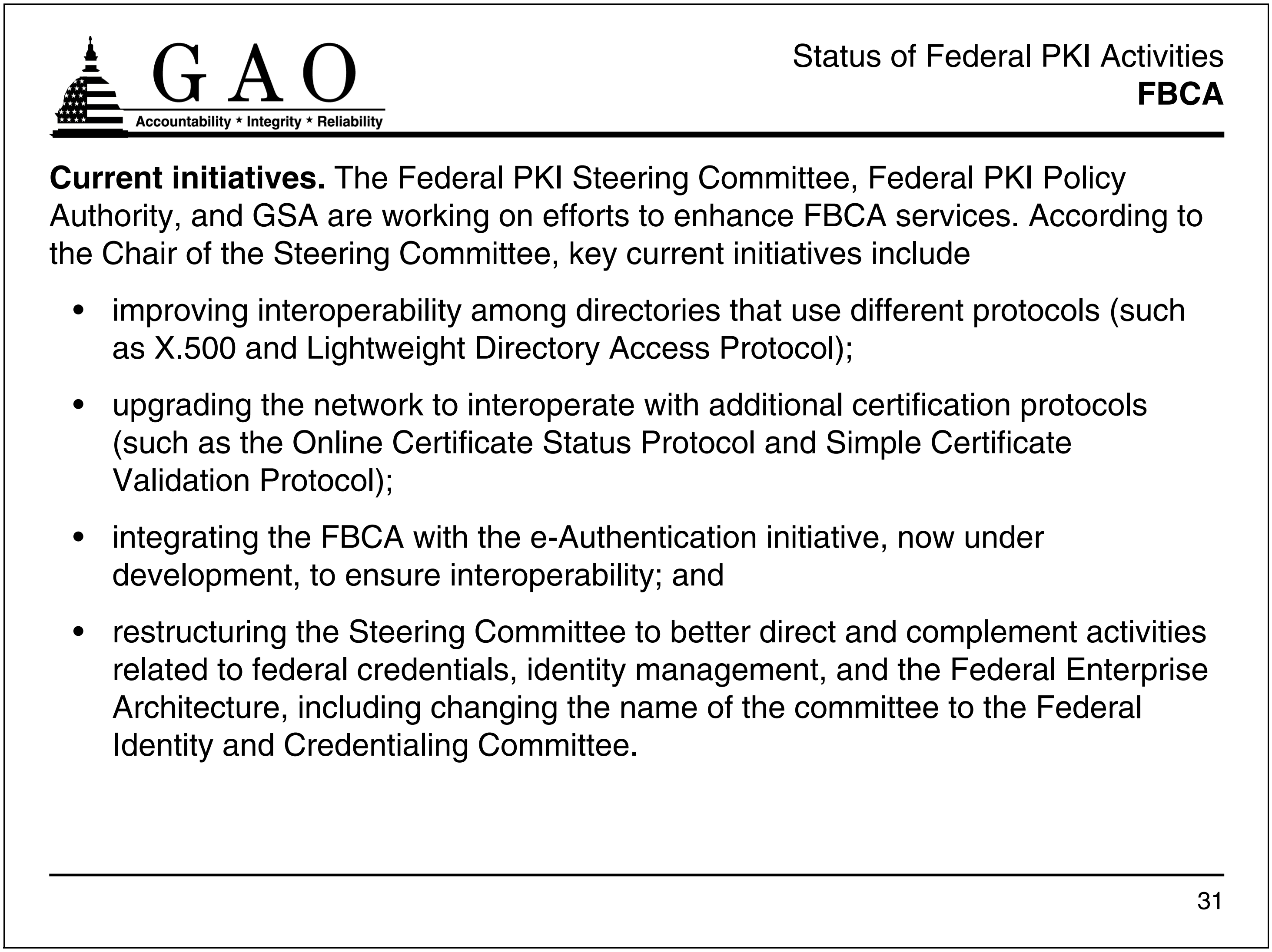
In response to our query, 21 agencies indicated that they were interoperating or had plans to interoperate with the FBCA. The remaining 3 agencies did not indicate whether they had plans to interoperate with the FBCA.

GAO
Accountability * Integrity * Reliability

Status of Federal PKI Activities
FBCA

Resources. According to the chair of the Federal PKI Steering Committee, about $3.5 million annually has been provided for the FBCA and Policy Authority since 2001. About $1.5 million was used for operations and maintenance of the FBCA's systems, and about $1 million was used for administrative purposes—including staffing, contracting support, and the Policy Authority. The remaining nearly $1 million was used for matching investment programs aimed at increasing PKI implementation across government and to encourage linking with the FBCA.

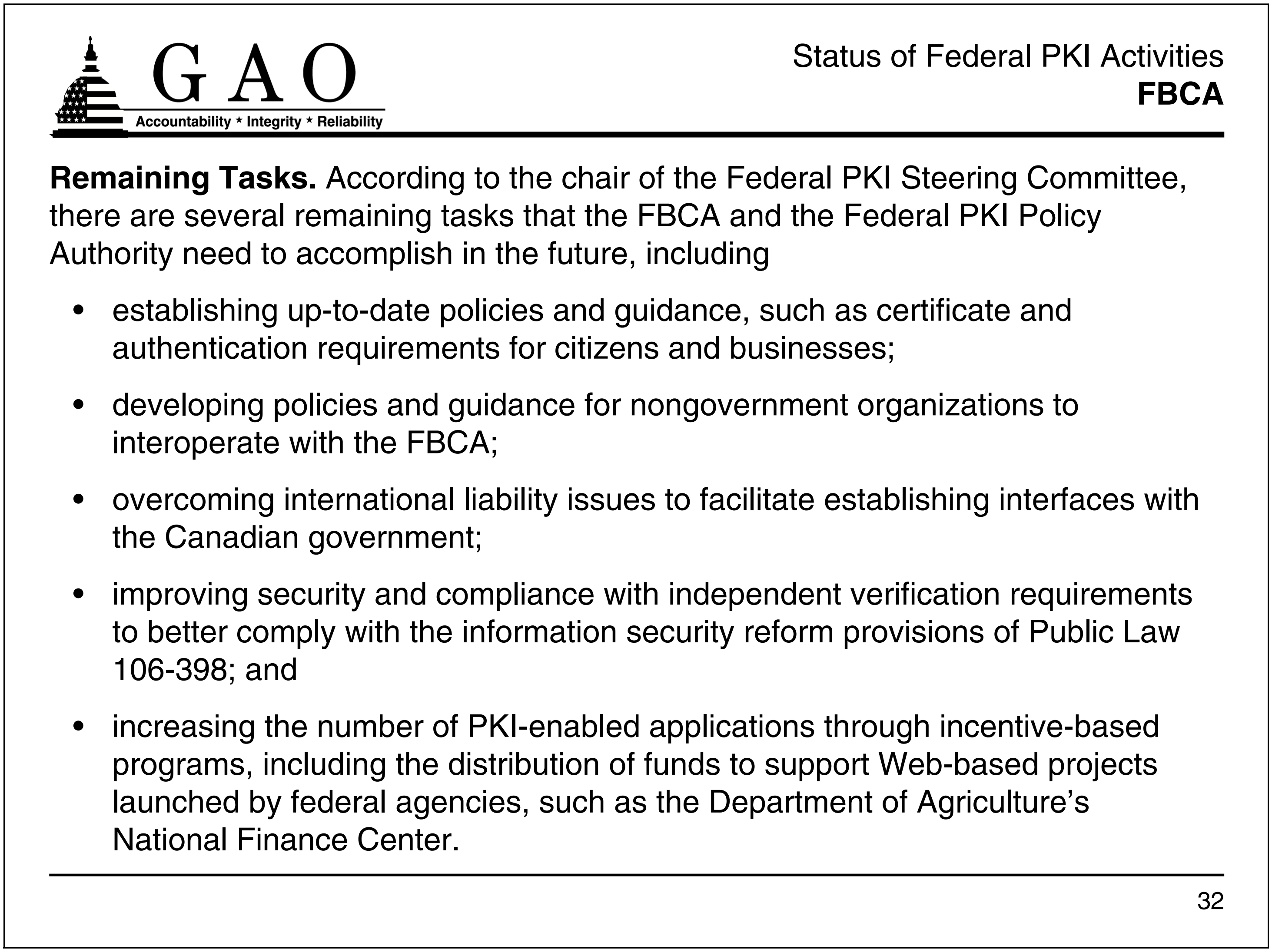
30



Status of Federal PKI Activities
FBCA

Current initiatives. The Federal PKI Steering Committee, Federal PKI Policy Authority, and GSA are working on efforts to enhance FBCA services. According to the Chair of the Steering Committee, key current initiatives include

- improving interoperability among directories that use different protocols (such as X.500 and Lightweight Directory Access Protocol);
- upgrading the network to interoperate with additional certification protocols (such as the Online Certificate Status Protocol and Simple Certificate Validation Protocol);
- integrating the FBCA with the e-Authentication initiative, now under development, to ensure interoperability; and
- restructuring the Steering Committee to better direct and complement activities related to federal credentials, identity management, and the Federal Enterprise Architecture, including changing the name of the committee to the Federal Identity and Credentialing Committee.



Status of Federal PKI Activities
FBCA

Remaining Tasks. According to the chair of the Federal PKI Steering Committee, there are several remaining tasks that the FBCA and the Federal PKI Policy Authority need to accomplish in the future, including

- establishing up-to-date policies and guidance, such as certificate and authentication requirements for citizens and businesses;
- developing policies and guidance for nongovernment organizations to interoperate with the FBCA;
- overcoming international liability issues to facilitate establishing interfaces with the Canadian government;
- improving security and compliance with independent verification requirements to better comply with the information security reform provisions of Public Law 106-398; and
- increasing the number of PKI-enabled applications through incentive-based programs, including the distribution of funds to support Web-based projects launched by federal agencies, such as the Department of Agriculture's National Finance Center.

32

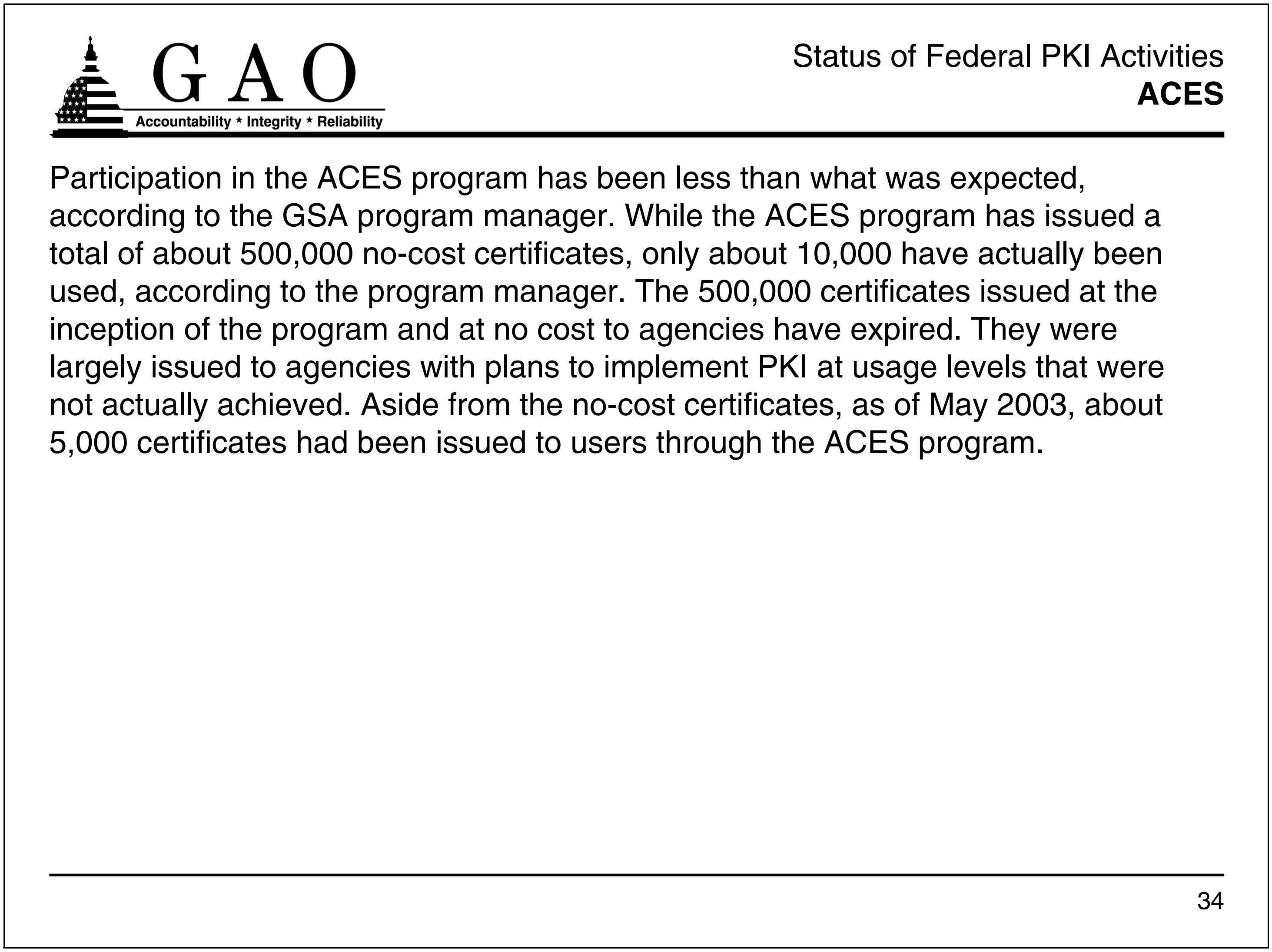
Status of Federal PKI Activities
ACES

For the ACES program, which offers PKI services to agencies through a GSA contract, the program manager stated that participation has been lower than expected because agencies have been slow to adopt PKI in general. As of May 2003, in response to our query, 11 agencies stated that they were either participating or planning to participate in the ACES program. For example, according to its program manager, Treasury was considering using ACES to issue certificates to financial institutions to comply with provisions of the USA PATRIOT Act.[8]

Another 12 agencies indicated that they did not plan to use the ACES program at this time. Of the 12 agencies, 3 indicated that it was too expensive to use these services, and one reported that ACES failed to meet its security requirements. The remaining 8 agencies either did not indicate why they would not use the ACES program or provided a variety of other reasons, such as waiting for contract modifications and having no requirement to use the program.

One agency did not indicate whether it would use the ACES program.

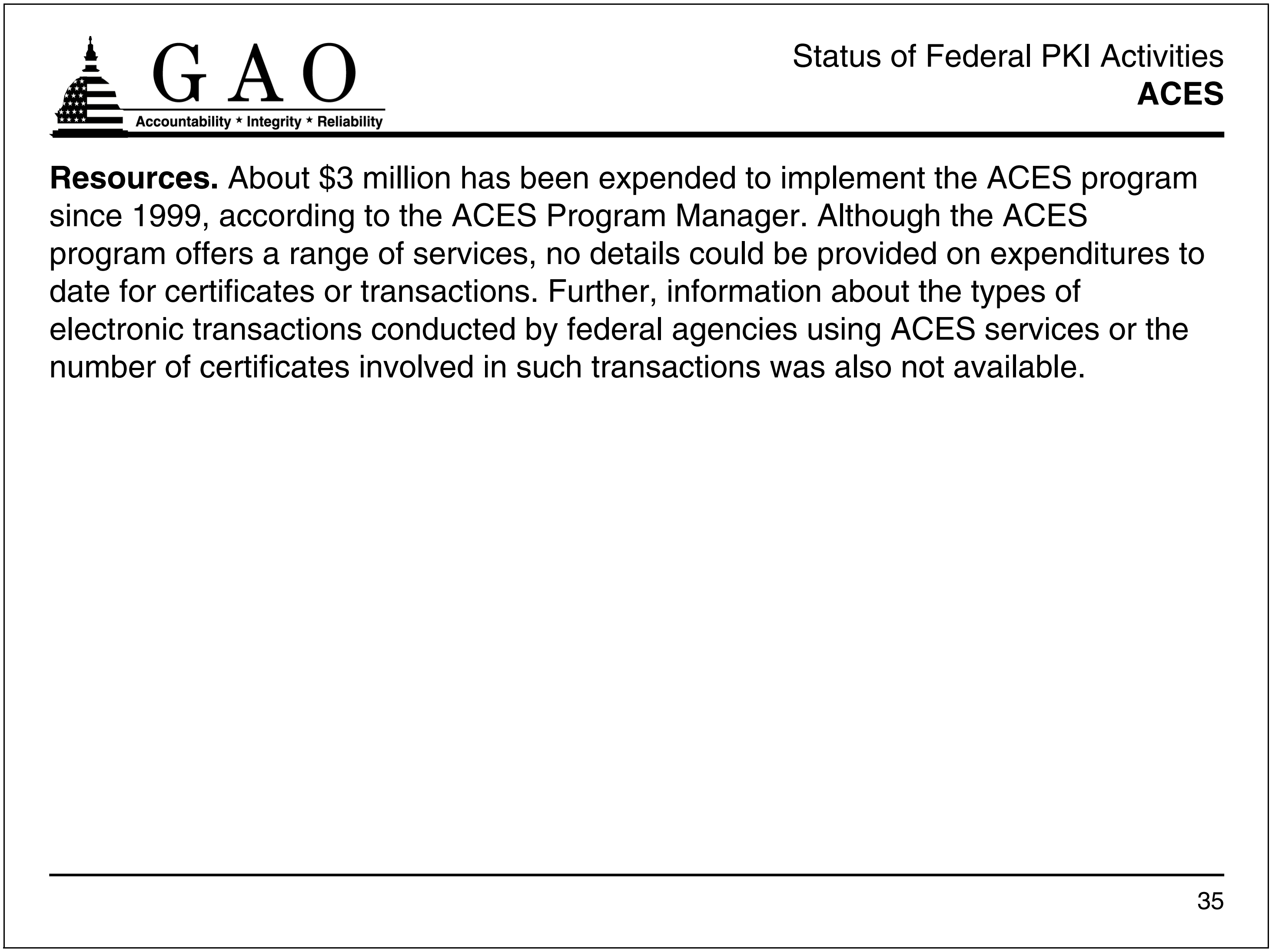
[8] USA PATRIOT Act, Public Law 107-56 (Oct. 26, 2001). Section 365 requires that a person or financial institution report cash transactions over $10,000.



Status of Federal PKI Activities
ACES

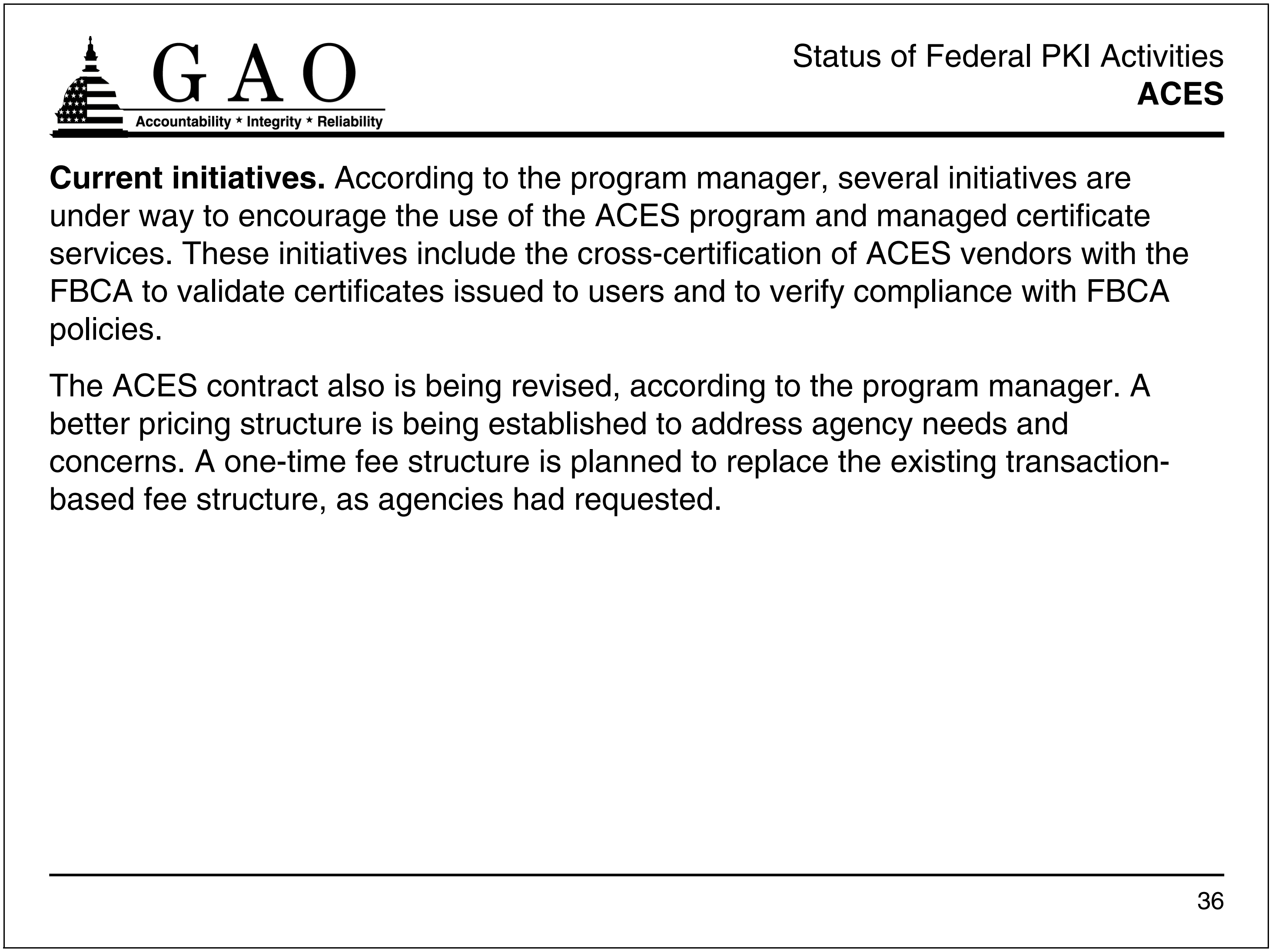
Participation in the ACES program has been less than what was expected, according to the GSA program manager. While the ACES program has issued a total of about 500,000 no-cost certificates, only about 10,000 have actually been used, according to the program manager. The 500,000 certificates issued at the inception of the program and at no cost to agencies have expired. They were largely issued to agencies with plans to implement PKI at usage levels that were not actually achieved. Aside from the no-cost certificates, as of May 2003, about 5,000 certificates had been issued to users through the ACES program.

34



Status of Federal PKI Activities
ACES

Resources. About $3 million has been expended to implement the ACES program since 1999, according to the ACES Program Manager. Although the ACES program offers a range of services, no details could be provided on expenditures to date for certificates or transactions. Further, information about the types of electronic transactions conducted by federal agencies using ACES services or the number of certificates involved in such transactions was also not available.

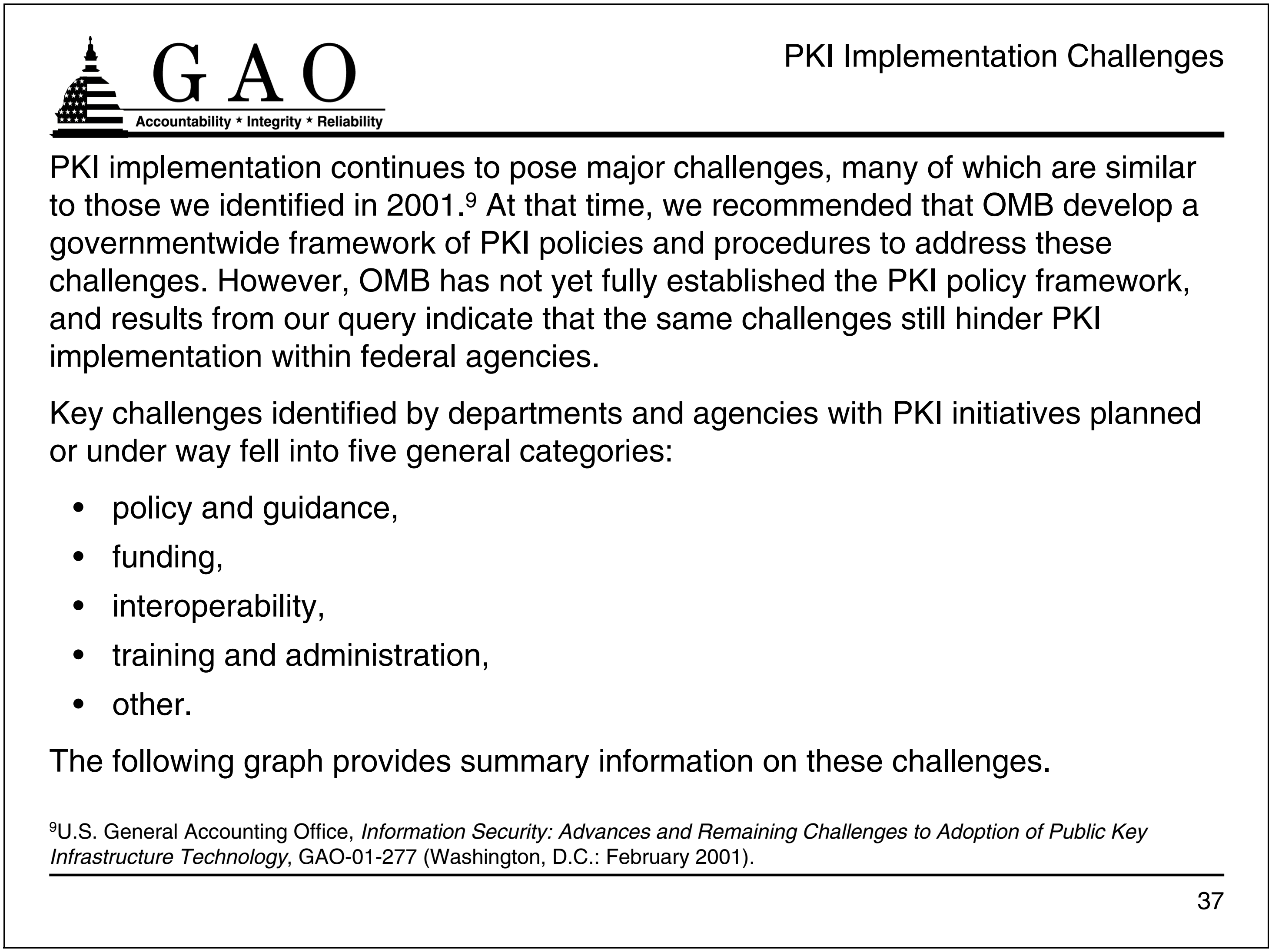


Status of Federal PKI Activities
ACES

Current initiatives. According to the program manager, several initiatives are under way to encourage the use of the ACES program and managed certificate services. These initiatives include the cross-certification of ACES vendors with the FBCA to validate certificates issued to users and to verify compliance with FBCA policies.

The ACES contract also is being revised, according to the program manager. A better pricing structure is being established to address agency needs and concerns. A one-time fee structure is planned to replace the existing transaction-based fee structure, as agencies had requested.

36



PKI Implementation Challenges

PKI implementation continues to pose major challenges, many of which are similar to those we identified in 2001.[9] At that time, we recommended that OMB develop a governmentwide framework of PKI policies and procedures to address these challenges. However, OMB has not yet fully established the PKI policy framework, and results from our query indicate that the same challenges still hinder PKI implementation within federal agencies.

Key challenges identified by departments and agencies with PKI initiatives planned or under way fell into five general categories:

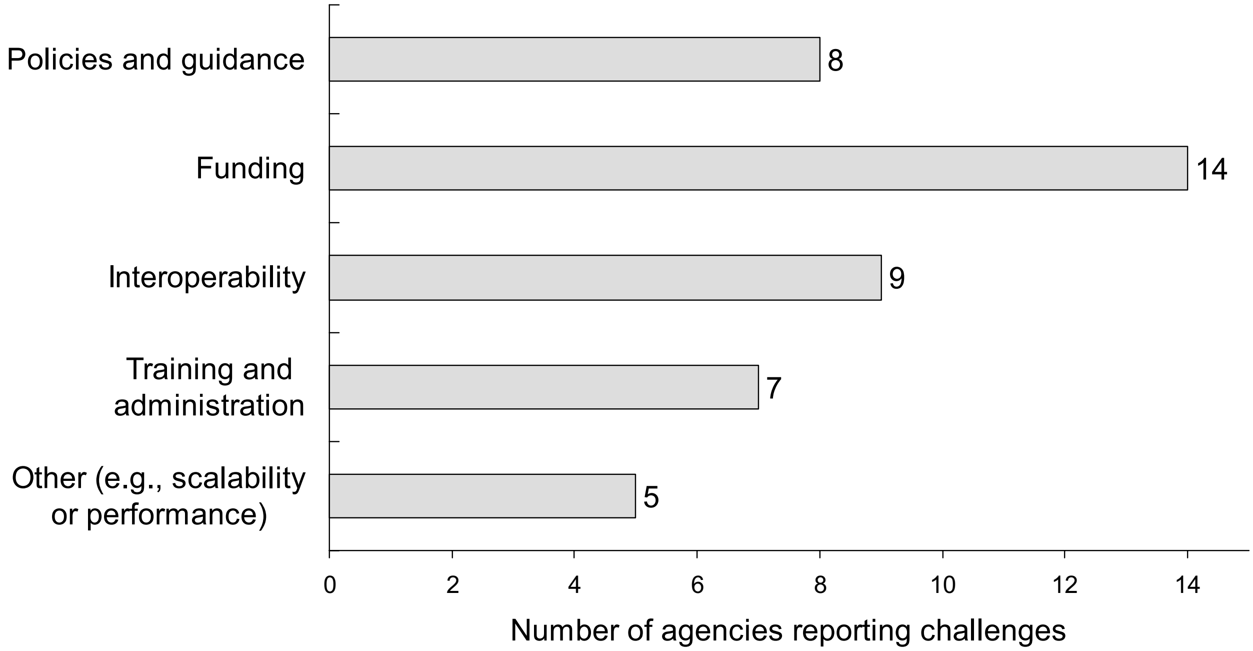
- policy and guidance,
- funding,
- interoperability,
- training and administration,
- other.

The following graph provides summary information on these challenges.

[9] U.S. General Accounting Office, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: February 2001).

PKI Implementation Challenges

Types of overall PKI challenges reported by agencies



Source: GAO query of 24 federal agencies.

GAO Accountability * Integrity * Reliability

PKI Implementation Challenges

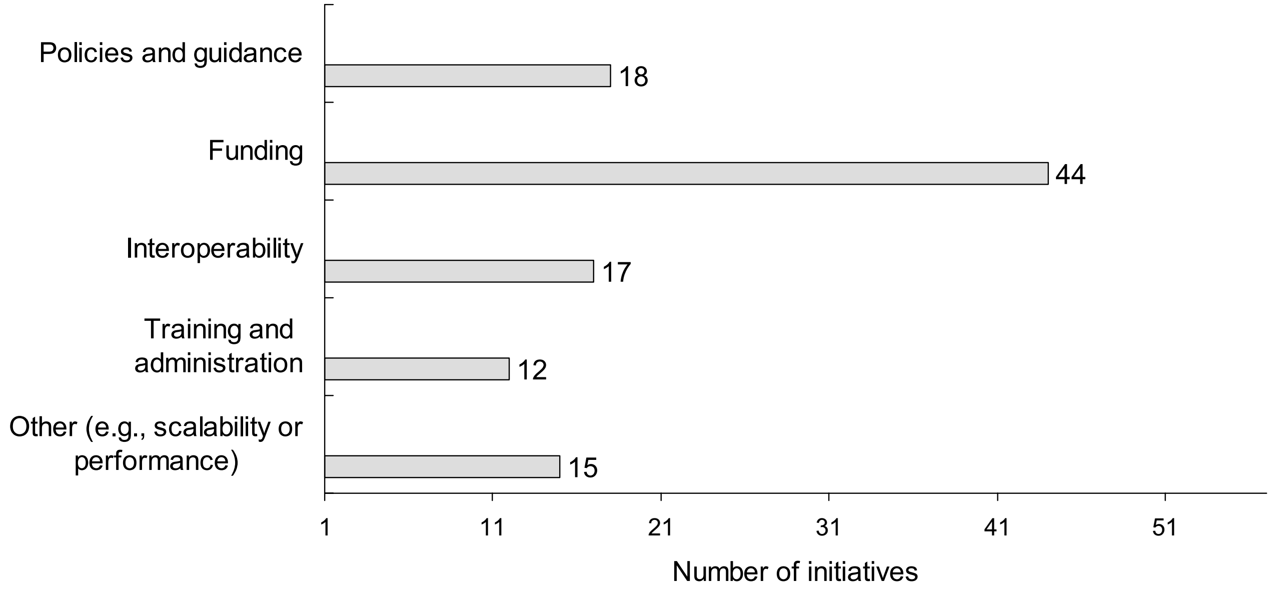
Additionally, 15 agencies provided information on challenges specifically related to their PKI initiatives planned or under way. For 57 out of the 89 PKI initiatives (about 64 percent), agencies reported experiencing at least one of the five key challenges. Many agencies identified multiple challenges for their PKI initiatives.

The following graph provides summary information on the key challenges encountered by these 57 initiatives.

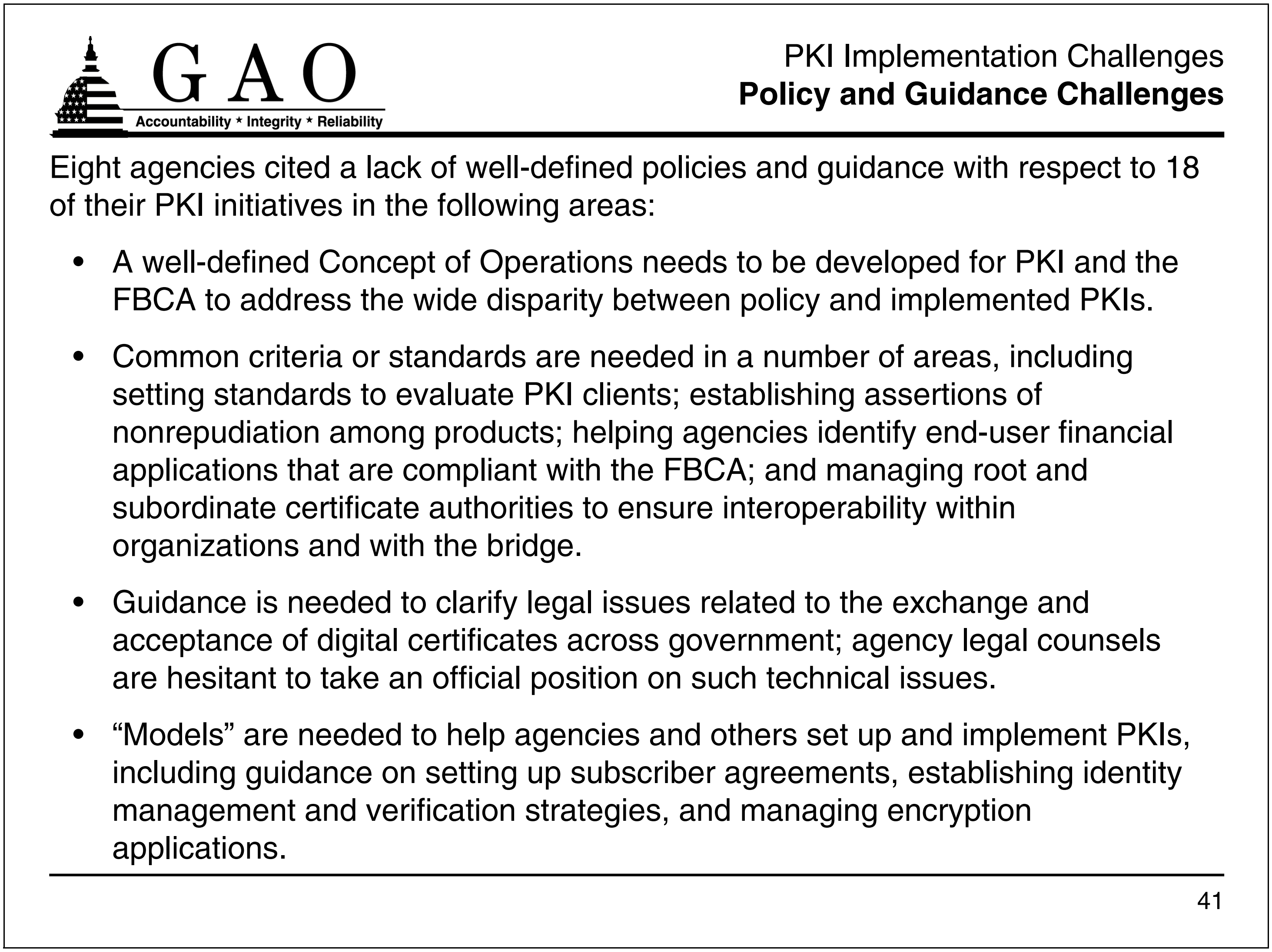
GAO
Accountability * Integrity * Reliability

PKI Implementation Challenges

Number of PKI initiatives and key challenges associated with them



Source: GAO query of 24 federal agencies.



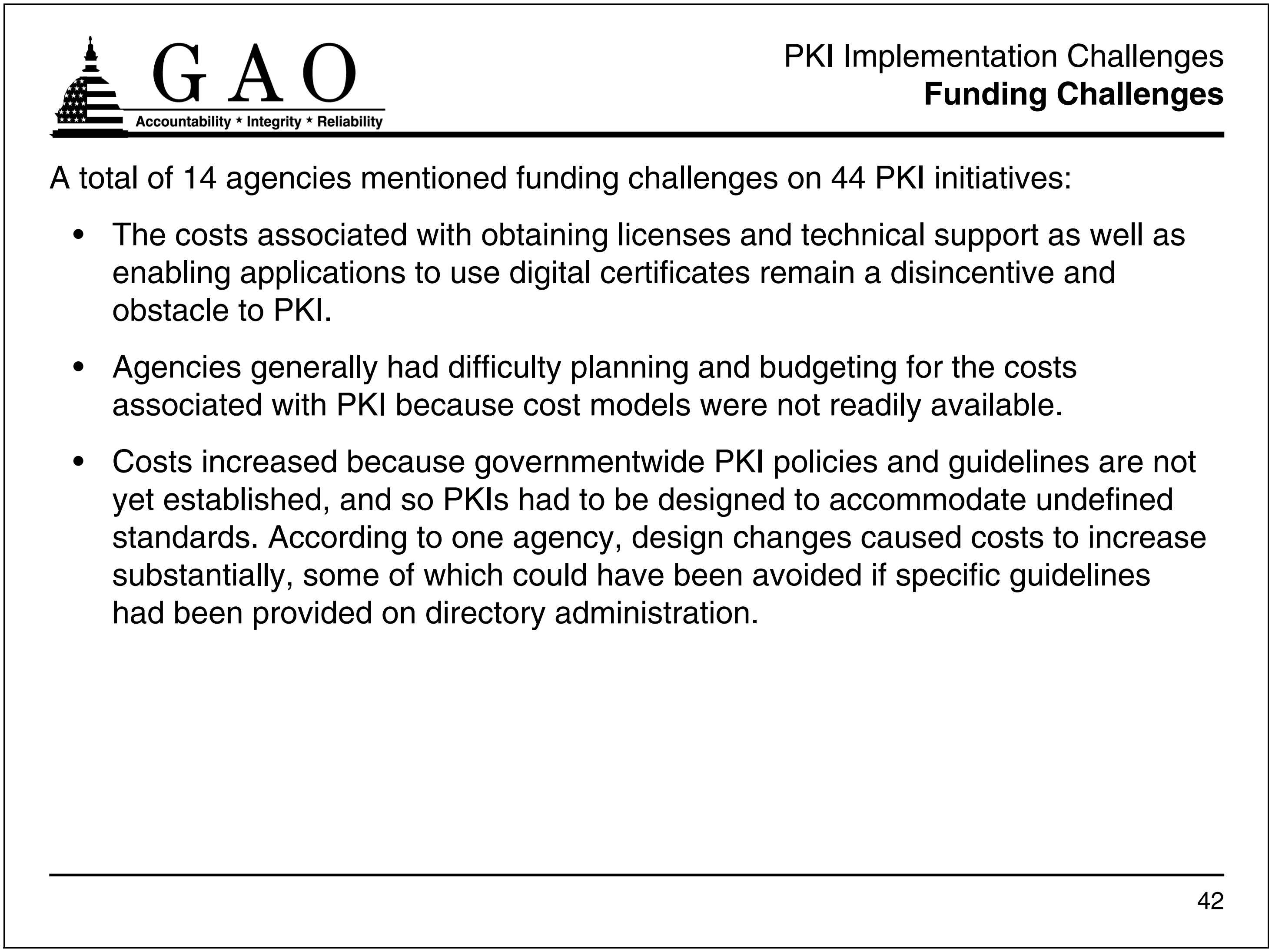
PKI Implementation Challenges

Policy and Guidance Challenges

Eight agencies cited a lack of well-defined policies and guidance with respect to 18 of their PKI initiatives in the following areas:

- A well-defined Concept of Operations needs to be developed for PKI and the FBCA to address the wide disparity between policy and implemented PKIs.
- Common criteria or standards are needed in a number of areas, including setting standards to evaluate PKI clients; establishing assertions of nonrepudiation among products; helping agencies identify end-user financial applications that are compliant with the FBCA; and managing root and subordinate certificate authorities to ensure interoperability within organizations and with the bridge.
- Guidance is needed to clarify legal issues related to the exchange and acceptance of digital certificates across government; agency legal counsels are hesitant to take an official position on such technical issues.
- “Models” are needed to help agencies and others set up and implement PKIs, including guidance on setting up subscriber agreements, establishing identity management and verification strategies, and managing encryption applications.

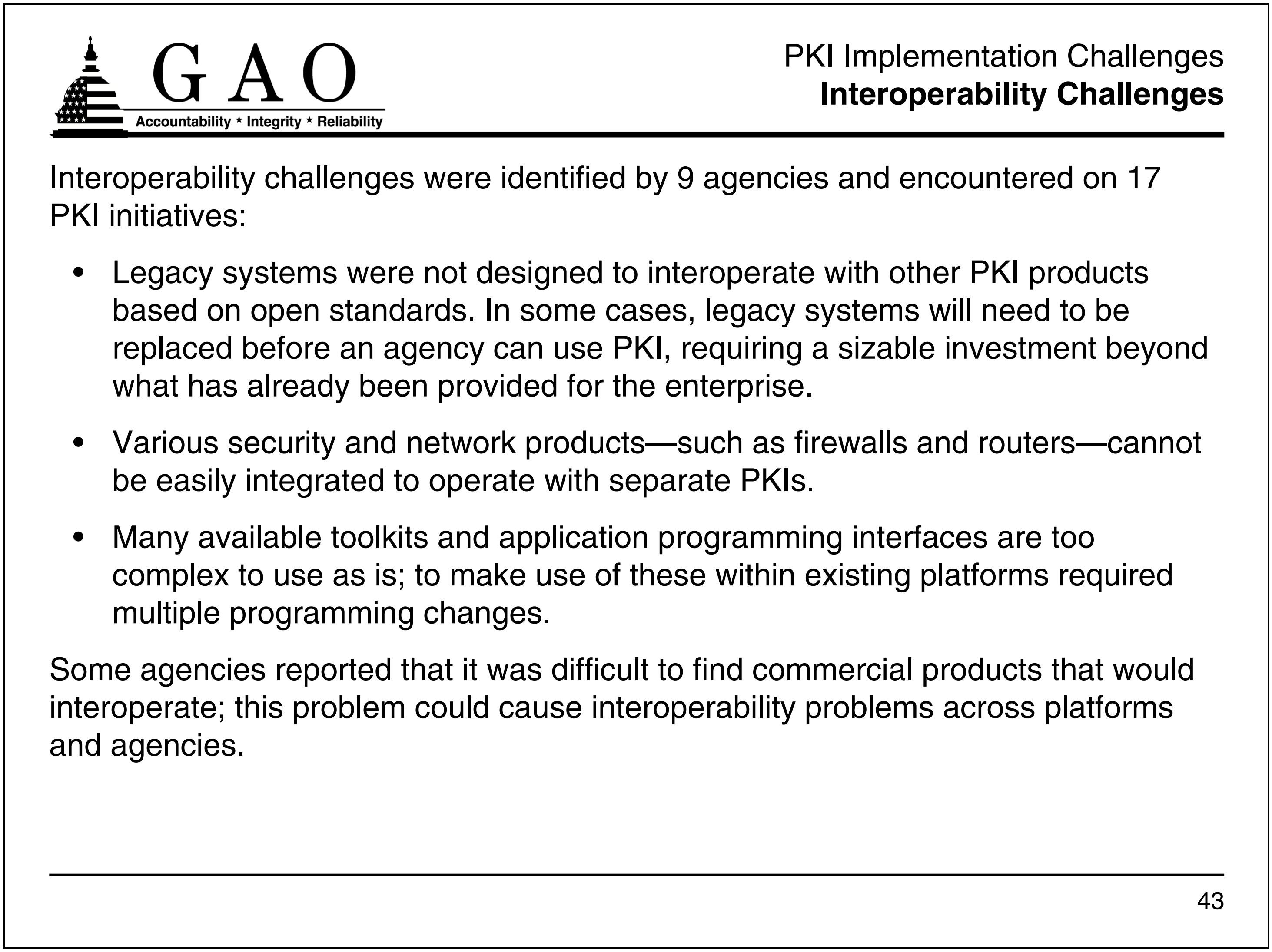
41



PKI Implementation Challenges
Funding Challenges

A total of 14 agencies mentioned funding challenges on 44 PKI initiatives:

- The costs associated with obtaining licenses and technical support as well as enabling applications to use digital certificates remain a disincentive and obstacle to PKI.
- Agencies generally had difficulty planning and budgeting for the costs associated with PKI because cost models were not readily available.
- Costs increased because governmentwide PKI policies and guidelines are not yet established, and so PKIs had to be designed to accommodate undefined standards. According to one agency, design changes caused costs to increase substantially, some of which could have been avoided if specific guidelines had been provided on directory administration.

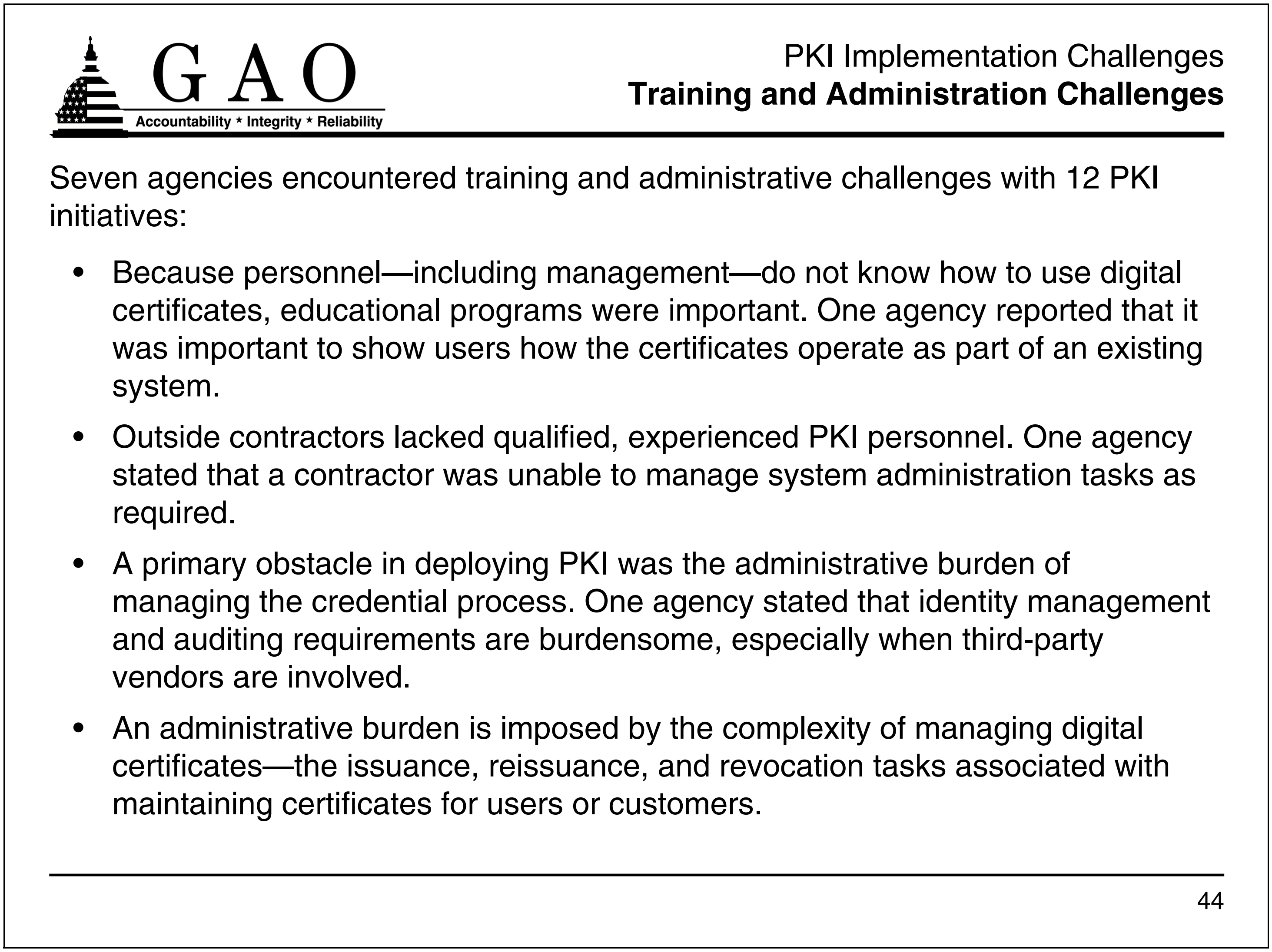


PKI Implementation Challenges
Interoperability Challenges

Interoperability challenges were identified by 9 agencies and encountered on 17 PKI initiatives:

- Legacy systems were not designed to interoperate with other PKI products based on open standards. In some cases, legacy systems will need to be replaced before an agency can use PKI, requiring a sizable investment beyond what has already been provided for the enterprise.
- Various security and network products—such as firewalls and routers—cannot be easily integrated to operate with separate PKIs.
- Many available toolkits and application programming interfaces are too complex to use as is; to make use of these within existing platforms required multiple programming changes.

Some agencies reported that it was difficult to find commercial products that would interoperate; this problem could cause interoperability problems across platforms and agencies.

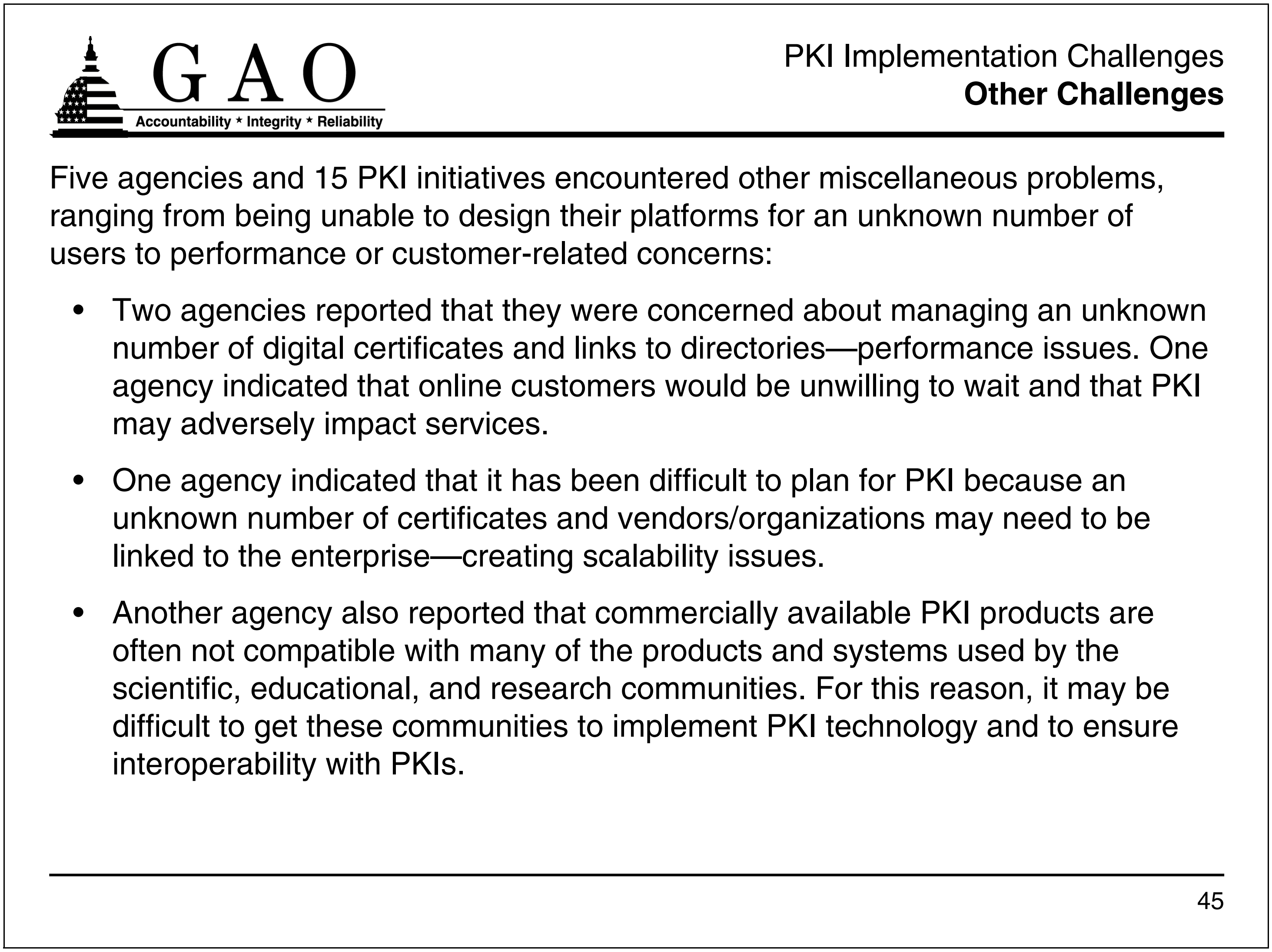


PKI Implementation Challenges

Training and Administration Challenges

Seven agencies encountered training and administrative challenges with 12 PKI initiatives:

- Because personnel—including management—do not know how to use digital certificates, educational programs were important. One agency reported that it was important to show users how the certificates operate as part of an existing system.
- Outside contractors lacked qualified, experienced PKI personnel. One agency stated that a contractor was unable to manage system administration tasks as required.
- A primary obstacle in deploying PKI was the administrative burden of managing the credential process. One agency stated that identity management and auditing requirements are burdensome, especially when third-party vendors are involved.
- An administrative burden is imposed by the complexity of managing digital certificates—the issuance, reissuance, and revocation tasks associated with maintaining certificates for users or customers.



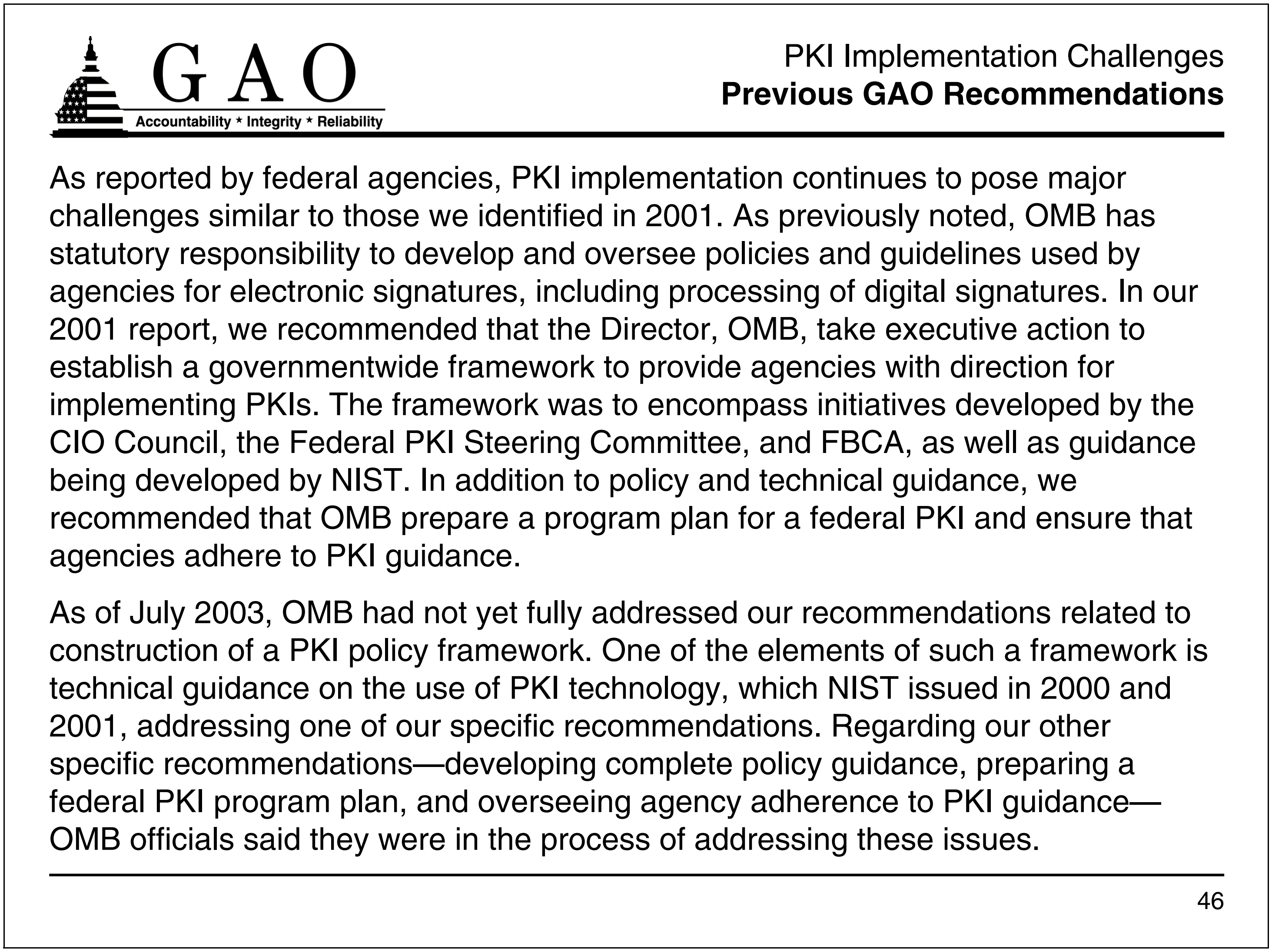
PKI Implementation Challenges

Other Challenges

Five agencies and 15 PKI initiatives encountered other miscellaneous problems, ranging from being unable to design their platforms for an unknown number of users to performance or customer-related concerns:

- Two agencies reported that they were concerned about managing an unknown number of digital certificates and links to directories—performance issues. One agency indicated that online customers would be unwilling to wait and that PKI may adversely impact services.
- One agency indicated that it has been difficult to plan for PKI because an unknown number of certificates and vendors/organizations may need to be linked to the enterprise—creating scalability issues.
- Another agency also reported that commercially available PKI products are often not compatible with many of the products and systems used by the scientific, educational, and research communities. For this reason, it may be difficult to get these communities to implement PKI technology and to ensure interoperability with PKIs.

45

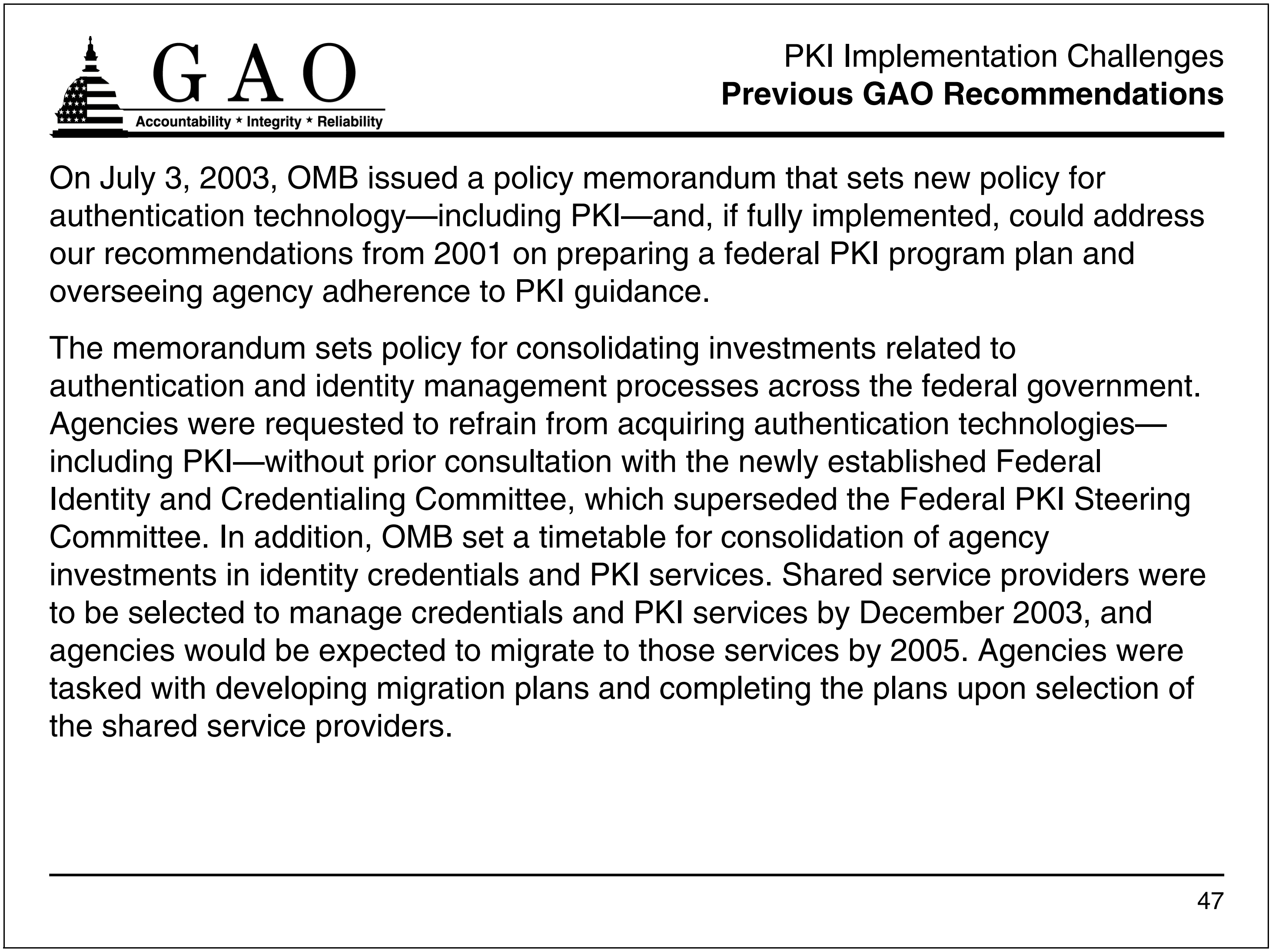


PKI Implementation Challenges
Previous GAO Recommendations

As reported by federal agencies, PKI implementation continues to pose major challenges similar to those we identified in 2001. As previously noted, OMB has statutory responsibility to develop and oversee policies and guidelines used by agencies for electronic signatures, including processing of digital signatures. In our 2001 report, we recommended that the Director, OMB, take executive action to establish a governmentwide framework to provide agencies with direction for implementing PKIs. The framework was to encompass initiatives developed by the CIO Council, the Federal PKI Steering Committee, and FBCA, as well as guidance being developed by NIST. In addition to policy and technical guidance, we recommended that OMB prepare a program plan for a federal PKI and ensure that agencies adhere to PKI guidance.

As of July 2003, OMB had not yet fully addressed our recommendations related to construction of a PKI policy framework. One of the elements of such a framework is technical guidance on the use of PKI technology, which NIST issued in 2000 and 2001, addressing one of our specific recommendations. Regarding our other specific recommendations—developing complete policy guidance, preparing a federal PKI program plan, and overseeing agency adherence to PKI guidance—OMB officials said they were in the process of addressing these issues.

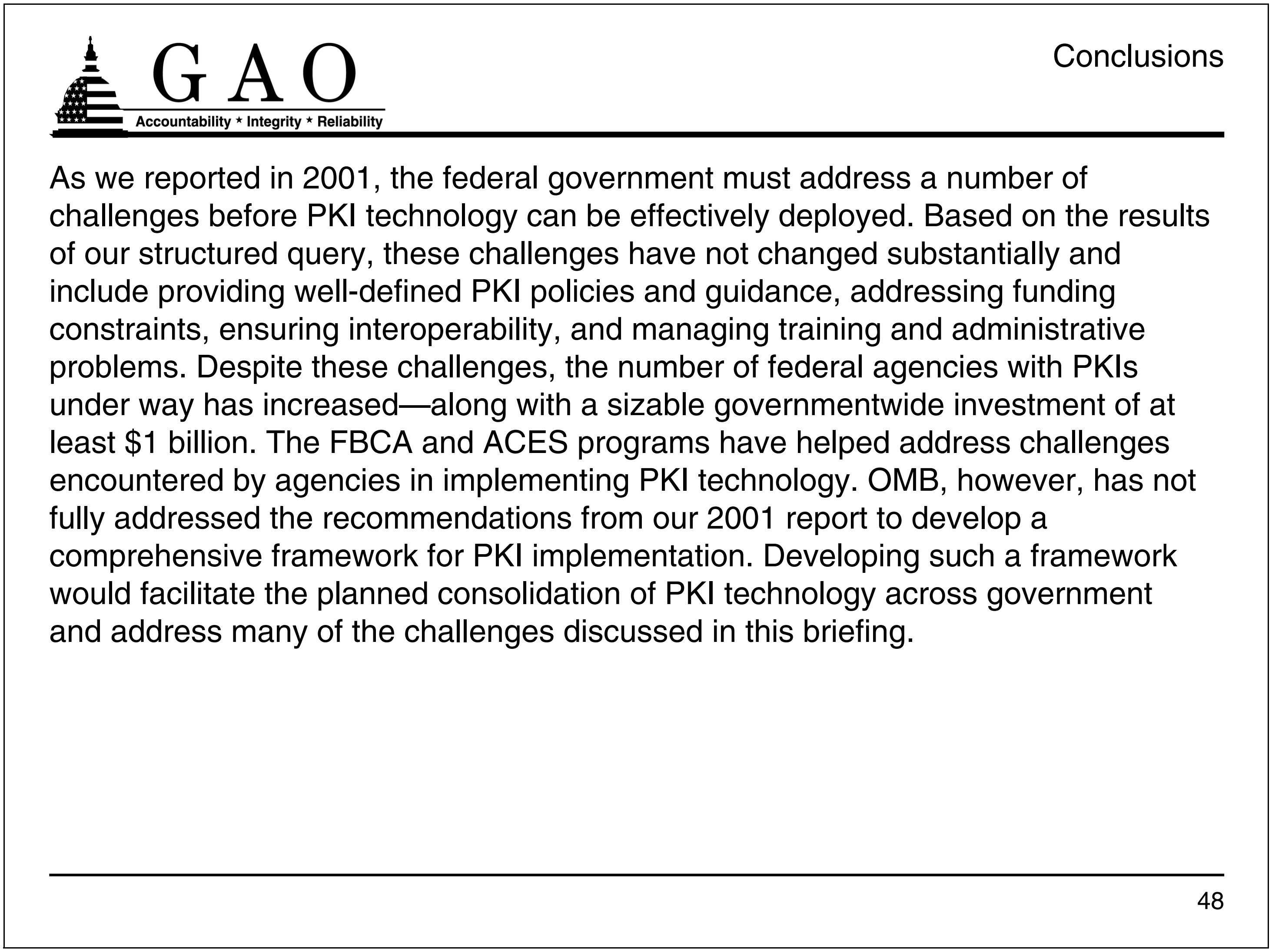
46



PKI Implementation Challenges
Previous GAO Recommendations

On July 3, 2003, OMB issued a policy memorandum that sets new policy for authentication technology—including PKI—and, if fully implemented, could address our recommendations from 2001 on preparing a federal PKI program plan and overseeing agency adherence to PKI guidance.

The memorandum sets policy for consolidating investments related to authentication and identity management processes across the federal government. Agencies were requested to refrain from acquiring authentication technologies—including PKI—without prior consultation with the newly established Federal Identity and Credentialing Committee, which superseded the Federal PKI Steering Committee. In addition, OMB set a timetable for consolidation of agency investments in identity credentials and PKI services. Shared service providers were to be selected to manage credentials and PKI services by December 2003, and agencies would be expected to migrate to those services by 2005. Agencies were tasked with developing migration plans and completing the plans upon selection of the shared service providers.

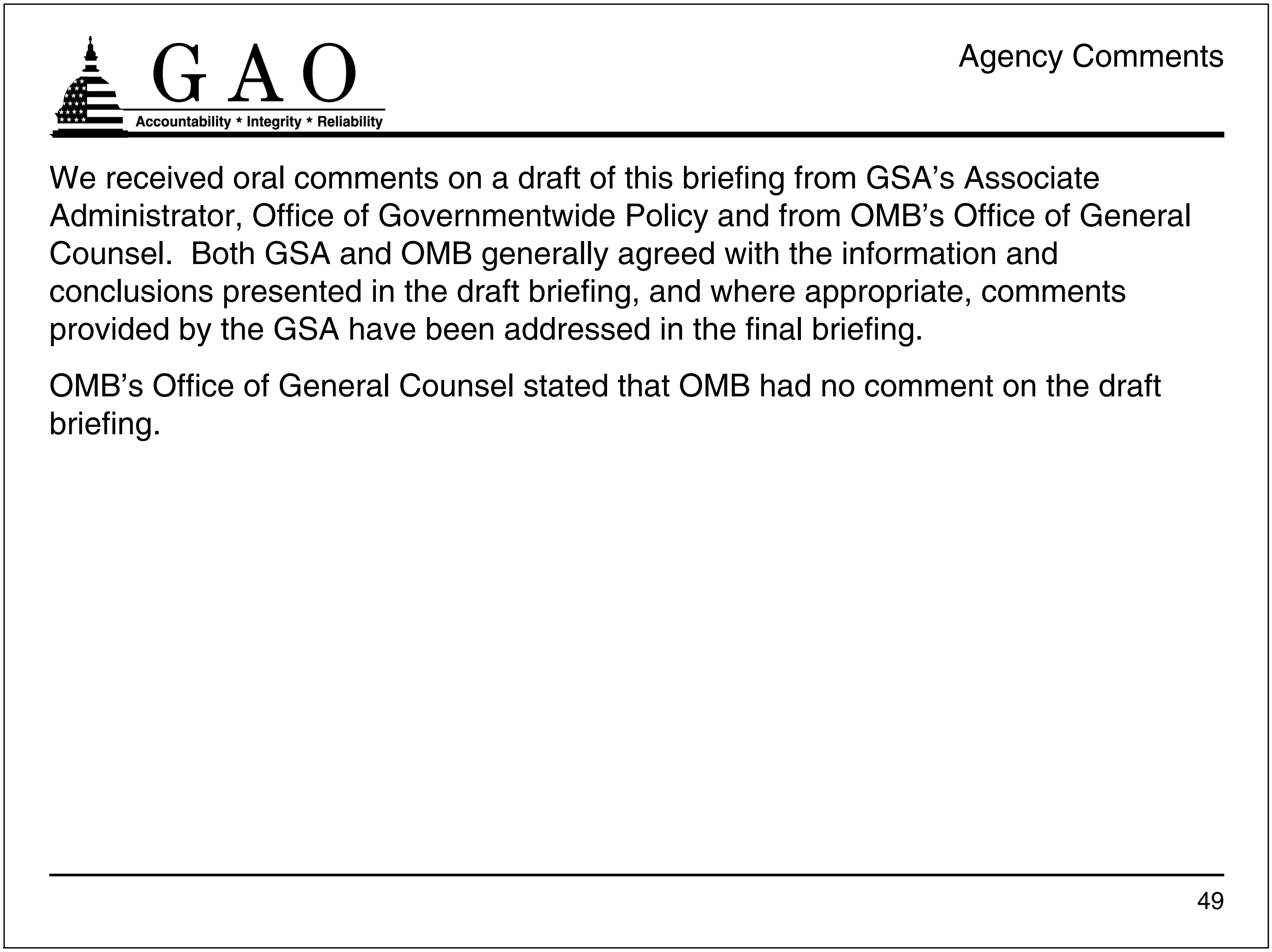


GAO
Accountability * Integrity * Reliability

Conclusions

As we reported in 2001, the federal government must address a number of challenges before PKI technology can be effectively deployed. Based on the results of our structured query, these challenges have not changed substantially and include providing well-defined PKI policies and guidance, addressing funding constraints, ensuring interoperability, and managing training and administrative problems. Despite these challenges, the number of federal agencies with PKIs under way has increased—along with a sizable governmentwide investment of at least $1 billion. The FBCA and ACES programs have helped address challenges encountered by agencies in implementing PKI technology. OMB, however, has not fully addressed the recommendations from our 2001 report to develop a comprehensive framework for PKI implementation. Developing such a framework would facilitate the planned consolidation of PKI technology across government and address many of the challenges discussed in this briefing.

48



Agency Comments

We received oral comments on a draft of this briefing from GSA's Associate Administrator, Office of Governmentwide Policy and from OMB's Office of General Counsel. Both GSA and OMB generally agreed with the information and conclusions presented in the draft briefing, and where appropriate, comments provided by the GSA have been addressed in the final briefing.

OMB's Office of General Counsel stated that OMB had no comment on the draft briefing.

GAO's Mission

The General Accounting Office, the audit, evaluation and 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) 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 and select "Subscribe to e-mail alerts" under the "Order GAO Products" 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
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

[redacted]