United States Government Accountability Office

GAO

Report to the Chairman, Committee on Homeland Security, House of Representatives

April 2007

INFORMATION TECHNOLOGY

Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives

GAO

Accountability ★ Integrity ★ Reliability

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-455, a report to the Chairman, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

A key challenge in securing our homeland is ensuring that critical information collected by the Department of Homeland Security (DHS) and the Department of Justice (DOJ) is shared in a timely manner with federal, state, and local governments and the private sector. It is important that federal networks and associated systems, applications, and data facilitate this vital information sharing. GAO was asked to (1) identify DHS and DOJ networks and Internet-based system applications that support homeland security and (2) determine whether DHS efforts associated with its Homeland Security Information Network are being coordinated with key state and local information-sharing initiatives. GAO assessed the coordination between DHS and two key state and local initiatives of the Regional Information Sharing System program.

What GAO Recommends

To improve coordination with state and local information sharing efforts and avoid duplication, GAO is recommending, among other things, that DHS inventory key state and local initiatives, implement coordination and collaboration practices, and ensure its efforts are consistent with the Administration's information-sharing initiative. In its written comments, DHS concurred with the above recommendations and noted actions it is taking to implement them.

www.gao.gov/cgi-bin/getrpt?GAO-07-455.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David Powner at (202) 512-9286 or pownerd@gao.gov.

April 2007

INFORMATION TECHNOLOGY

Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information Sharing Initiatives

What GAO Found

The Departments of Homeland Security and Justice have 17 major networks that support their homeland security missions, including sharing information with state and local governments. Examples include DHS's Homeland Secure Data Network and DOJ's Justice Consolidated Network. The departments also have four system applications that use the Internet. Among the four are DHS's Homeland Security Information Network—the department's primary information technology system for sharing terrorism and related information—and DOJ's Law Enforcement Online. While some networks and applications are used solely within their respective departments, others are used both within the department and by other federal, state, and local agencies and the private sector. For example, of the 17 networks, 9 are used only within their own department, and 8 are used within the department and by other federal, state, and local agencies. The reported cost to develop, operate, and maintain these networks and applications in fiscal years 2005 and 2006 was $893.1 million.

DHS is statutorily responsible for coordinating the federal government's networks and related systems with state and local governments. Federal guidance directs DHS to foster such coordination and collaboration as a means to enhance information sharing and avoid duplicative efforts. Key practices to help implement the guidance include establishing joint strategies and compatible policies and procedures to operate across agency boundaries. However, DHS did not fully adhere to these practices in coordinating efforts on its Homeland Security Information Network with key state and local information-sharing initiatives. For example, it did not work with the two key state and local information-sharing initiatives (of the Regional Information Sharing System program) to fully develop joint strategies to meet mutual needs. It also did not develop compatible policies, procedures, and other means to operate across organizational boundaries. DHS's limited use of these practices is attributable in part to the department's expediting its schedule to deploy information-sharing capabilities after September 11, 2001, and in doing so not developing an inventory of key state and local information-sharing initiatives.

DHS officials have efforts planned and under way to improve coordination and collaboration, including establishing an advisory committee to obtain state and local views on network operations. DHS also plans to coordinate its efforts with the Administration's Information Sharing Environment initiative that aims to improve information sharing among all levels of government and the private sector. However, these activities have either just begun or are being planned. Consequently, until DHS develops an inventory of key state and local initiatives and fully implements coordination and collaboration practices, it is at risk that effective information sharing is not occurring and that its Homeland Security Information Network may be duplicating state and local capabilities. This also raises the issue of whether similar coordination and duplication issues exist with the other homeland security networks, systems, and applications under DHS's purview.

Contents

Appendixes

Abbreviations

DHS	Department of Homeland Security
DOJ	Department of Justice
HSIN	Homeland Security Information Network
IT	information technology
OMB	Office of Management and Budget
RISS	Regional Information Sharing System
RISSNET	Regional Information Sharing System Secure Intranet
RISS ATIX	Regional Information Sharing System Automated Trusted Information Exchange

GAO
Accountability ★ Integrity ★ Reliability

United States Government Accountability Office
Washington, D.C. 20548

April 16, 2007

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

Dear Chairman Thompson:

One of the challenges in securing our homeland is ensuring that critical information collected and analyzed by the Department of Homeland Security (DHS) and the Department of Justice (DOJ) is shared in a timely and secure manner with a variety of parties within federal, state, and local governments, as well as the private sector. In 2005,[1] and more recently in January 2007,[2] we designated homeland security information sharing as a high-risk area. Consequently, it is important that federal networks and associated systems, applications, and data facilitate this vital information sharing, and do so in a manner that produces effective information sharing among and between the various levels of government and avoids unnecessary and duplicative efforts. This is particularly crucial for DHS's Homeland Security Information Network, which is the department's primary information technology system for sharing terrorism and related information. To address these and related information sharing challenges, the Administration, in response to congressional direction, recently issued a plan to establish, in 3 years, an Information Sharing Environment. This initiative is intended to combine policies, procedures, and networks and other technologies that link people, systems, and information among all appropriate federal, state, local, and tribal entities and the private sector.

This report responds to your request that we (1) identify existing and planned communications networks and Internet-based system applications within DHS and DOJ that support homeland security and (2) determine whether DHS efforts associated with its Homeland Security Information Network are being coordinated with key state and local information-sharing initiatives.

[1] GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

[2] GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

On January 24, 2007, we provided this briefing to House Homeland Security Committee staff. This report transmits the presentation slides we used to brief the staff and recommendations that we made to the Secretary of Homeland Security and the Director, Office of Operations Coordination, who is responsible for managing the Homeland Security Information Network program. The full briefing, including our scope and methodology, is reprinted as appendix I.

DHS and DOJ Networks and Internet-Based System Applications That Support Homeland Security

The Departments of Homeland Security and Justice have 17 major networks that they use to support their homeland security missions, including sharing information with state and local governments. Examples include DHS's Homeland Secure Data Network and DOJ's Justice Consolidated Network. The departments also have four system applications that use the Internet. Among the four are DHS's Homeland Security Information Network and DOJ's Law Enforcement Online.

The networks and system applications range from top secret to unclassified. Of the 17 federal networks, 4 are categorized as either top secret or secret, 12 are categorized as sensitive but unclassified, and 1 is unclassified. All of the four system applications are categorized as sensitive but unclassified.

While some networks and applications are used solely within their respective departments, others are used both within the department and by other federal agencies, as well as state and local governments and private sector entities. Of the 17 networks, 9 are used only within their own department, and 8 are used within the department and by other federal, state, and/or local agencies. All four of the Internet-based applications are used both within the department and by other federal agencies, as well as state and local organizations.

The total cost to develop, operate, and maintain these networks and applications in fiscal years 2005 and 2006, as reported by DHS and DOJ, was $893.1 million. Of this total, the networks accounted for the vast majority of the cost at $830.5 million.

DHS Efforts to Coordinate Its Homeland Security Information Network with Key State and Local Information-Sharing Initiatives

DHS is statutorily responsible for coordinating the federal government's networks and other communications systems, like the department's Homeland Security Information Network, with state and local governments. The Office of Management and Budget (OMB) guidance requires DHS to foster such coordination and collaboration as a means to improve government performance, including enhancing information sharing and avoiding duplication of effort. Key practices to help implement the guidance include establishing joint strategies and developing compatible policies and procedures to operate across agency boundaries.

However, DHS did not fully adhere to these practices or guidance in coordinating its efforts on the Homeland Security Information Network with key state and local information-sharing initiatives. For example, in developing the system, the department did not work with the two key state and local initiatives, which are major parts of the Regional Information Sharing System program,[3] to fully develop joint strategies to meet mutual needs. In addition, it did not develop compatible policies, procedures, and other means to operate across organizational boundaries.

DHS's limited use of these practices is attributable to a number of factors, including the department's expediting its schedule to deploy information-sharing capabilities after the events of September 11, 2001, and in doing so not developing a comprehensive inventory of key state and local information-sharing initiatives. Consequently, the department faces the risk that, among other things, effective information sharing is not occurring. It also faces the risk that the Homeland Security Information Network may be duplicating state and local capabilities.

DHS officials stated that the department has efforts planned and under way to improve coordination and collaboration. For example, it is developing an integration strategy to allow other entities' applications and networks to more easily connect with its Homeland Security Information Network. In addition, the department is establishing a Homeland Security Information Network Advisory Committee, that includes state and local officials, whose charge is to advise the department on how it can better meet user needs, including examining DHS processes for deploying the Homeland Security

[3] This program is a nationwide initiative, operated and managed by state and local officials since 1974, to share criminal intelligence among stakeholders in law enforcement, first responders, and the private sector to coordinate efforts against crime that operates across jurisdictional lines. Funding for the program is administered through federal grant money.

Information Network to the states as well as assessing what resources states already have and how DHS can leverage them. DHS also plans to coordinate its improvements efforts with the Administration's initiative to establish the Information Sharing Environment. While these are steps in the right direction, they have either just begun or are being planned, with milestones for implementation yet to be defined.

Conclusions

DHS and DOJ have a vast array of major federal networks and Internet-based applications, reported to cost almost one billion dollars over the past 2 years, that are key to these departments achieving their homeland security missions, including sharing information with state and local governments.

While DHS is responsible for coordinating these network and system efforts among federal, state, and local governments, it has not done so effectively with regard to its primary information-sharing system and two key state and local initiatives. This was due largely to the department's hasty approach to delivering needed information-sharing capabilities; in doing so, DHS did not follow key coordination and collaboration practices and guidance or invest the time to inventory and fully understand how it could leverage state and local approaches. Consequently, the department faces the risk that effective information sharing is not occurring and that its Homeland Security Information Network may be duplicating existing state and local capabilities. DHS recognizes these risks and has improvements planned and under way to address them, but it has yet to establish dates for when the improvements will be fully completed and institutionalized.

The limited use of the guidance and practices and the absence of an inventory raise doubt about whether DHS is effectively coordinating its Homeland Security Information Network efforts with all other key state and local information initiatives. DHS's activities at the state and local level also raise questions about whether it has adequately addressed coordination and duplication issues with regard to the other federal homeland security networks and associated systems and applications under the department's purview. Given what is at stake, it is extremely important that DHS authorities expeditiously address these issues and mitigate the associated risks. Further, in doing so, it is imperative to ensure that any and all efforts to address coordination issues are not done in isolation but rather in a manner that is consistent with implementation of the recently issued Information Sharing Environment plan.

Recommendations

We recommend that the Secretary of Homeland Security direct the Director, Office of Operations Coordination, to ensure that the Homeland Security Information Network efforts are effectively coordinated with key state and local government information-sharing initiatives. This should include,

- identifying existing and planned key state and local information-sharing initiatives and assessing whether there are opportunities for the program to improve information sharing and avoid duplication of effort;
- where there are opportunities, adopting and institutionalizing key practices related to OMB's guidance on enhancing and sustaining agency coordination and collaboration, including developing documented policies and procedures to operate across organizational boundaries; and
- ensuring that its coordination efforts are consistent with implementation of the Information Sharing Environment plan.

We also recommend that the Secretary of Homeland Security determine whether there are coordination and duplication issues with other homeland security networks and associated systems and applications. In each case where issues are identified, the Secretary should direct the appropriate department executive to ensure that the efforts are effectively coordinated consistent with our recommendation above.

Agency Comments and Our Evaluation

In DHS's written comments on a draft of this report, which were contained in a letter signed by the Director, Departmental GAO/Office of Inspector General Liaison, the department stated it agreed with our recommendations on identifying and inventorying key state and local initiatives, implementing coordination and collaboration practices, and ensuring its efforts are consistent with implementation of the Information Sharing Environment plan. In addition, DHS described actions it is taking to address each recommendation. However, these actions did not specifically include whether the department is to identify and inventory existing and planned key state and local information-sharing initiatives. As we stated in our briefing, without this inventory, the department will have limited knowledge of state and local initiatives and will continue to risk duplicating these capabilities.

With regard to our recommendation on determining whether coordination and duplication issues exist with other homeland security systems, DHS said that it is still taking the recommendation under advisement and plans to provide an update to appropriate congressional committees and the OMB within 60 days of our report's issuance. DHS's comments are reprinted in appendix II.

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 report date. At that time, we will send copies of this report to the Secretary of Homeland Security, the Attorney General, and the Director of OMB. Copies are also available at no charge on the GAO Web site at http://www.gao.gov.

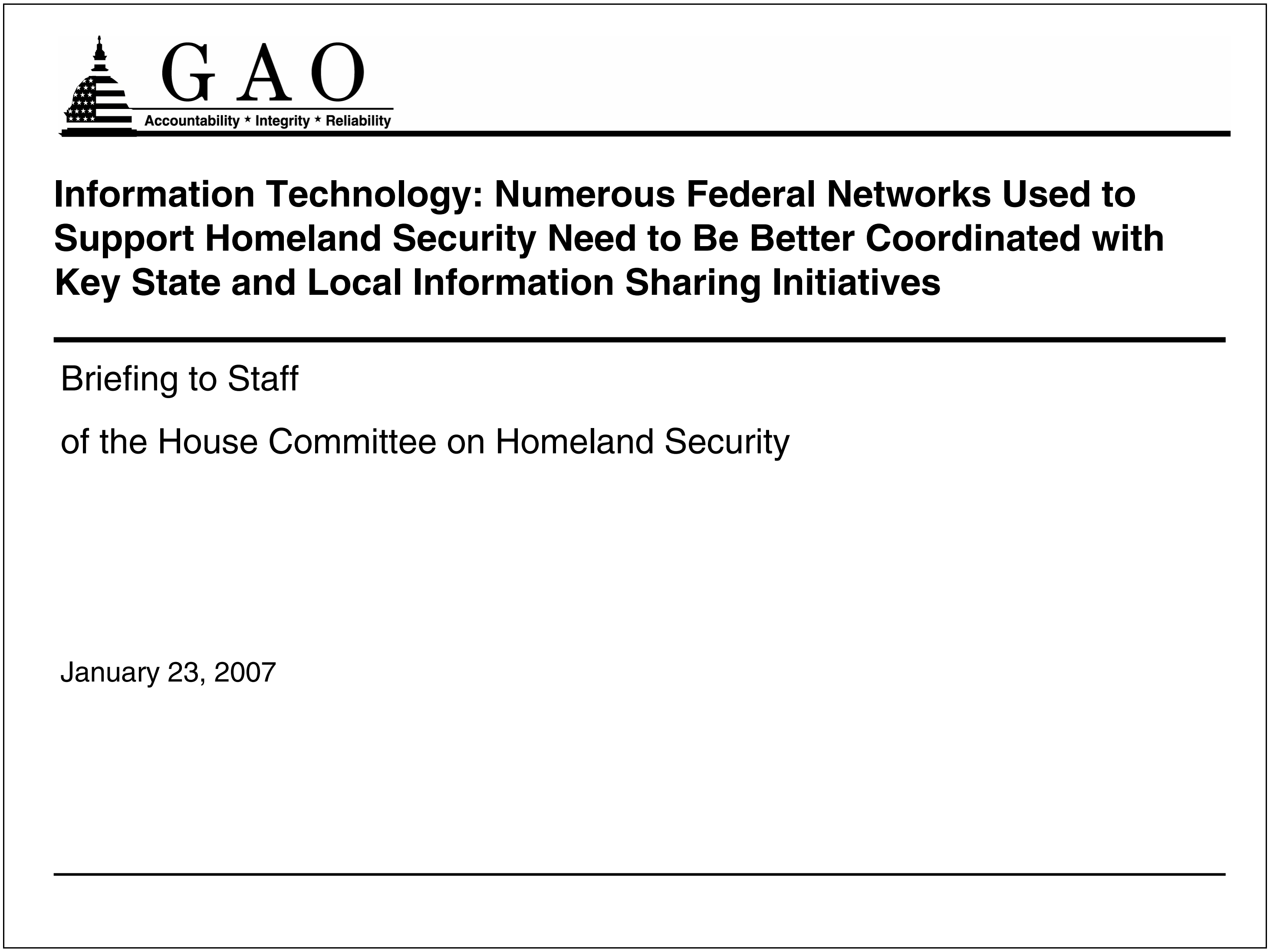
Should you or your office have questions on matters discussed in this report, please contact me at (202) 512-9286 or at pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Sincerely yours,

David A. Pow

David A. Powner
Director, Information Technology
Management Issues

Briefing Provided to Staff, House Committee on Homeland Security



GAO

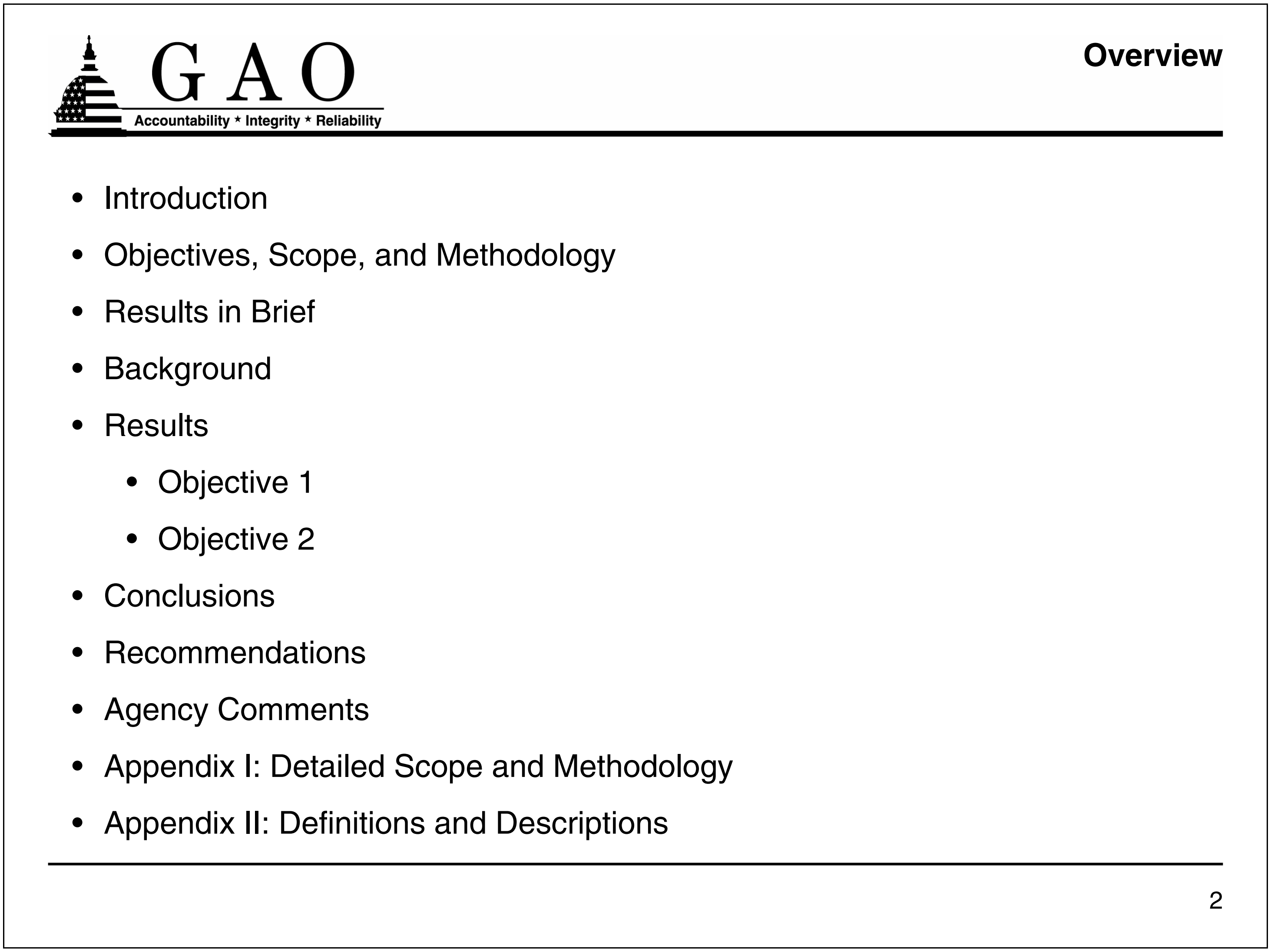
Accountability * Integrity * Reliability

Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information Sharing Initiatives

Briefing to Staff

of the House Committee on Homeland Security

January 23, 2007

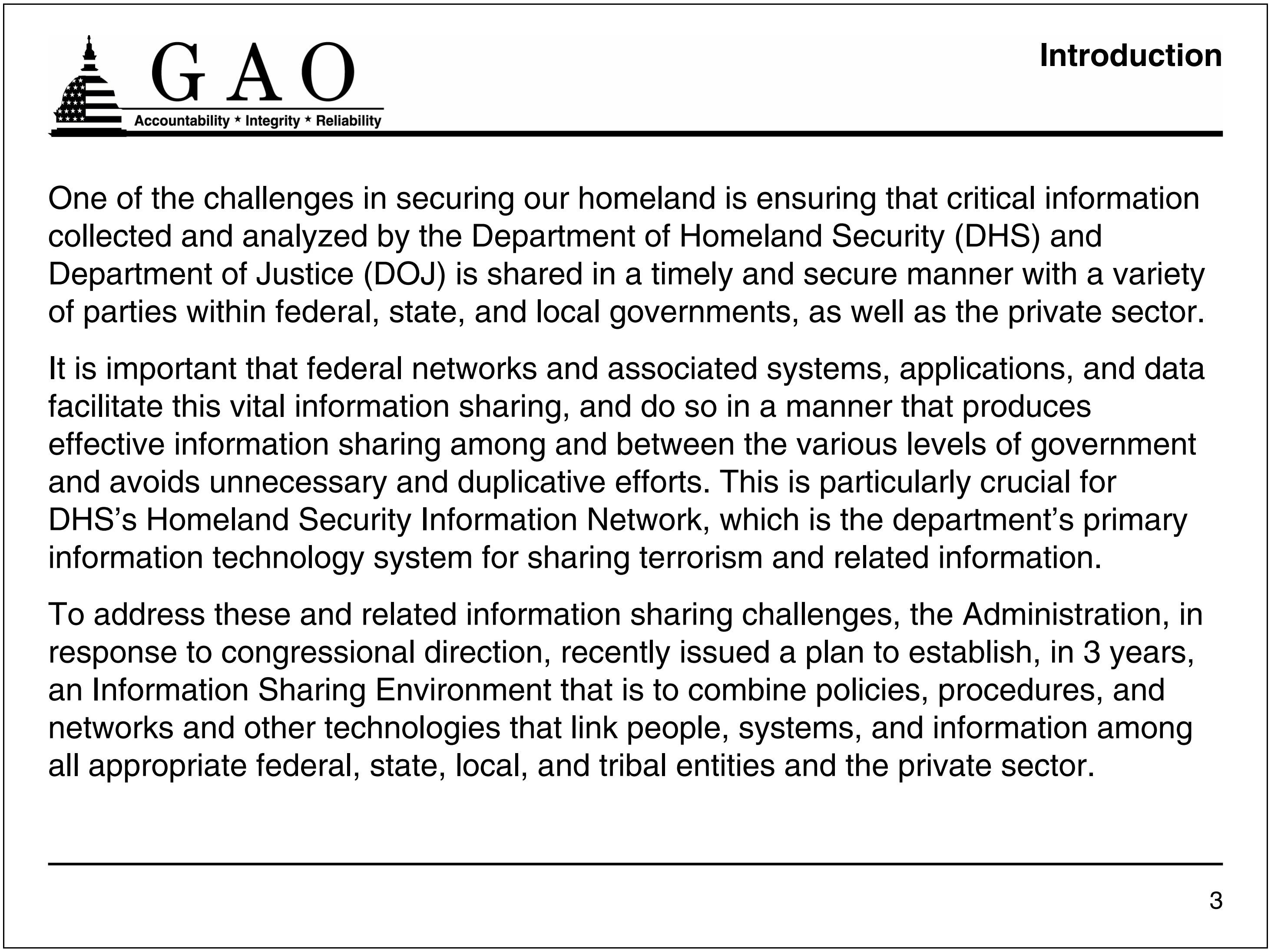


GAO
Accountability * Integrity * Reliability

Overview

- Introduction
- Objectives, Scope, and Methodology
- Results in Brief
- Background
- Results
    - Objective 1
    - Objective 2
- Conclusions
- Recommendations
- Agency Comments
- Appendix I: Detailed Scope and Methodology
- Appendix II: Definitions and Descriptions

2



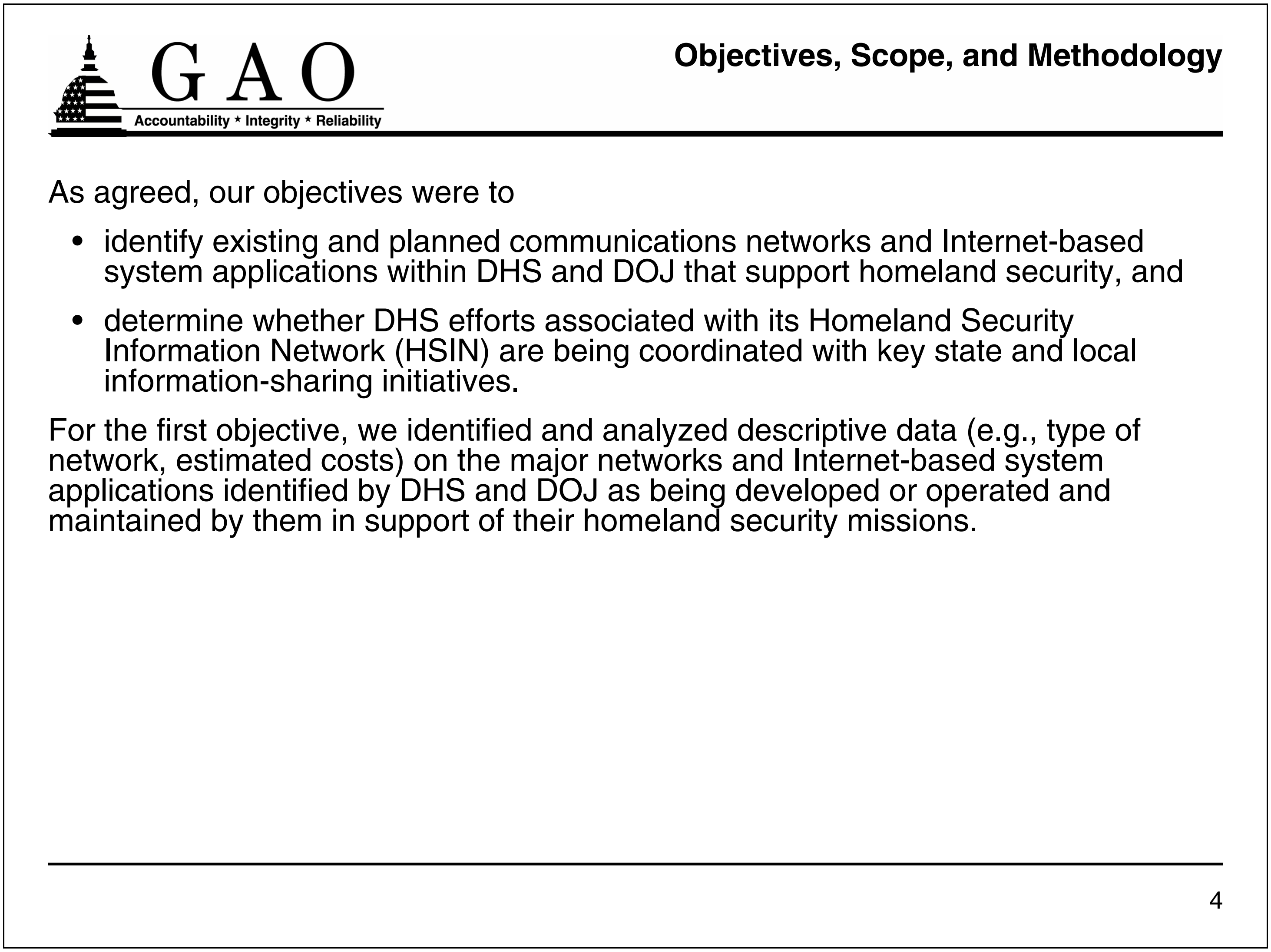
Introduction

One of the challenges in securing our homeland is ensuring that critical information collected and analyzed by the Department of Homeland Security (DHS) and Department of Justice (DOJ) is shared in a timely and secure manner with a variety of parties within federal, state, and local governments, as well as the private sector.

It is important that federal networks and associated systems, applications, and data facilitate this vital information sharing, and do so in a manner that produces effective information sharing among and between the various levels of government and avoids unnecessary and duplicative efforts. This is particularly crucial for DHS's Homeland Security Information Network, which is the department's primary information technology system for sharing terrorism and related information.

To address these and related information sharing challenges, the Administration, in response to congressional direction, recently issued a plan to establish, in 3 years, an Information Sharing Environment that is to combine policies, procedures, and networks and other technologies that link people, systems, and information among all appropriate federal, state, local, and tribal entities and the private sector.

3

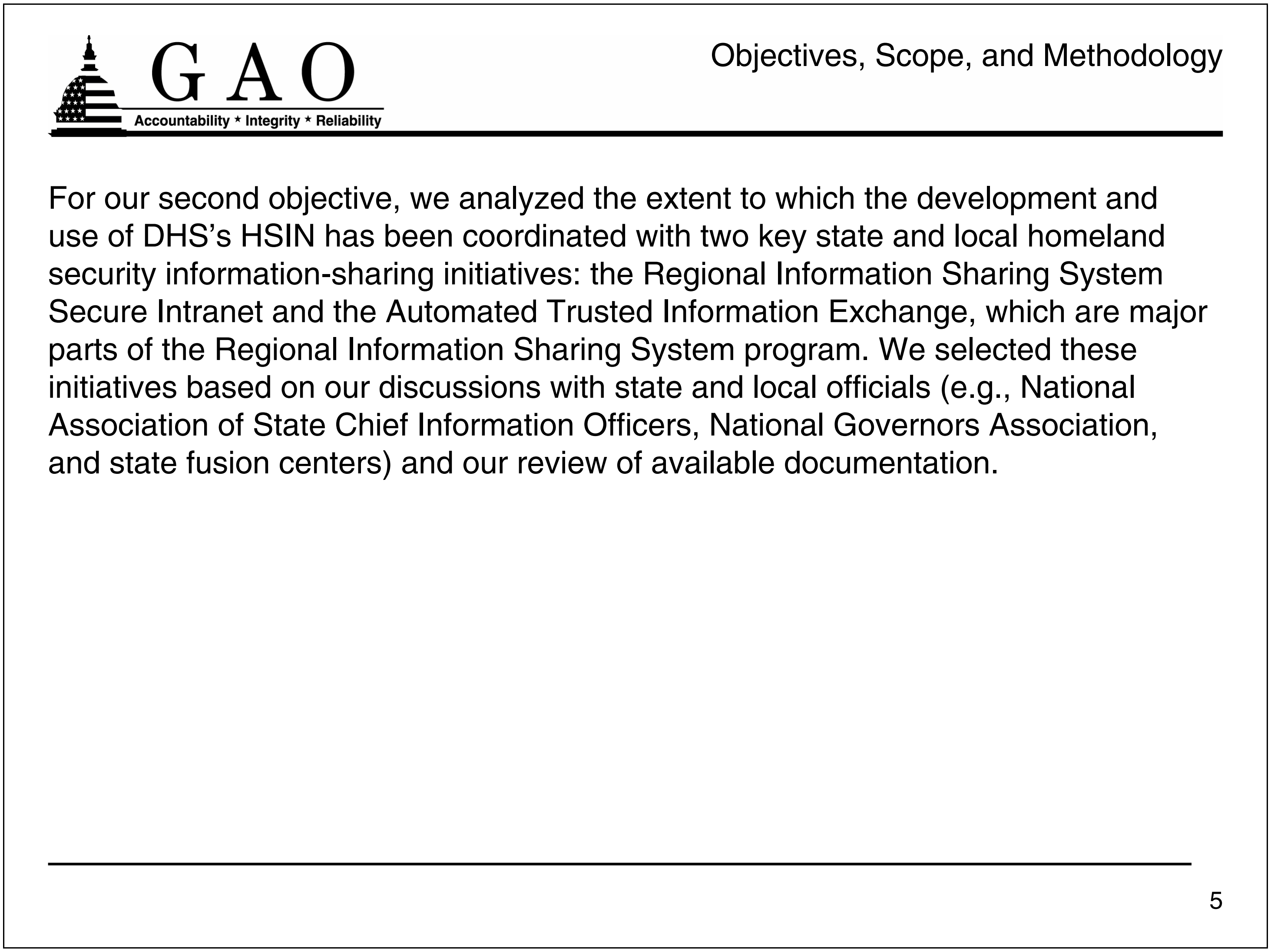


Objectives, Scope, and Methodology

As agreed, our objectives were to

- identify existing and planned communications networks and Internet-based system applications within DHS and DOJ that support homeland security, and
- determine whether DHS efforts associated with its Homeland Security Information Network (HSIN) are being coordinated with key state and local information-sharing initiatives.

For the first objective, we identified and analyzed descriptive data (e.g., type of network, estimated costs) on the major networks and Internet-based system applications identified by DHS and DOJ as being developed or operated and maintained by them in support of their homeland security missions.

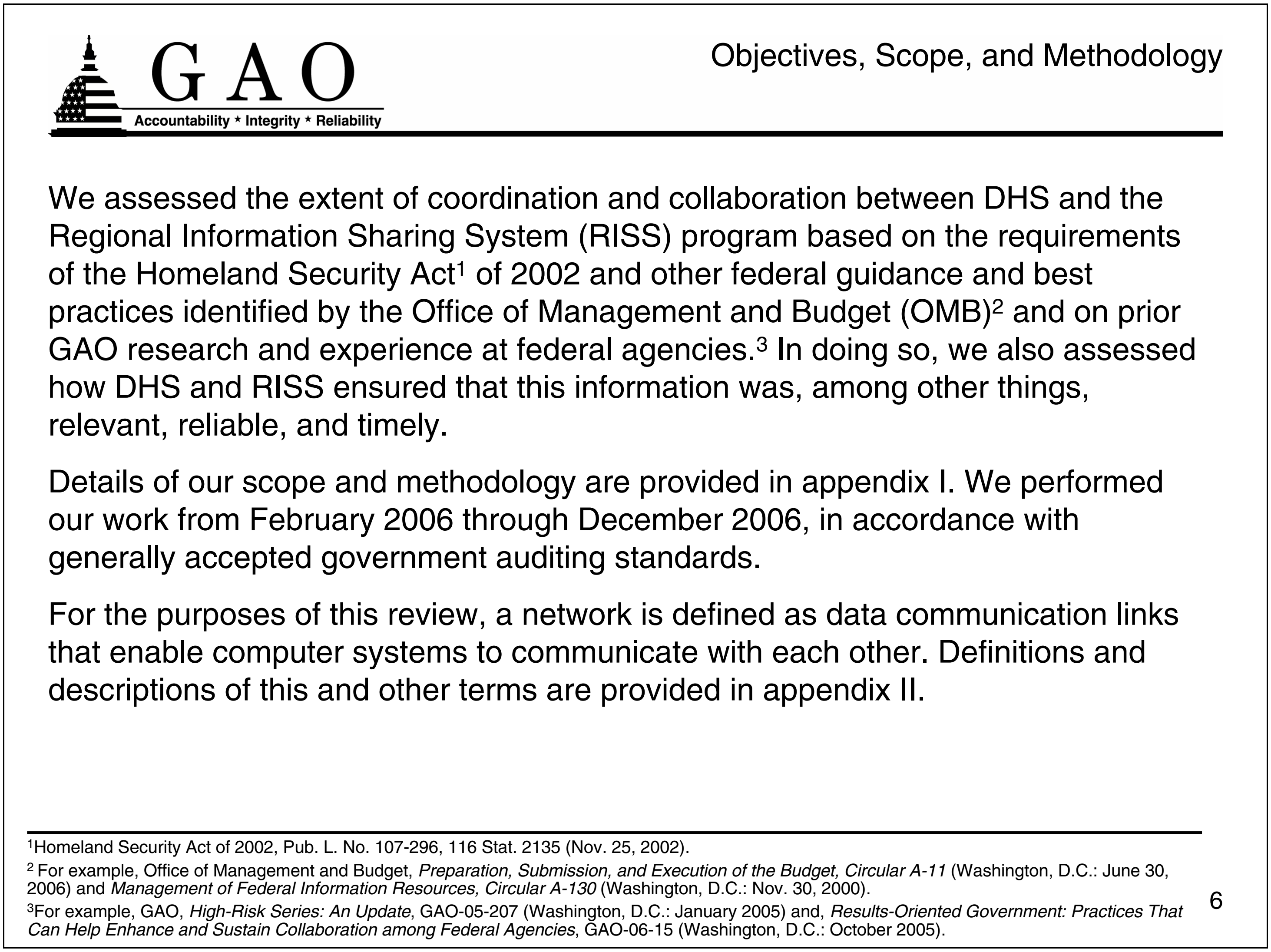


GAO
Accountability * Integrity * Reliability

Objectives, Scope, and Methodology

For our second objective, we analyzed the extent to which the development and use of DHS's HSIN has been coordinated with two key state and local homeland security information-sharing initiatives: the Regional Information Sharing System Secure Intranet and the Automated Trusted Information Exchange, which are major parts of the Regional Information Sharing System program. We selected these initiatives based on our discussions with state and local officials (e.g., National Association of State Chief Information Officers, National Governors Association, and state fusion centers) and our review of available documentation.

5



Objectives, Scope, and Methodology

We assessed the extent of coordination and collaboration between DHS and the Regional Information Sharing System (RISS) program based on the requirements of the Homeland Security Act[1] of 2002 and other federal guidance and best practices identified by the Office of Management and Budget (OMB)[2] and on prior GAO research and experience at federal agencies.[3] In doing so, we also assessed how DHS and RISS ensured that this information was, among other things, relevant, reliable, and timely.

Details of our scope and methodology are provided in appendix I. We performed our work from February 2006 through December 2006, in accordance with generally accepted government auditing standards.

For the purposes of this review, a network is defined as data communication links that enable computer systems to communicate with each other. Definitions and descriptions of this and other terms are provided in appendix II.

[1] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (Nov. 25, 2002).

[2] For example, Office of Management and Budget, *Preparation, Submission, and Execution of the Budget, Circular A-11* (Washington, D.C.: June 30, 2006) and *Management of Federal Information Resources, Circular A-130* (Washington, D.C.: Nov. 30, 2000).

[3] For example, GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005) and, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: October 2005).

6

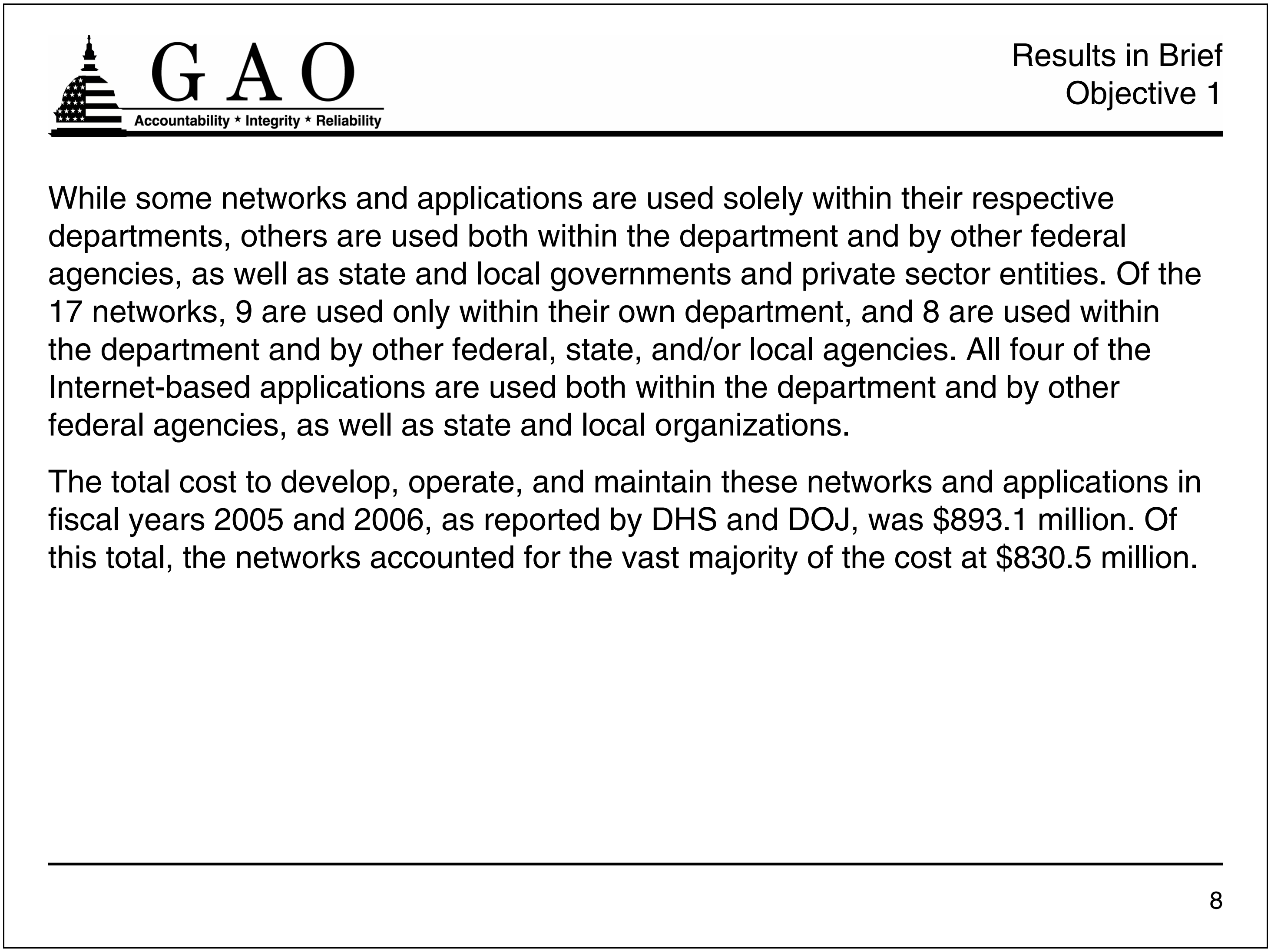
GAO
Accountability * Integrity * Reliability

Results in Brief
Objective 1

Objective 1: DHS and DOJ Have Numerous Networks and Internet-Based System Applications That Support Homeland Security

The Departments of Homeland Security and Justice have 17 major networks that they use to support their homeland security missions, including sharing information with state and local governments. Examples include DHS's Homeland Secure Data Network and DOJ's Justice Consolidated Network. The departments also have four system applications that use the Internet. Among the four are DHS's primary information-sharing system, HSIN, and DOJ's Law Enforcement Online (LEO).

The networks and system applications range from top secret to unclassified. Of the 17 federal networks, 4 are categorized as either top secret or secret, 12 are categorized as sensitive but unclassified, and 1 is unclassified. All of the four system applications are categorized as sensitive but unclassified.

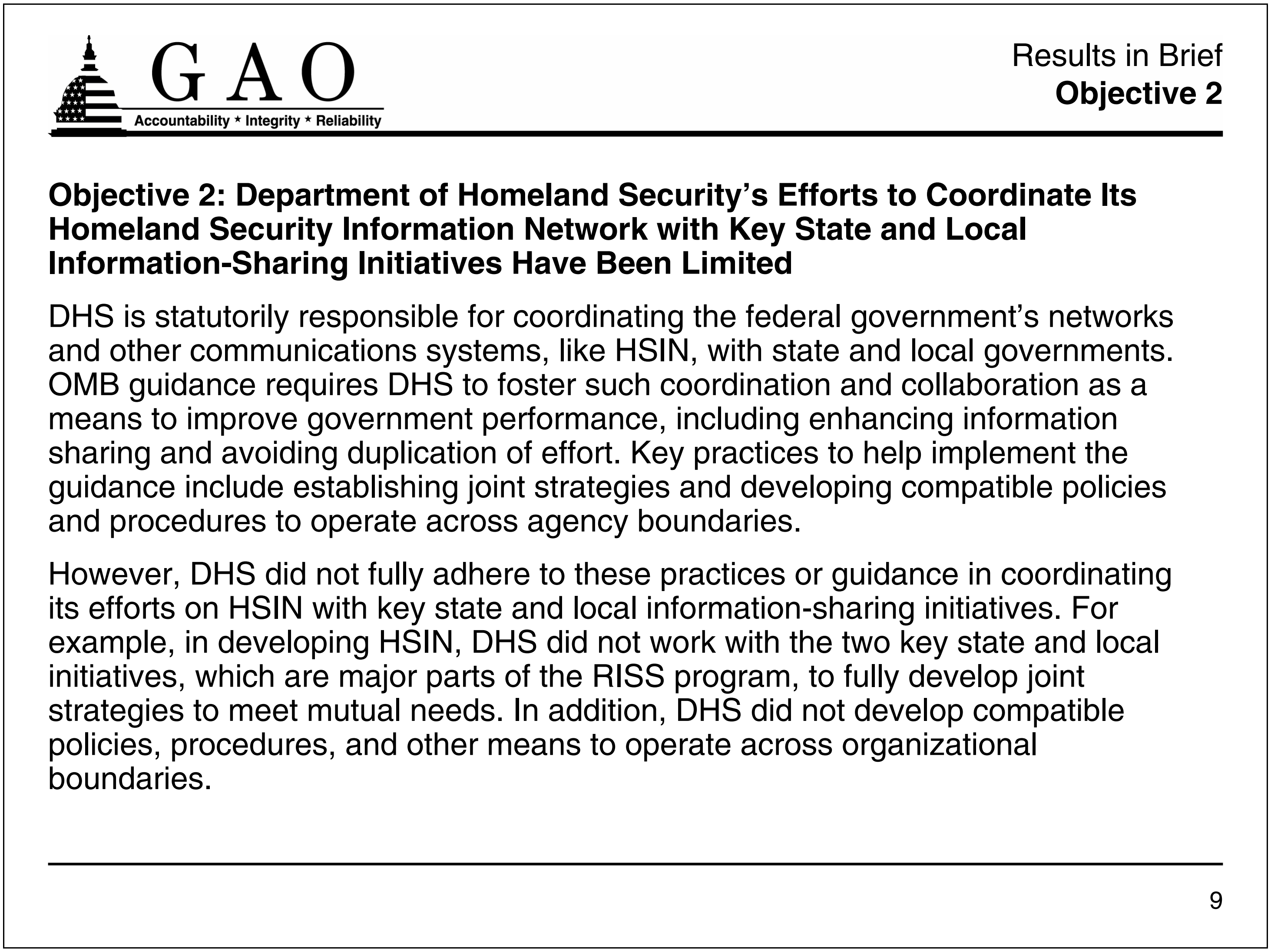


GAO
Accountability * Integrity * Reliability

Results in Brief
Objective 1

While some networks and applications are used solely within their respective departments, others are used both within the department and by other federal agencies, as well as state and local governments and private sector entities. Of the 17 networks, 9 are used only within their own department, and 8 are used within the department and by other federal, state, and/or local agencies. All four of the Internet-based applications are used both within the department and by other federal agencies, as well as state and local organizations.

The total cost to develop, operate, and maintain these networks and applications in fiscal years 2005 and 2006, as reported by DHS and DOJ, was $893.1 million. Of this total, the networks accounted for the vast majority of the cost at $830.5 million.

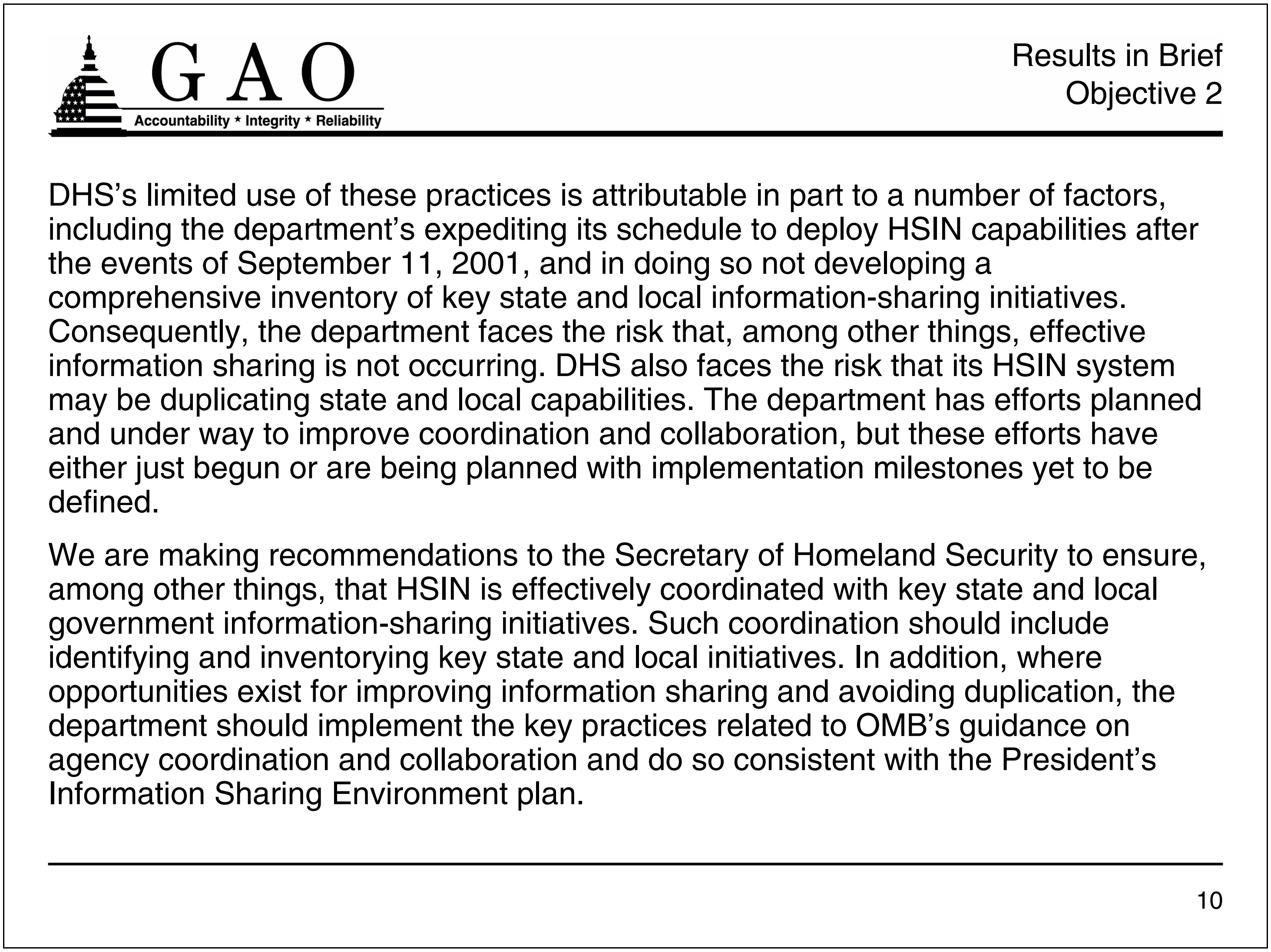


Results in Brief
Objective 2

Objective 2: Department of Homeland Security's Efforts to Coordinate Its Homeland Security Information Network with Key State and Local Information-Sharing Initiatives Have Been Limited

DHS is statutorily responsible for coordinating the federal government's networks and other communications systems, like HSIN, with state and local governments. OMB guidance requires DHS to foster such coordination and collaboration as a means to improve government performance, including enhancing information sharing and avoiding duplication of effort. Key practices to help implement the guidance include establishing joint strategies and developing compatible policies and procedures to operate across agency boundaries.

However, DHS did not fully adhere to these practices or guidance in coordinating its efforts on HSIN with key state and local information-sharing initiatives. For example, in developing HSIN, DHS did not work with the two key state and local initiatives, which are major parts of the RISS program, to fully develop joint strategies to meet mutual needs. In addition, DHS did not develop compatible policies, procedures, and other means to operate across organizational boundaries.



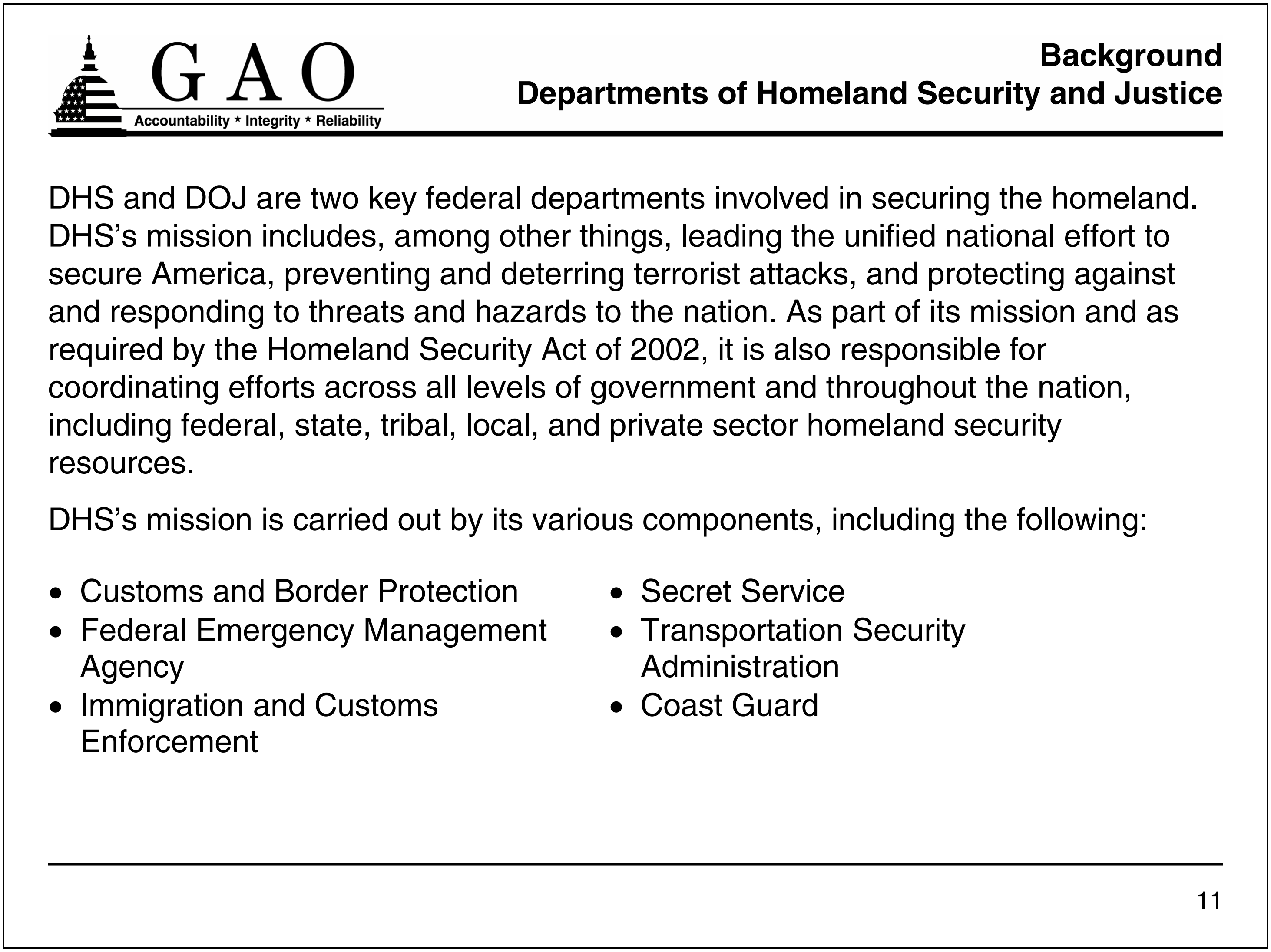
GAO
Accountability * Integrity * Reliability

Results in Brief
Objective 2

DHS’s limited use of these practices is attributable in part to a number of factors, including the department’s expediting its schedule to deploy HSIN capabilities after the events of September 11, 2001, and in doing so not developing a comprehensive inventory of key state and local information-sharing initiatives. Consequently, the department faces the risk that, among other things, effective information sharing is not occurring. DHS also faces the risk that its HSIN system may be duplicating state and local capabilities. The department has efforts planned and under way to improve coordination and collaboration, but these efforts have either just begun or are being planned with implementation milestones yet to be defined.

We are making recommendations to the Secretary of Homeland Security to ensure, among other things, that HSIN is effectively coordinated with key state and local government information-sharing initiatives. Such coordination should include identifying and inventorying key state and local initiatives. In addition, where opportunities exist for improving information sharing and avoiding duplication, the department should implement the key practices related to OMB’s guidance on agency coordination and collaboration and do so consistent with the President’s Information Sharing Environment plan.

10

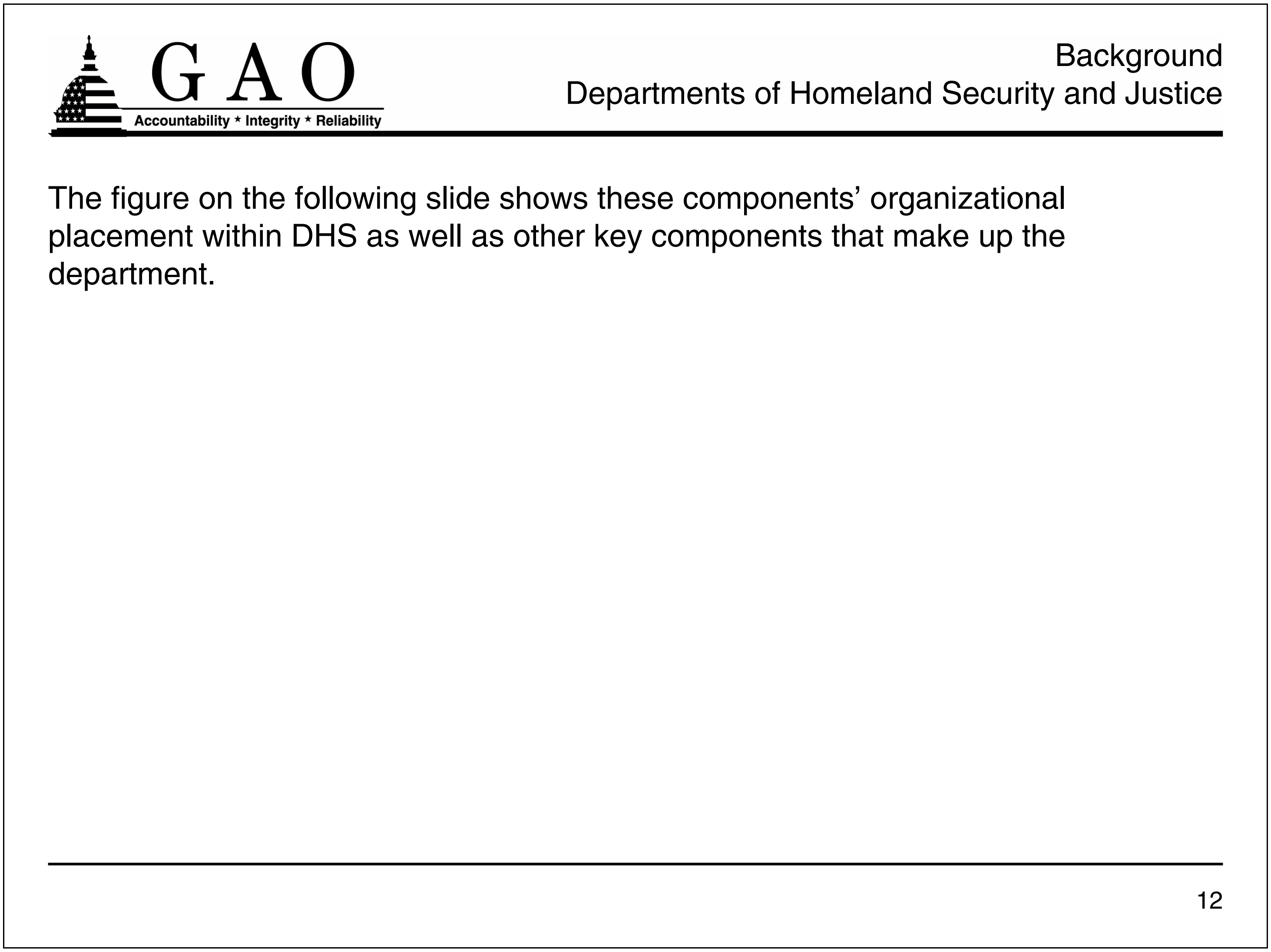


Background
Departments of Homeland Security and Justice

DHS and DOJ are two key federal departments involved in securing the homeland. DHS's mission includes, among other things, leading the unified national effort to secure America, preventing and deterring terrorist attacks, and protecting against and responding to threats and hazards to the nation. As part of its mission and as required by the Homeland Security Act of 2002, it is also responsible for coordinating efforts across all levels of government and throughout the nation, including federal, state, tribal, local, and private sector homeland security resources.

DHS's mission is carried out by its various components, including the following:

- Customs and Border Protection
- Federal Emergency Management Agency
- Immigration and Customs Enforcement
- Secret Service
- Transportation Security Administration
- Coast Guard



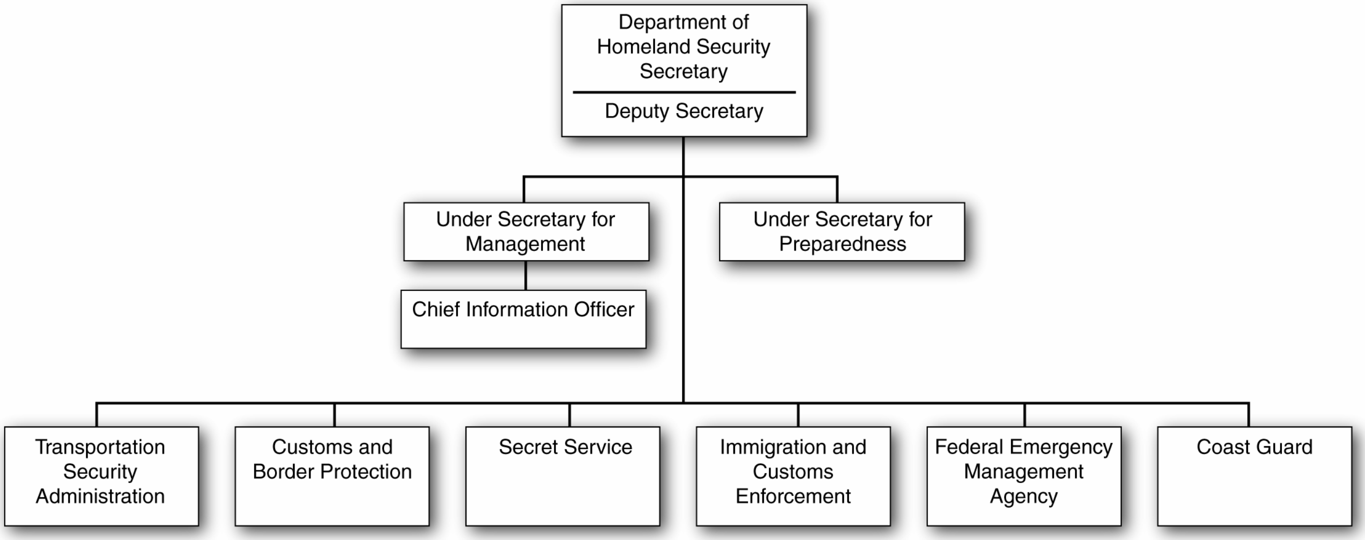
Background
Departments of Homeland Security and Justice

The figure on the following slide shows these components' organizational placement within DHS as well as other key components that make up the department.

GAO
Accountability * Integrity * Reliability

Background
Departments of Homeland Security and Justice

DHS Organizational Structure (simplified)



Department of Homeland Security Secretary

Deputy Secretary

Under Secretary for Management

Chief Information Officer

Under Secretary for Preparedness

Transportation Security Administration

Customs and Border Protection

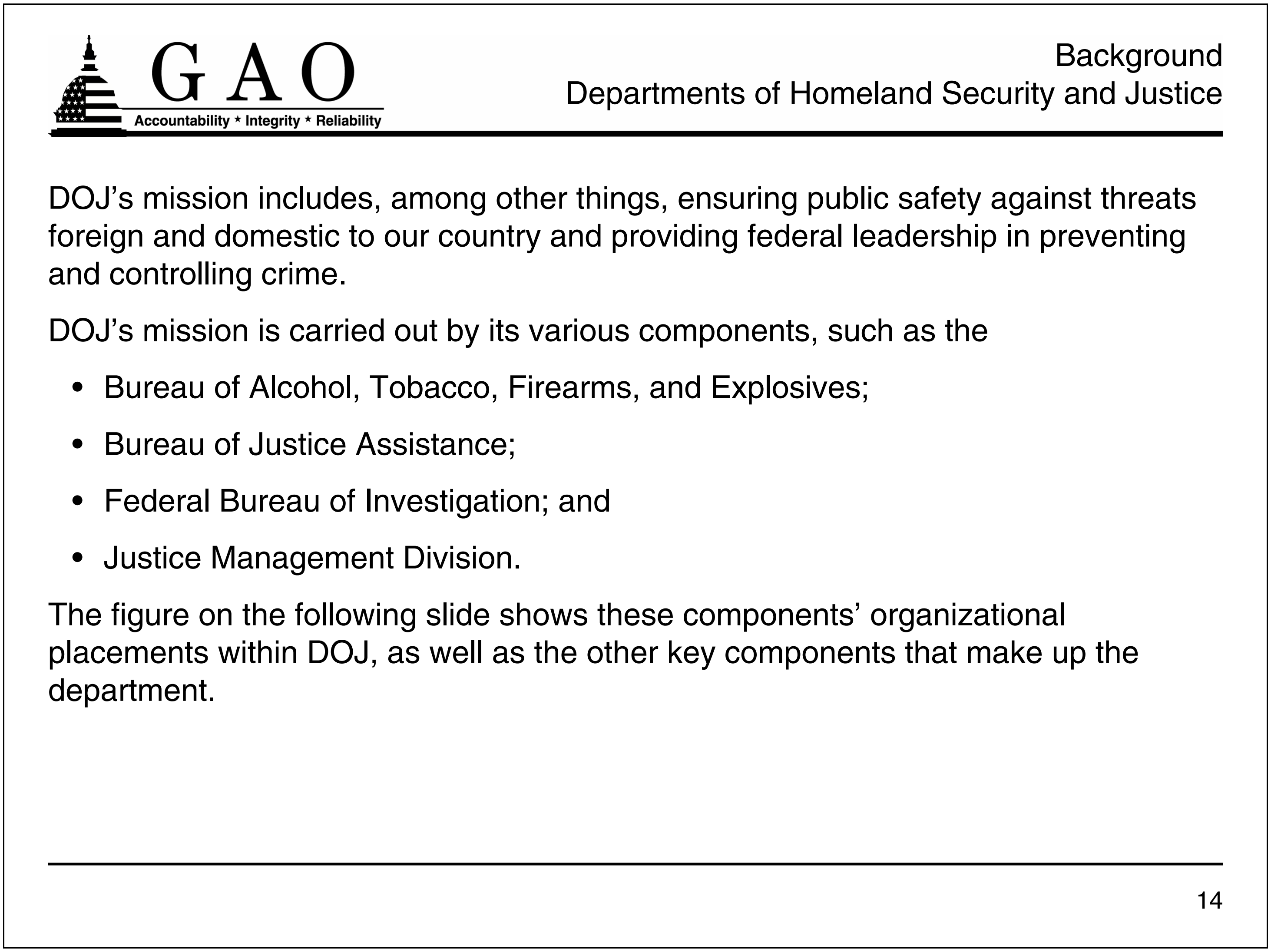
Secret Service

Immigration and Customs Enforcement

Federal Emergency Management Agency

Coast Guard

Source: GAO analysis of DHS data.



Background
Departments of Homeland Security and Justice

DOJ’s mission includes, among other things, ensuring public safety against threats foreign and domestic to our country and providing federal leadership in preventing and controlling crime.

DOJ’s mission is carried out by its various components, such as the

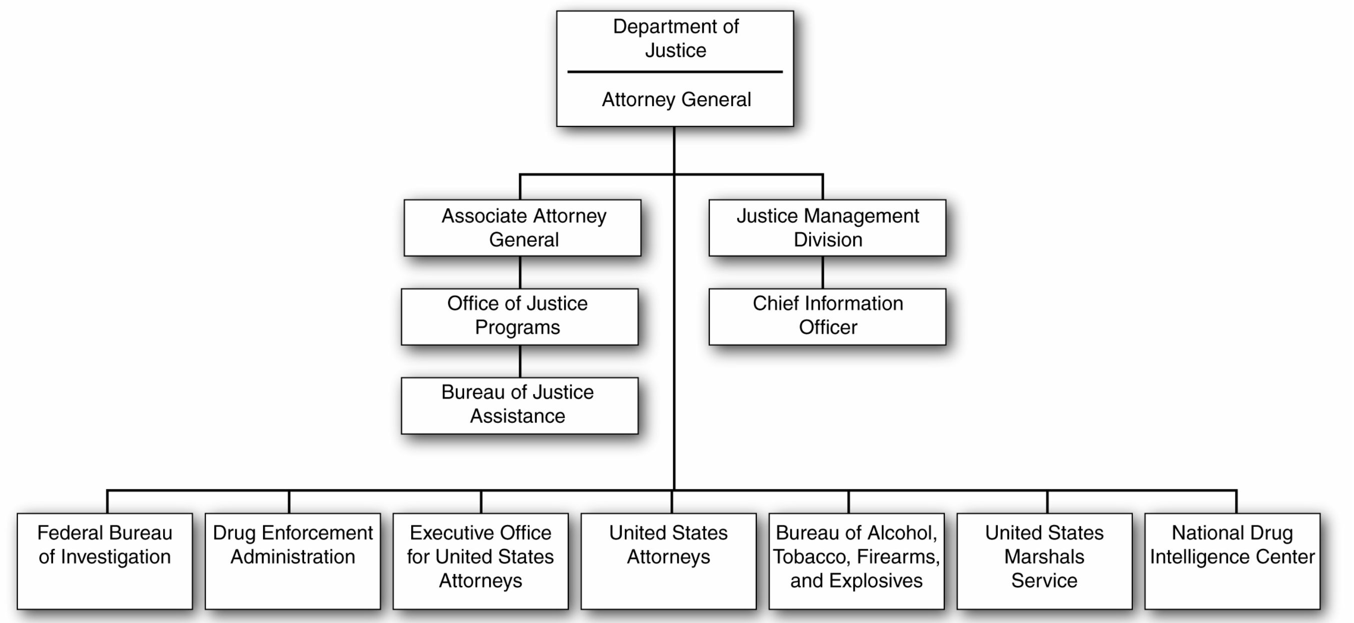
- Bureau of Alcohol, Tobacco, Firearms, and Explosives;
- Bureau of Justice Assistance;
- Federal Bureau of Investigation; and
- Justice Management Division.

The figure on the following slide shows these components’ organizational placements within DOJ, as well as the other key components that make up the department.

GAO
Accountability * Integrity * Reliability

Background
Departments of Homeland Security and Justice

DOJ Organizational Structure (simplified)



Department of Justice

Attorney General

Associate Attorney General

Office of Justice Programs

Bureau of Justice Assistance

Justice Management Division

Chief Information Officer

Federal Bureau of Investigation

Drug Enforcement Administration

Executive Office for United States Attorneys

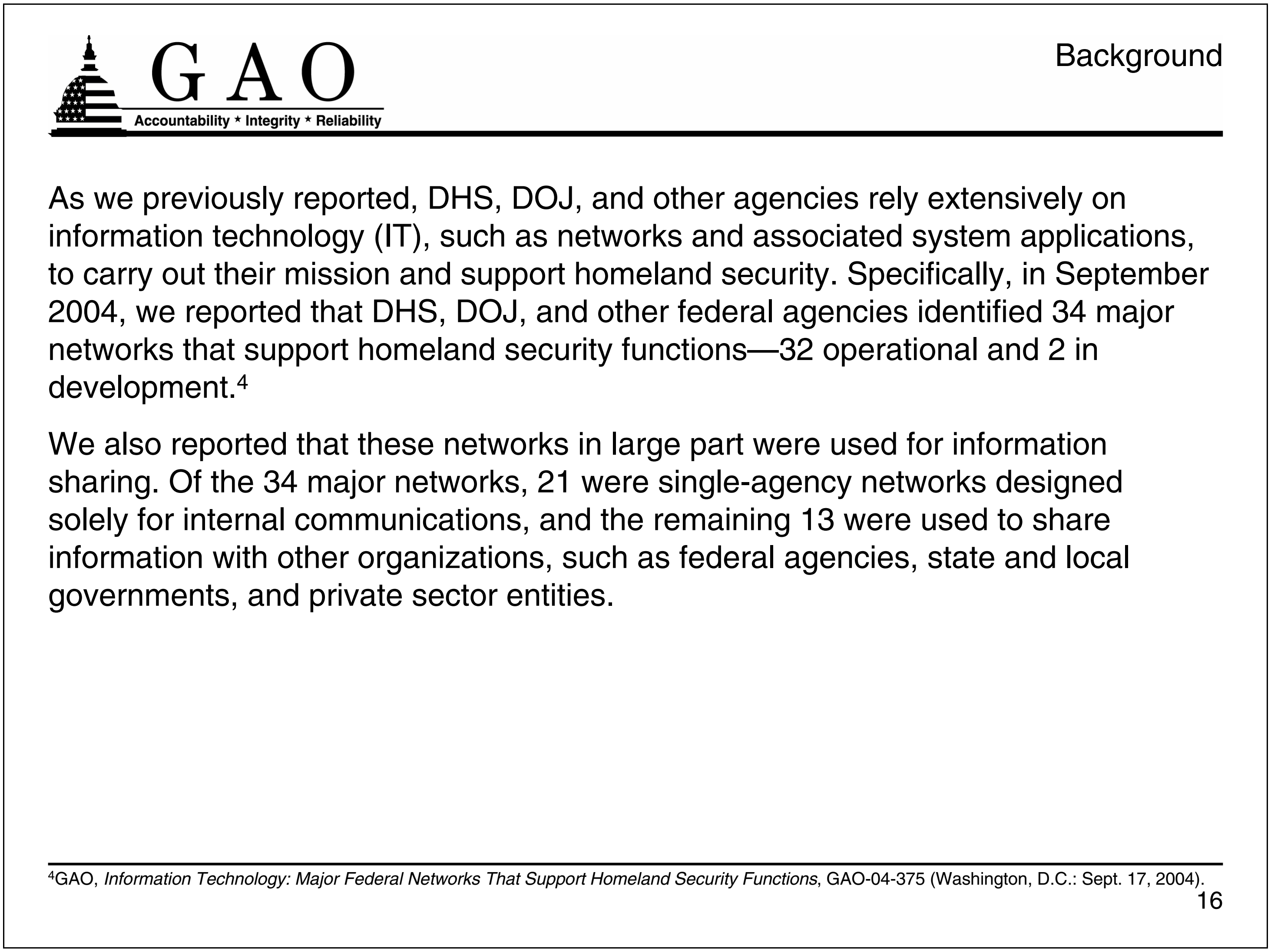
United States Attorneys

Bureau of Alcohol, Tobacco, Firearms, and Explosives

United States Marshals Service

National Drug Intelligence Center

Source: GAO analysis of DOJ data.



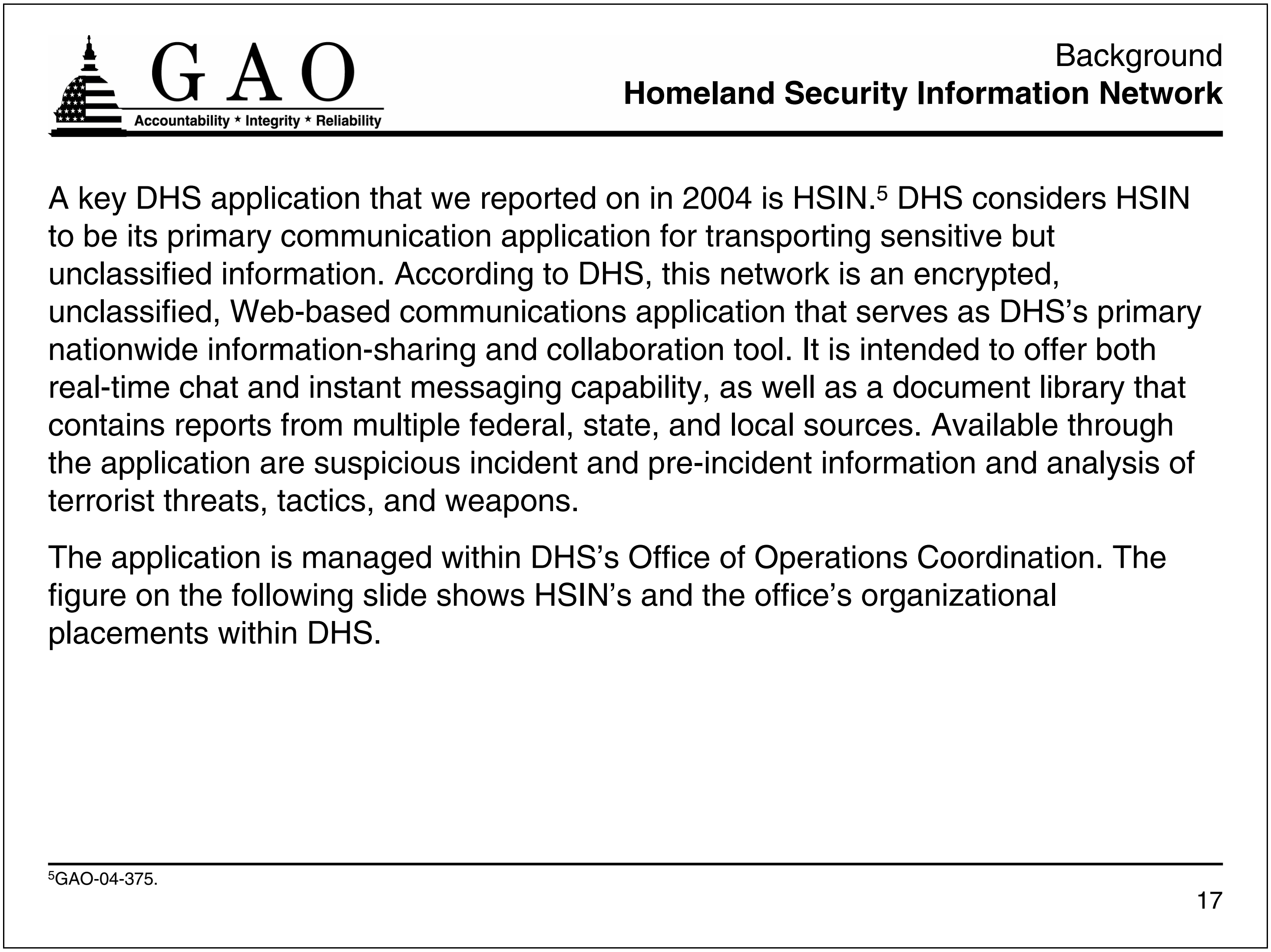
Background

As we previously reported, DHS, DOJ, and other agencies rely extensively on information technology (IT), such as networks and associated system applications, to carry out their mission and support homeland security. Specifically, in September 2004, we reported that DHS, DOJ, and other federal agencies identified 34 major networks that support homeland security functions—32 operational and 2 in development.[4]

We also reported that these networks in large part were used for information sharing. Of the 34 major networks, 21 were single-agency networks designed solely for internal communications, and the remaining 13 were used to share information with other organizations, such as federal agencies, state and local governments, and private sector entities.

[4] GAO, *Information Technology: Major Federal Networks That Support Homeland Security Functions*, GAO-04-375 (Washington, D.C.: Sept. 17, 2004).

16



GAO
Accountability * Integrity * Reliability

Background
Homeland Security Information Network

A key DHS application that we reported on in 2004 is HSIN.[5] DHS considers HSIN to be its primary communication application for transporting sensitive but unclassified information. According to DHS, this network is an encrypted, unclassified, Web-based communications application that serves as DHS's primary nationwide information-sharing and collaboration tool. It is intended to offer both real-time chat and instant messaging capability, as well as a document library that contains reports from multiple federal, state, and local sources. Available through the application are suspicious incident and pre-incident information and analysis of terrorist threats, tactics, and weapons.

The application is managed within DHS's Office of Operations Coordination. The figure on the following slide shows HSIN's and the office's organizational placements within DHS.

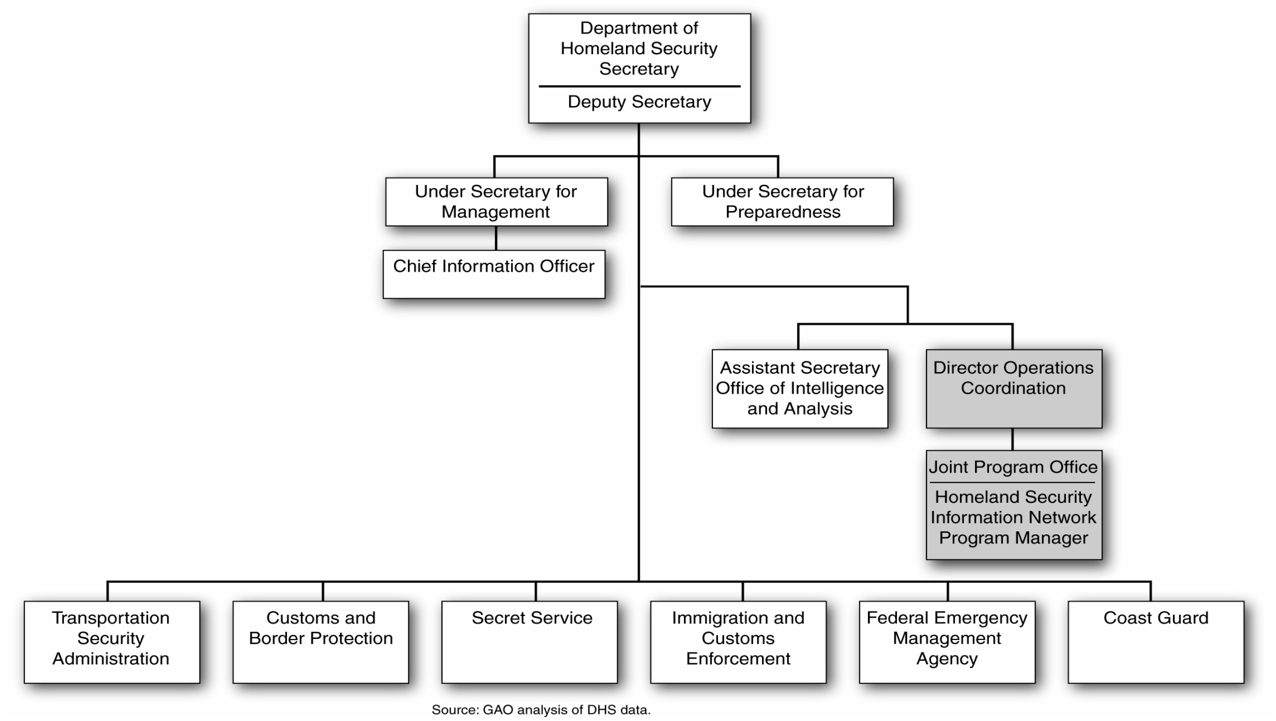
[5] GAO-04-375.

17

GAO
Accountability * Integrity * Reliability

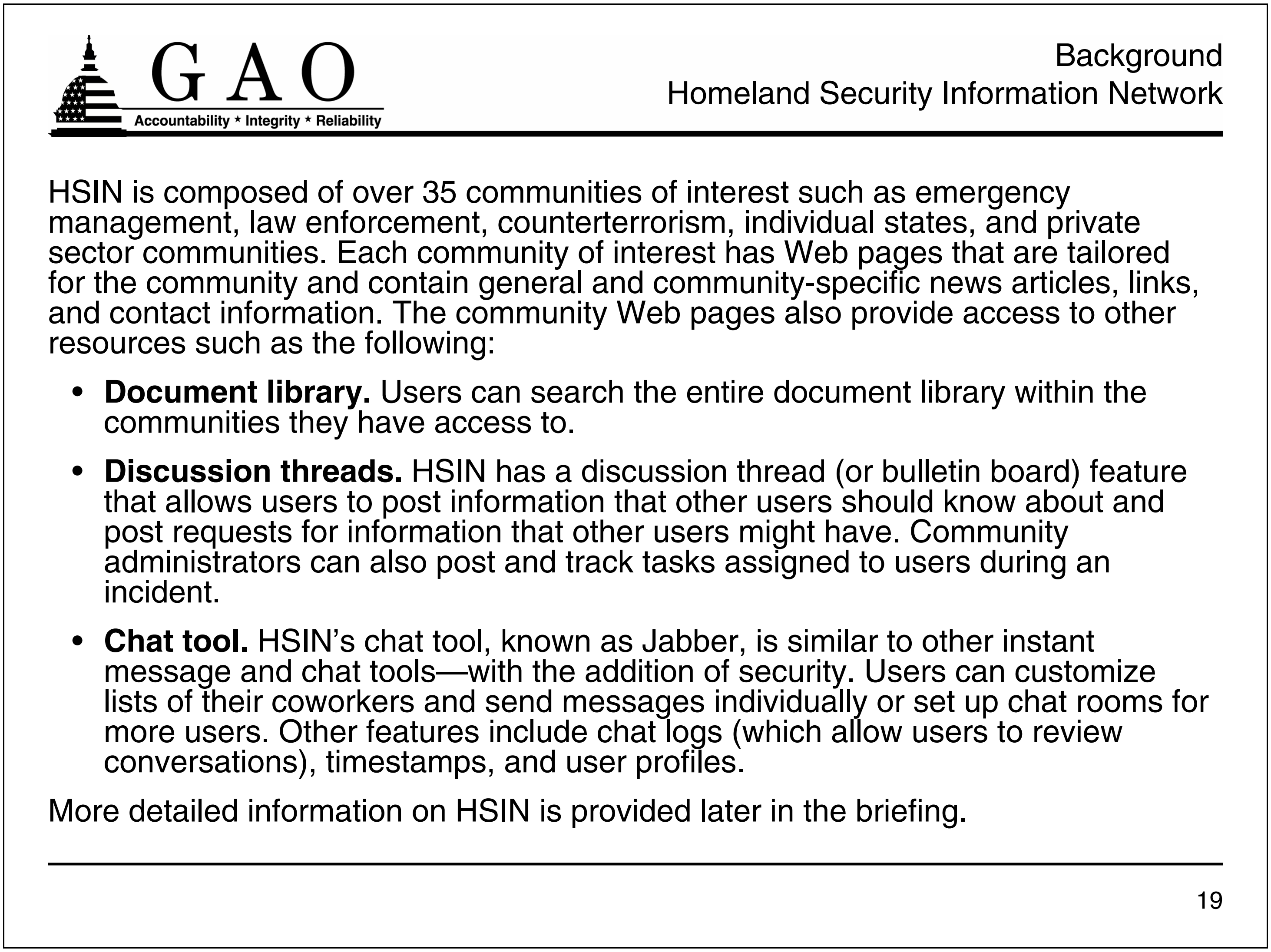
Background
Homeland Security Information Network

DHS Organizational Structure (simplified)


Department of Homeland Security Secretary
Deputy Secretary
Under Secretary for Management
Under Secretary for Preparedness
Chief Information Officer
Assistant Secretary Office of Intelligence and Analysis
Director Operations Coordination
Joint Program Office
Homeland Security Information Network Program Manager
Transportation Security Administration
Customs and Border Protection
Secret Service
Immigration and Customs Enforcement
Federal Emergency Management Agency
Coast Guard

Source: GAO analysis of DHS data.

18



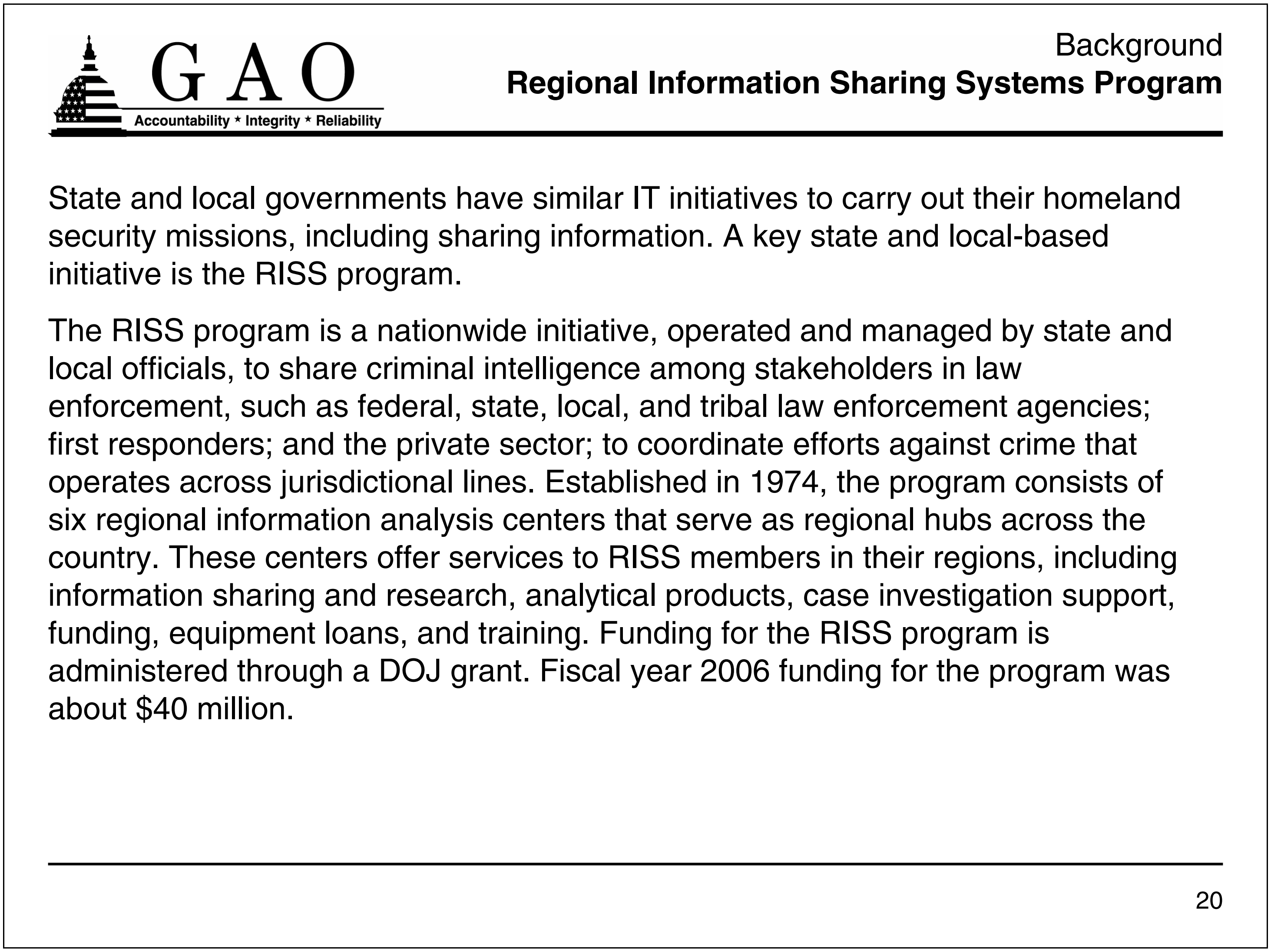
Background
Homeland Security Information Network

HSIN is composed of over 35 communities of interest such as emergency management, law enforcement, counterterrorism, individual states, and private sector communities. Each community of interest has Web pages that are tailored for the community and contain general and community-specific news articles, links, and contact information. The community Web pages also provide access to other resources such as the following:

- **Document library.** Users can search the entire document library within the communities they have access to.
- **Discussion threads.** HSIN has a discussion thread (or bulletin board) feature that allows users to post information that other users should know about and post requests for information that other users might have. Community administrators can also post and track tasks assigned to users during an incident.
- **Chat tool.** HSIN's chat tool, known as Jabber, is similar to other instant message and chat tools—with the addition of security. Users can customize lists of their coworkers and send messages individually or set up chat rooms for more users. Other features include chat logs (which allow users to review conversations), timestamps, and user profiles.

More detailed information on HSIN is provided later in the briefing.

19



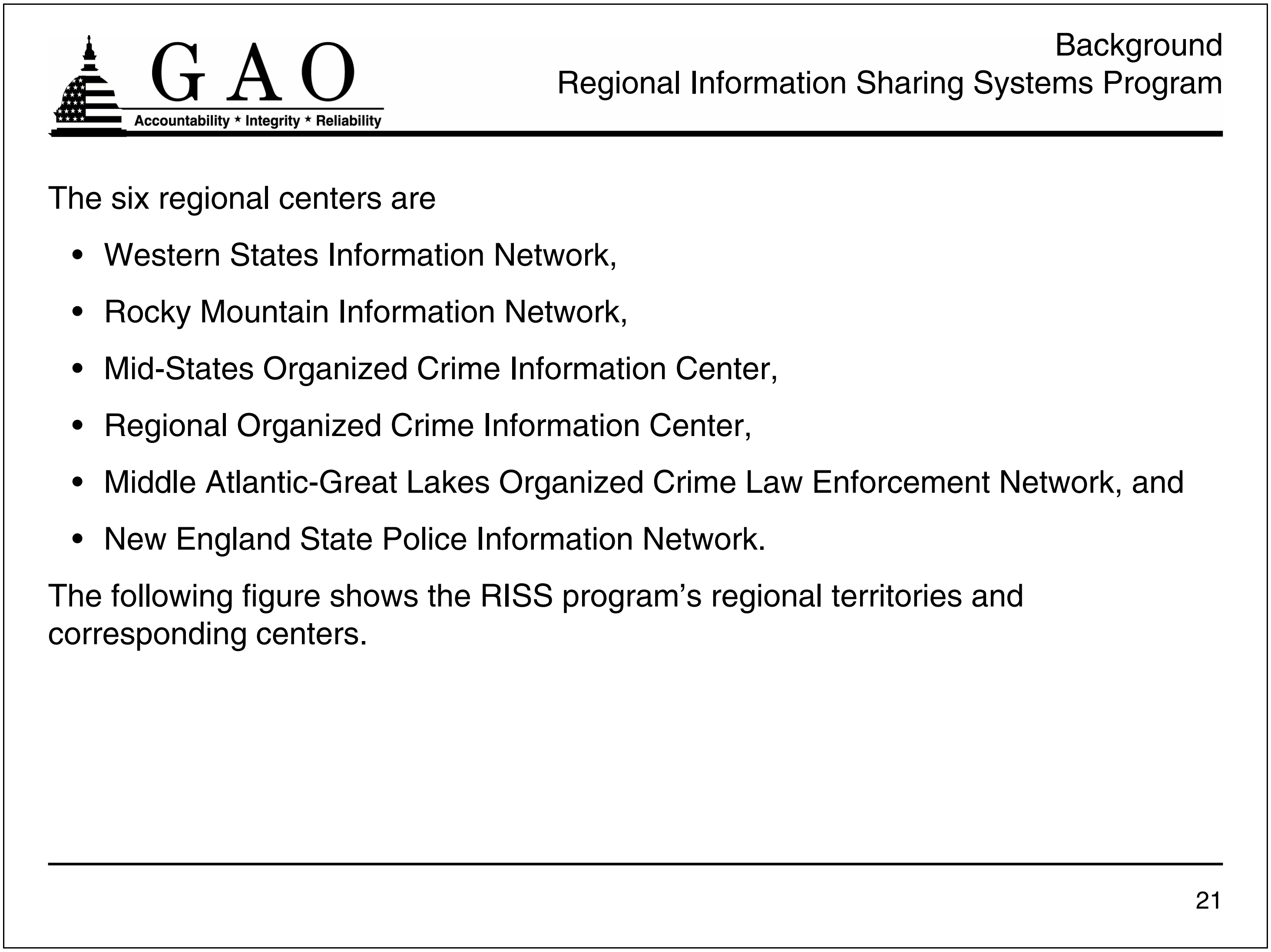
Background

Regional Information Sharing Systems Program

State and local governments have similar IT initiatives to carry out their homeland security missions, including sharing information. A key state and local-based initiative is the RISS program.

The RISS program is a nationwide initiative, operated and managed by state and local officials, to share criminal intelligence among stakeholders in law enforcement, such as federal, state, local, and tribal law enforcement agencies; first responders; and the private sector; to coordinate efforts against crime that operates across jurisdictional lines. Established in 1974, the program consists of six regional information analysis centers that serve as regional hubs across the country. These centers offer services to RISS members in their regions, including information sharing and research, analytical products, case investigation support, funding, equipment loans, and training. Funding for the RISS program is administered through a DOJ grant. Fiscal year 2006 funding for the program was about $40 million.

20



Background
Regional Information Sharing Systems Program

The six regional centers are

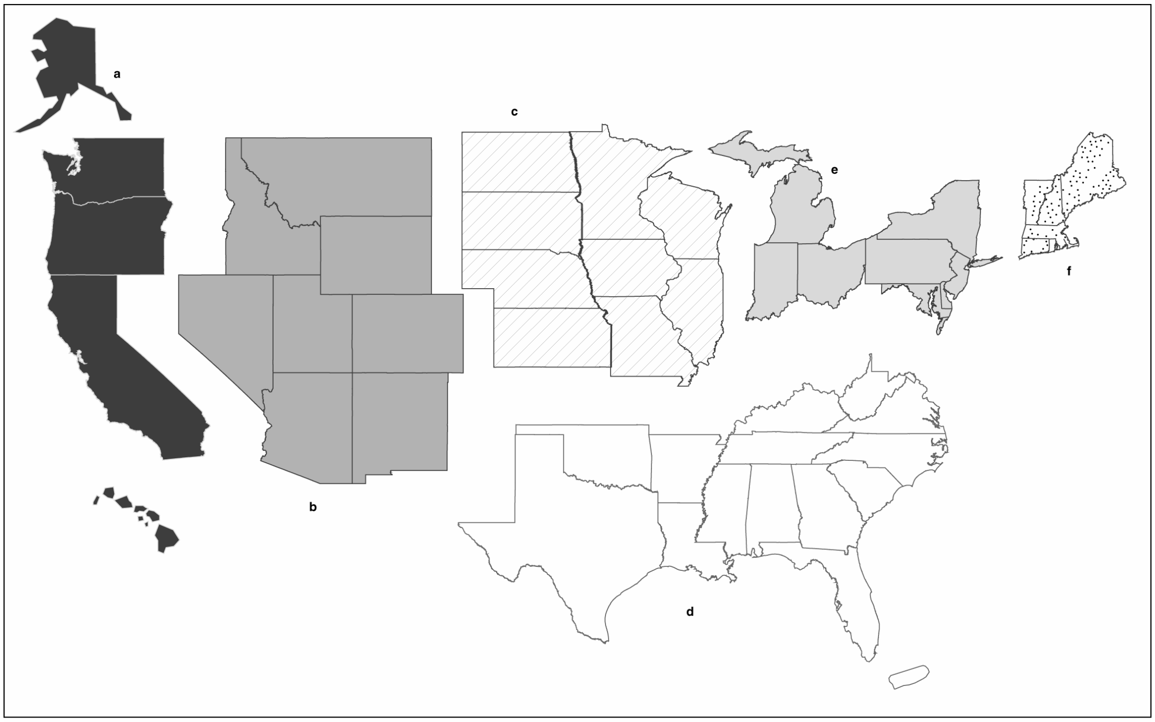
- Western States Information Network,
- Rocky Mountain Information Network,
- Mid-States Organized Crime Information Center,
- Regional Organized Crime Information Center,
- Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network, and
- New England State Police Information Network.

The following figure shows the RISS program's regional territories and corresponding centers.

GAO
Accountability * Integrity * Reliability

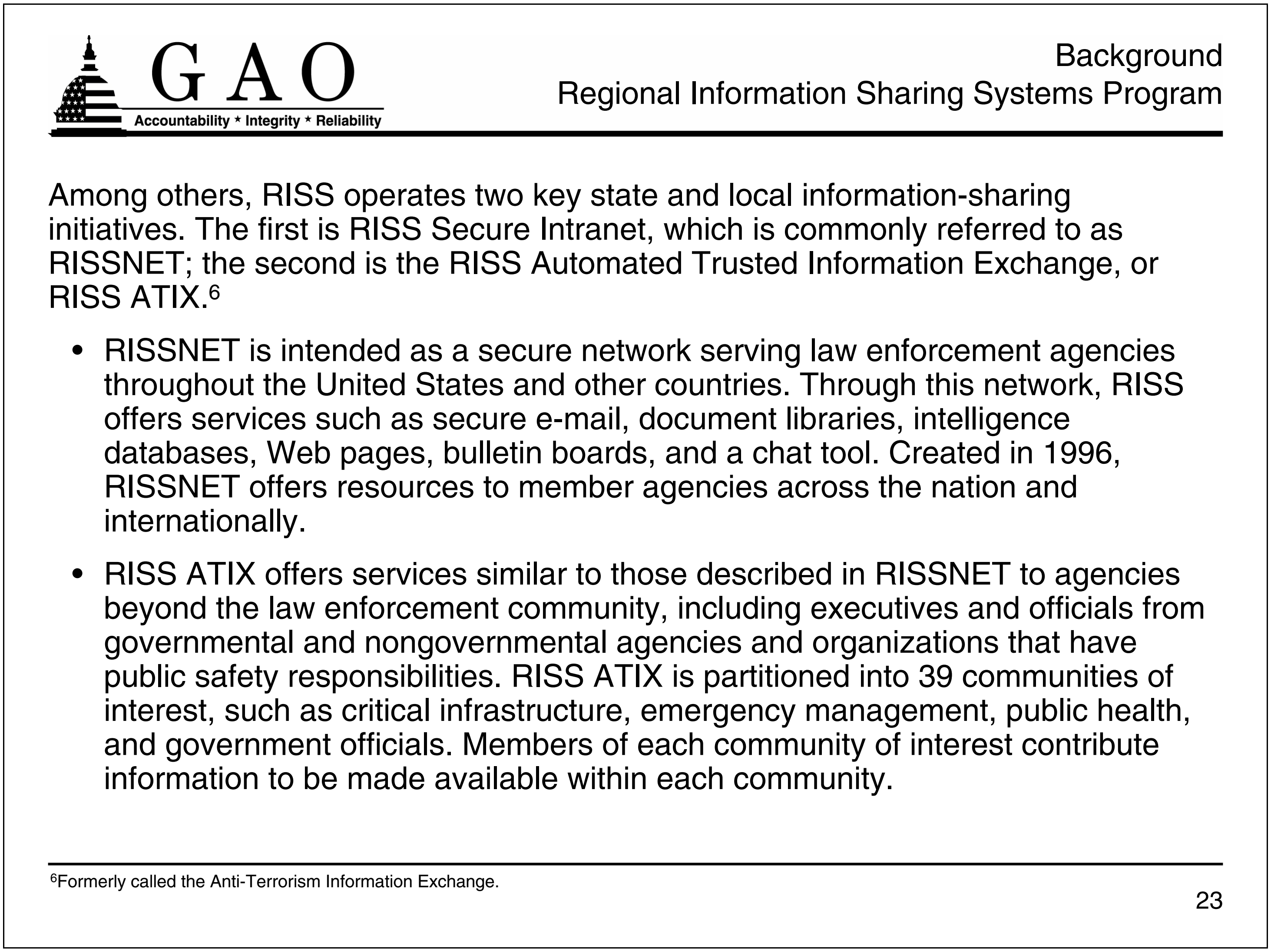
Background
Regional Information Sharing Systems Program

RISS Jurisdictional Map



Sources: RISS and Map Resources (map).

[a] Western States Information Network.
[b] Rocky Mountain Information Network.
[c] Mid-States Organized Crime Information Center.
[d] Regional Organized Crime Information Center.
[e] Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network.
[f] New England State Police Information Network.



GAO
Accountability * Integrity * Reliability

Background
Regional Information Sharing Systems Program

Among others, RISS operates two key state and local information-sharing initiatives. The first is RISS Secure Intranet, which is commonly referred to as RISSNET; the second is the RISS Automated Trusted Information Exchange, or RISS ATIX.[6]

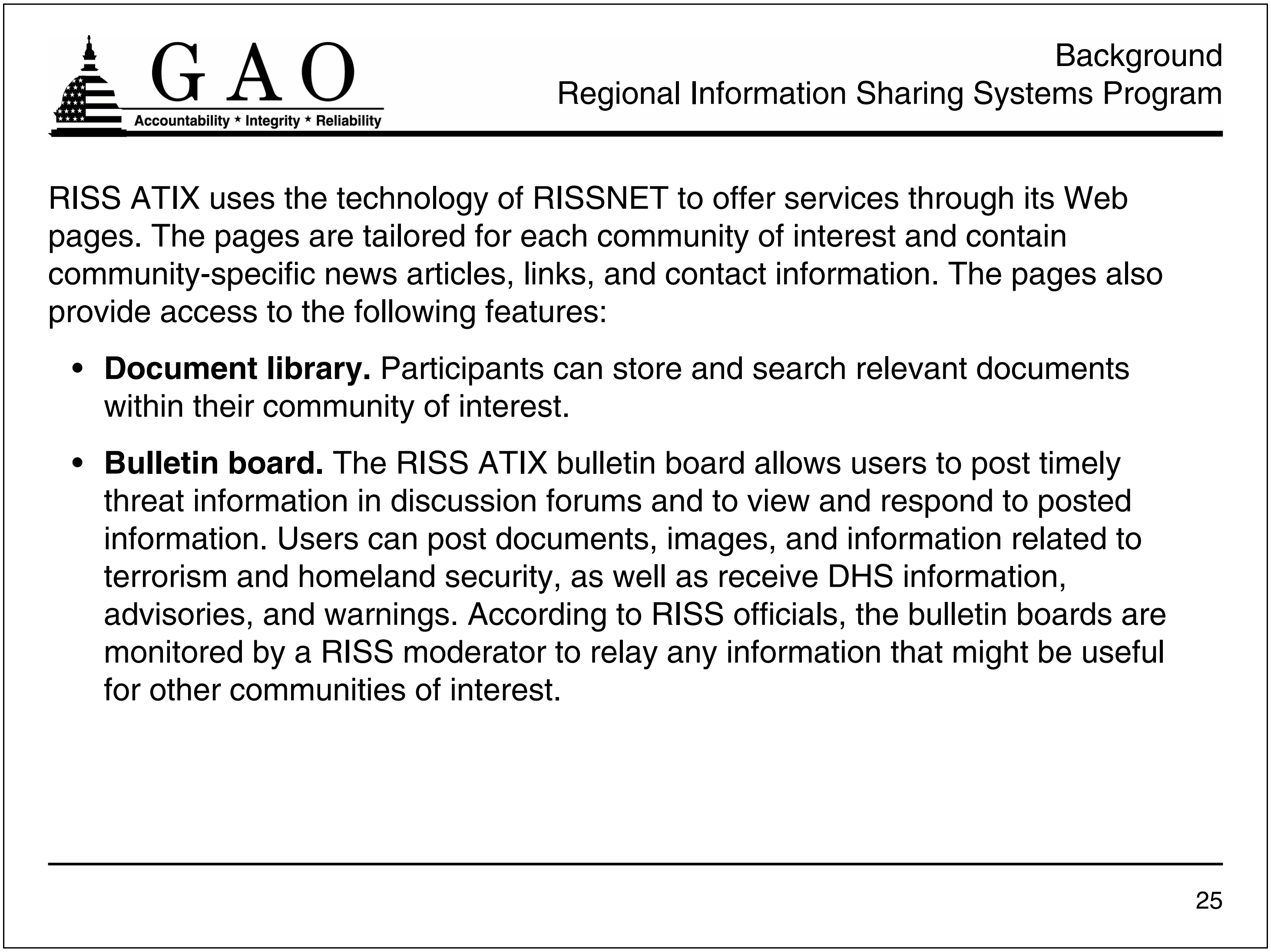
- RISSNET is intended as a secure network serving law enforcement agencies throughout the United States and other countries. Through this network, RISS offers services such as secure e-mail, document libraries, intelligence databases, Web pages, bulletin boards, and a chat tool. Created in 1996, RISSNET offers resources to member agencies across the nation and internationally.
- RISS ATIX offers services similar to those described in RISSNET to agencies beyond the law enforcement community, including executives and officials from governmental and nongovernmental agencies and organizations that have public safety responsibilities. RISS ATIX is partitioned into 39 communities of interest, such as critical infrastructure, emergency management, public health, and government officials. Members of each community of interest contribute information to be made available within each community.

[6] Formerly called the Anti-Terrorism Information Exchange.

GAO
Accountability * Integrity * Reliability

Background
Regional Information Sharing Systems Program

According to RISS officials, the RISS ATIX application was developed in response to the events of September 11, 2001, and initiated in 2002 as an application to provide tools for information sharing and collaboration among public safety stakeholders, such as first responders and schools. As of July 2006, RISS ATIX supported 1,922 users beyond the traditional users of RISSNET.

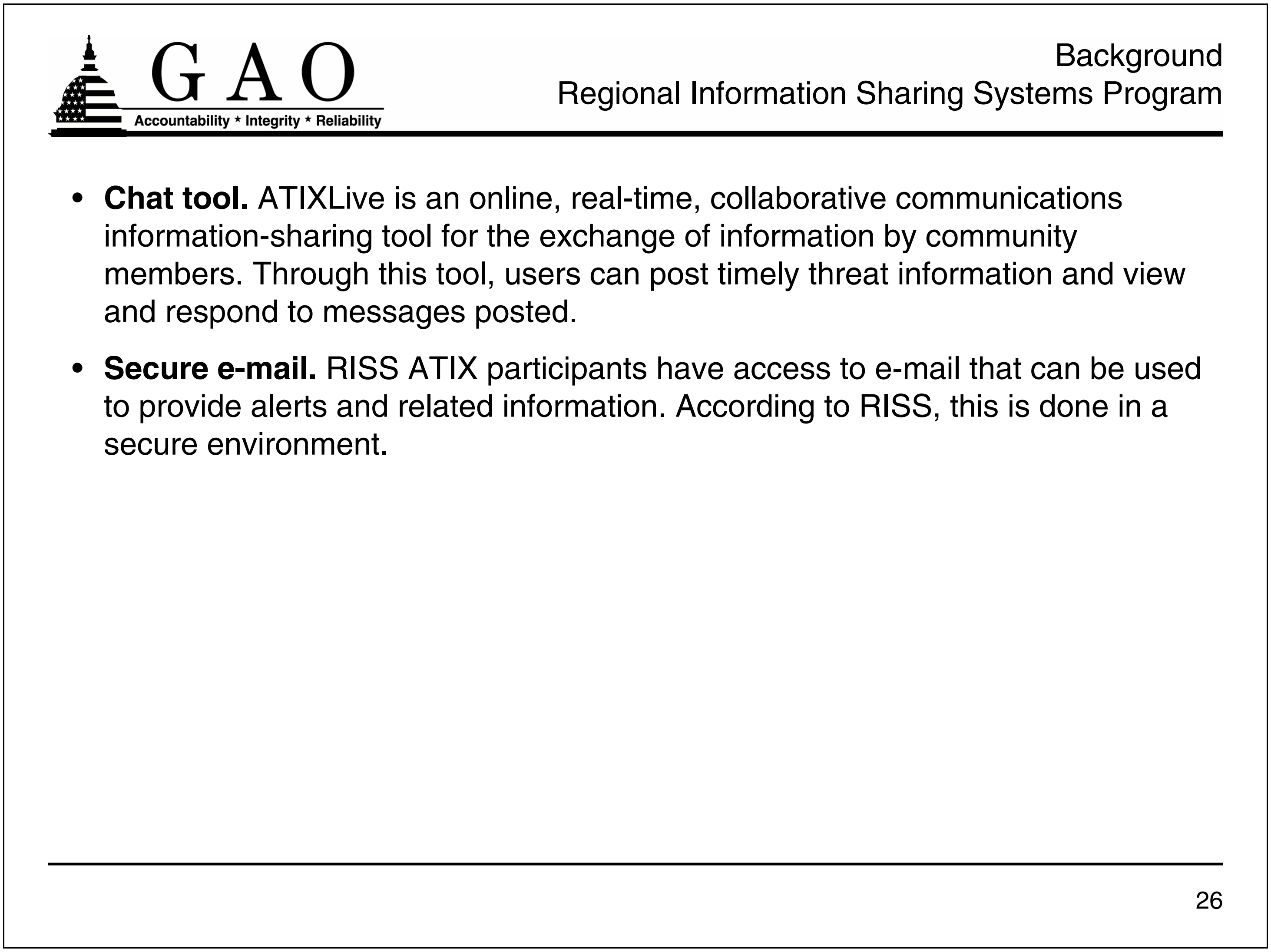


GAO
Accountability * Integrity * Reliability

Background
Regional Information Sharing Systems Program

RISS ATIX uses the technology of RISSNET to offer services through its Web pages. The pages are tailored for each community of interest and contain community-specific news articles, links, and contact information. The pages also provide access to the following features:

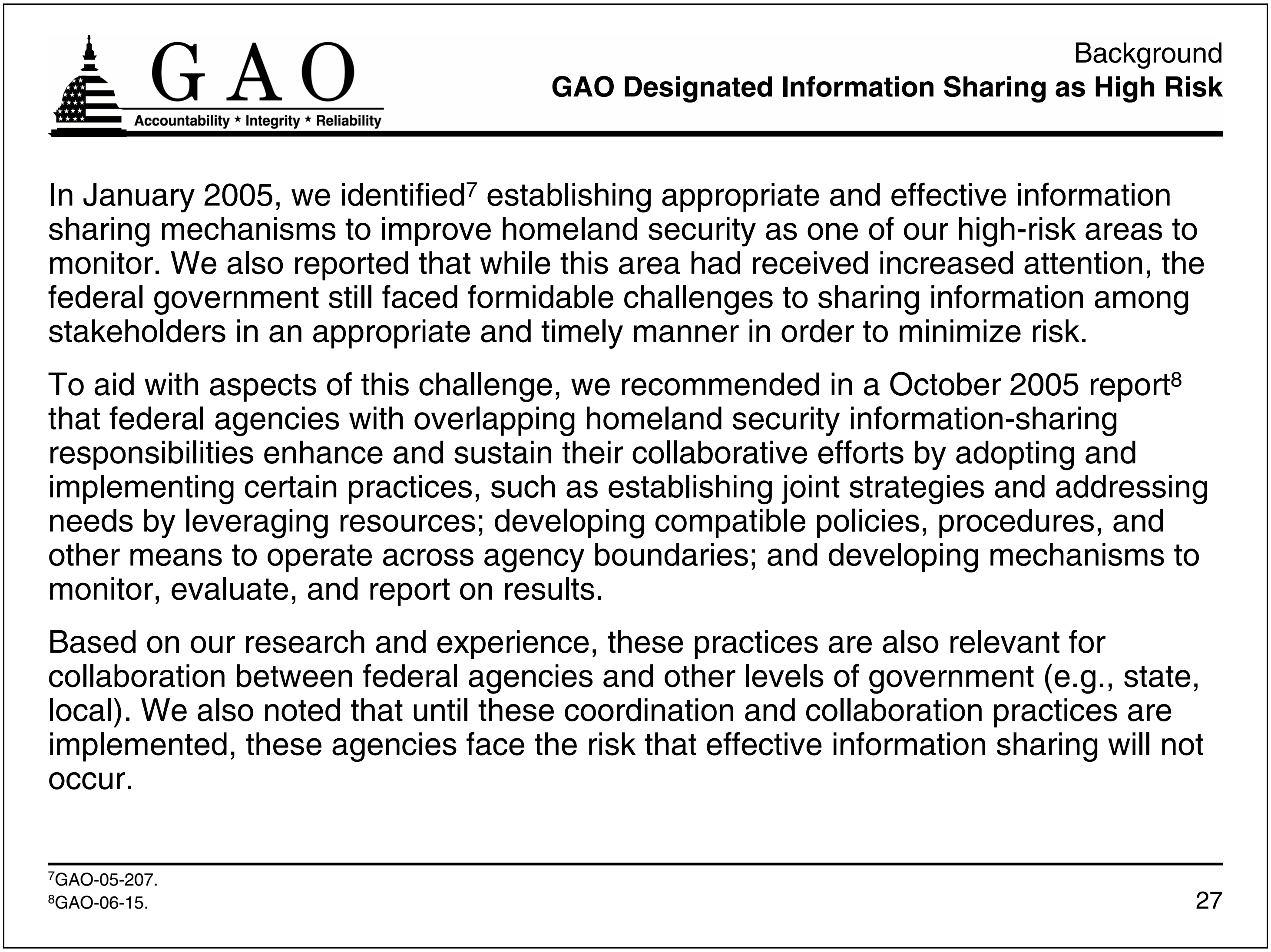
- **Document library.** Participants can store and search relevant documents within their community of interest.
- **Bulletin board.** The RISS ATIX bulletin board allows users to post timely threat information in discussion forums and to view and respond to posted information. Users can post documents, images, and information related to terrorism and homeland security, as well as receive DHS information, advisories, and warnings. According to RISS officials, the bulletin boards are monitored by a RISS moderator to relay any information that might be useful for other communities of interest.



GAO
Accountability * Integrity * Reliability

Background
Regional Information Sharing Systems Program

- **Chat tool.** ATIXLive is an online, real-time, collaborative communications information-sharing tool for the exchange of information by community members. Through this tool, users can post timely threat information and view and respond to messages posted.
- **Secure e-mail.** RISS ATIX participants have access to e-mail that can be used to provide alerts and related information. According to RISS, this is done in a secure environment.



Background

GAO Designated Information Sharing as High Risk

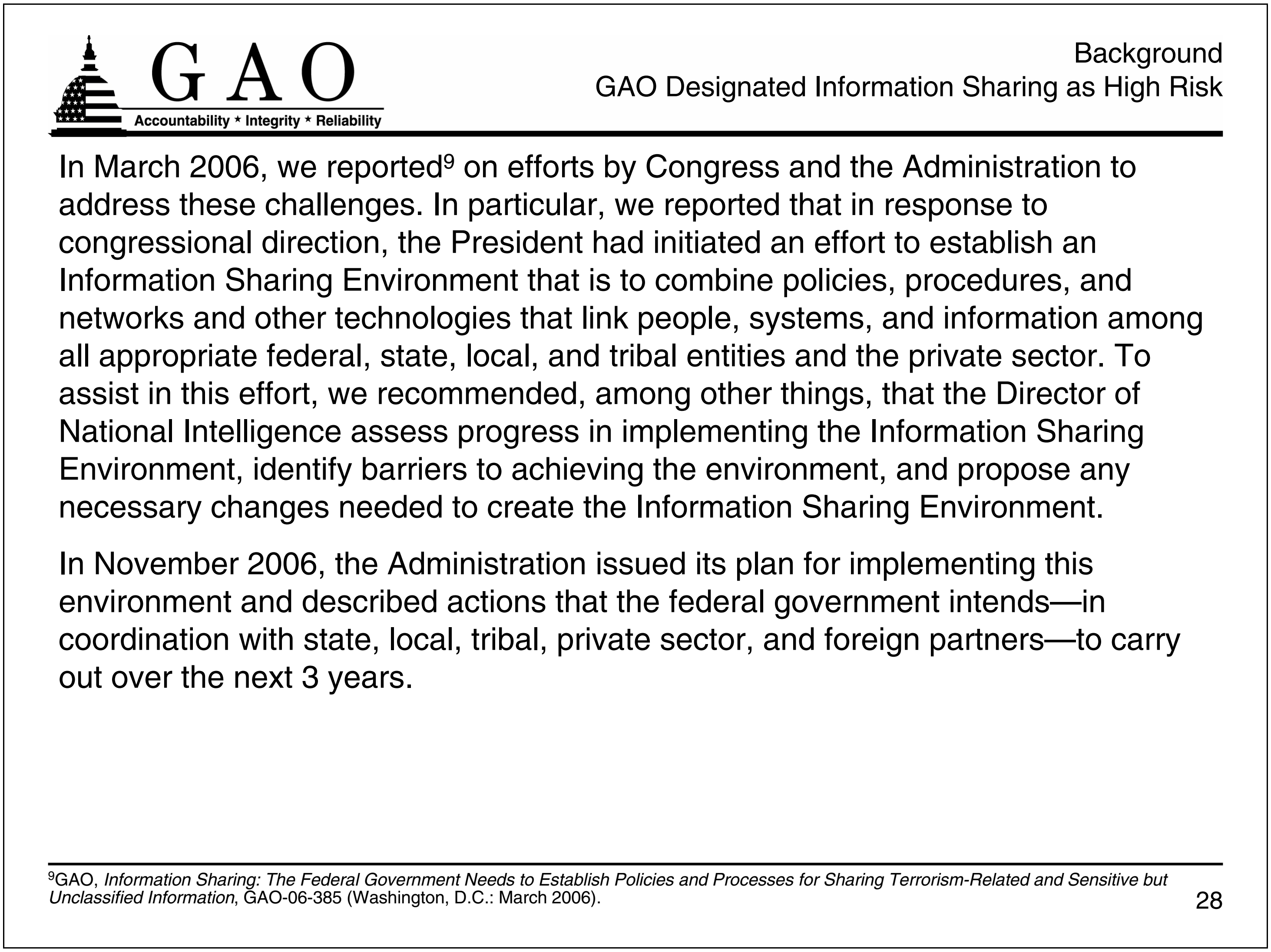
In January 2005, we identified[7] establishing appropriate and effective information sharing mechanisms to improve homeland security as one of our high-risk areas to monitor. We also reported that while this area had received increased attention, the federal government still faced formidable challenges to sharing information among stakeholders in an appropriate and timely manner in order to minimize risk.

To aid with aspects of this challenge, we recommended in a October 2005 report[8] that federal agencies with overlapping homeland security information-sharing responsibilities enhance and sustain their collaborative efforts by adopting and implementing certain practices, such as establishing joint strategies and addressing needs by leveraging resources; developing compatible policies, procedures, and other means to operate across agency boundaries; and developing mechanisms to monitor, evaluate, and report on results.

Based on our research and experience, these practices are also relevant for collaboration between federal agencies and other levels of government (e.g., state, local). We also noted that until these coordination and collaboration practices are implemented, these agencies face the risk that effective information sharing will not occur.

[7] GAO-05-207.

[8] GAO-06-15.



GAO
Accountability * Integrity * Reliability

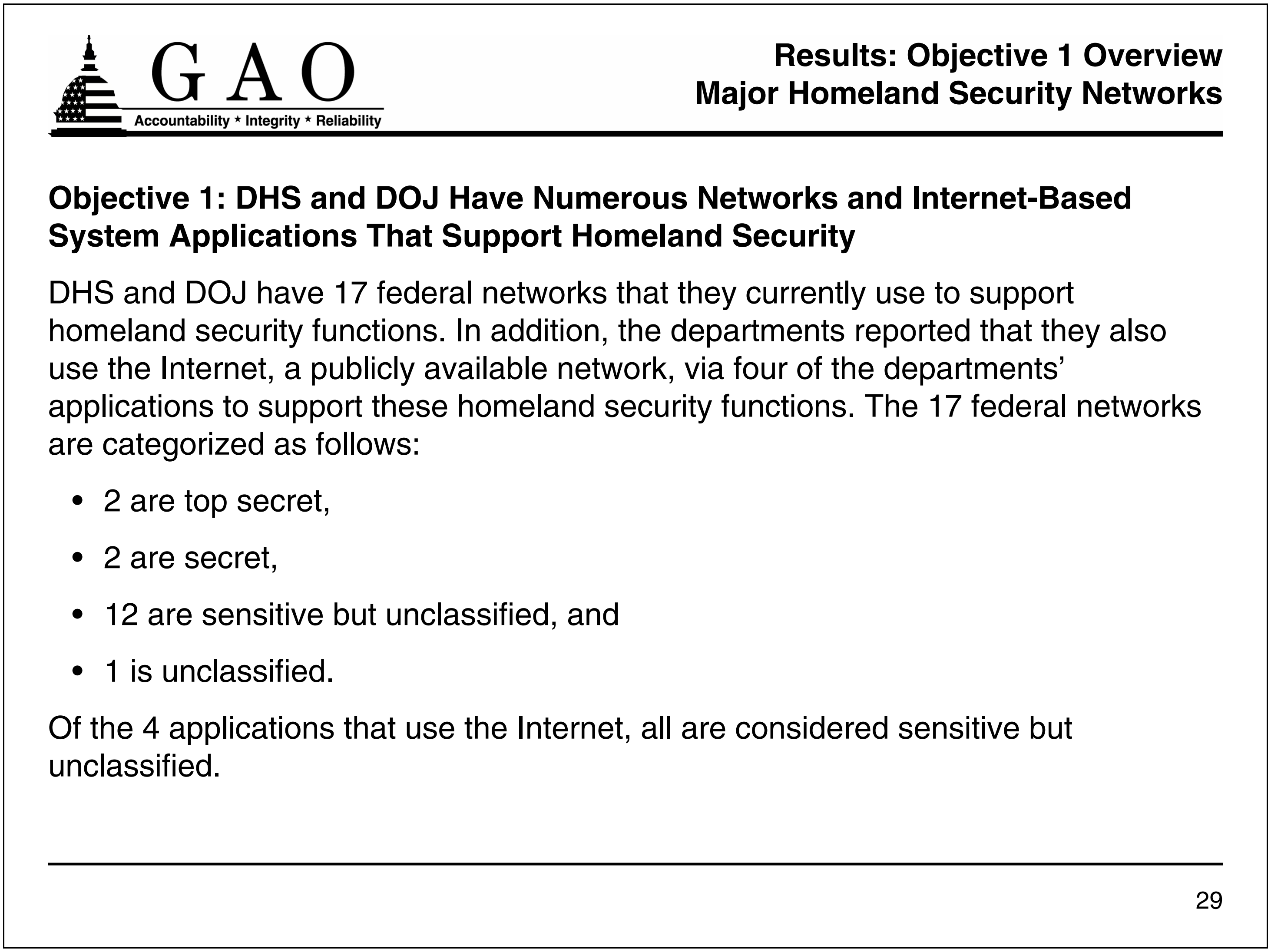
Background
GAO Designated Information Sharing as High Risk

In March 2006, we reported[9] on efforts by Congress and the Administration to address these challenges. In particular, we reported that in response to congressional direction, the President had initiated an effort to establish an Information Sharing Environment that is to combine policies, procedures, and networks and other technologies that link people, systems, and information among all appropriate federal, state, local, and tribal entities and the private sector. To assist in this effort, we recommended, among other things, that the Director of National Intelligence assess progress in implementing the Information Sharing Environment, identify barriers to achieving the environment, and propose any necessary changes needed to create the Information Sharing Environment.

In November 2006, the Administration issued its plan for implementing this environment and described actions that the federal government intends—in coordination with state, local, tribal, private sector, and foreign partners—to carry out over the next 3 years.

[9] GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: March 2006).

28



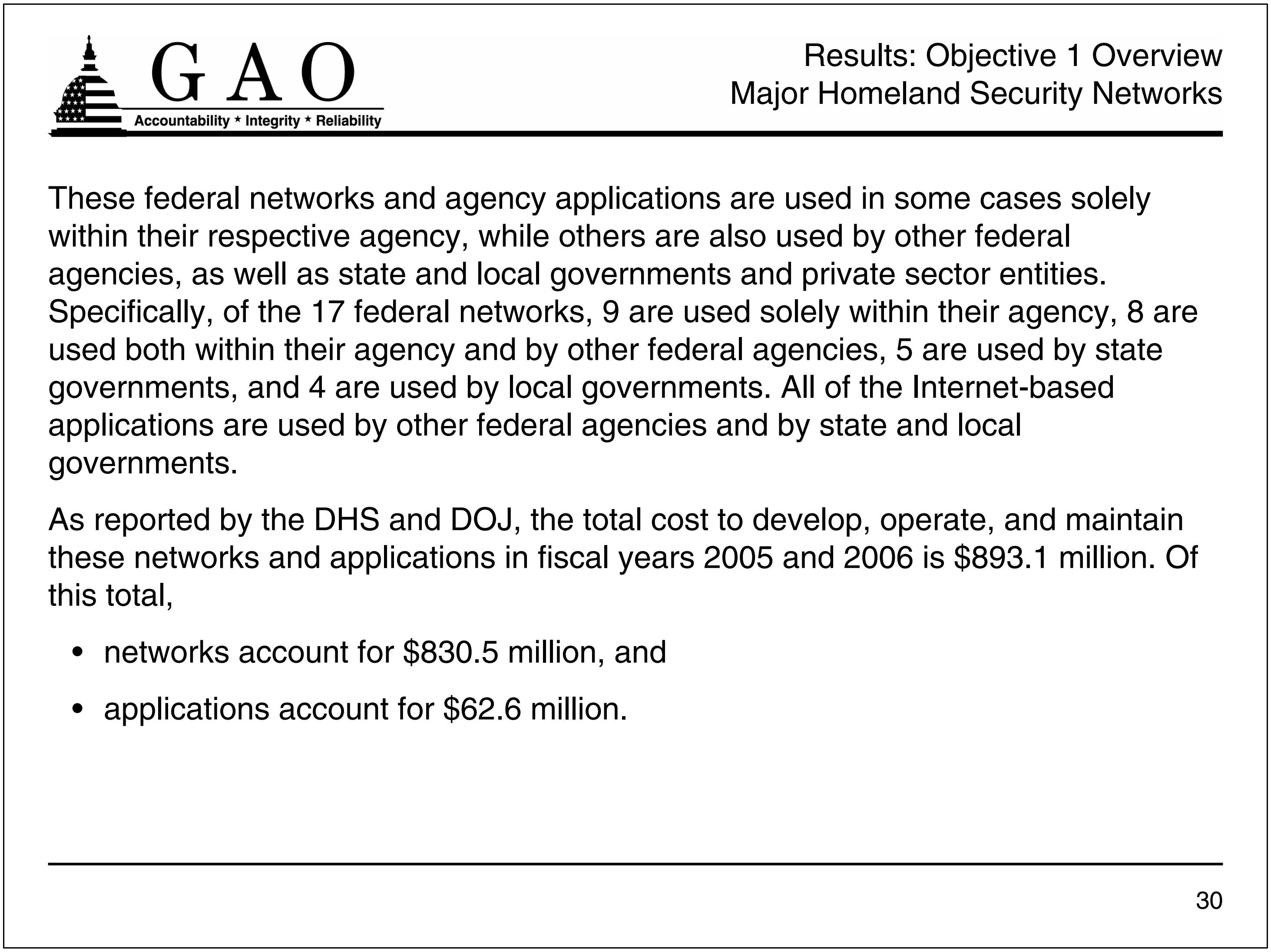
Results: Objective 1 Overview
Major Homeland Security Networks

Objective 1: DHS and DOJ Have Numerous Networks and Internet-Based System Applications That Support Homeland Security

DHS and DOJ have 17 federal networks that they currently use to support homeland security functions. In addition, the departments reported that they also use the Internet, a publicly available network, via four of the departments' applications to support these homeland security functions. The 17 federal networks are categorized as follows:

- 2 are top secret,
- 2 are secret,
- 12 are sensitive but unclassified, and
- 1 is unclassified.

Of the 4 applications that use the Internet, all are considered sensitive but unclassified.



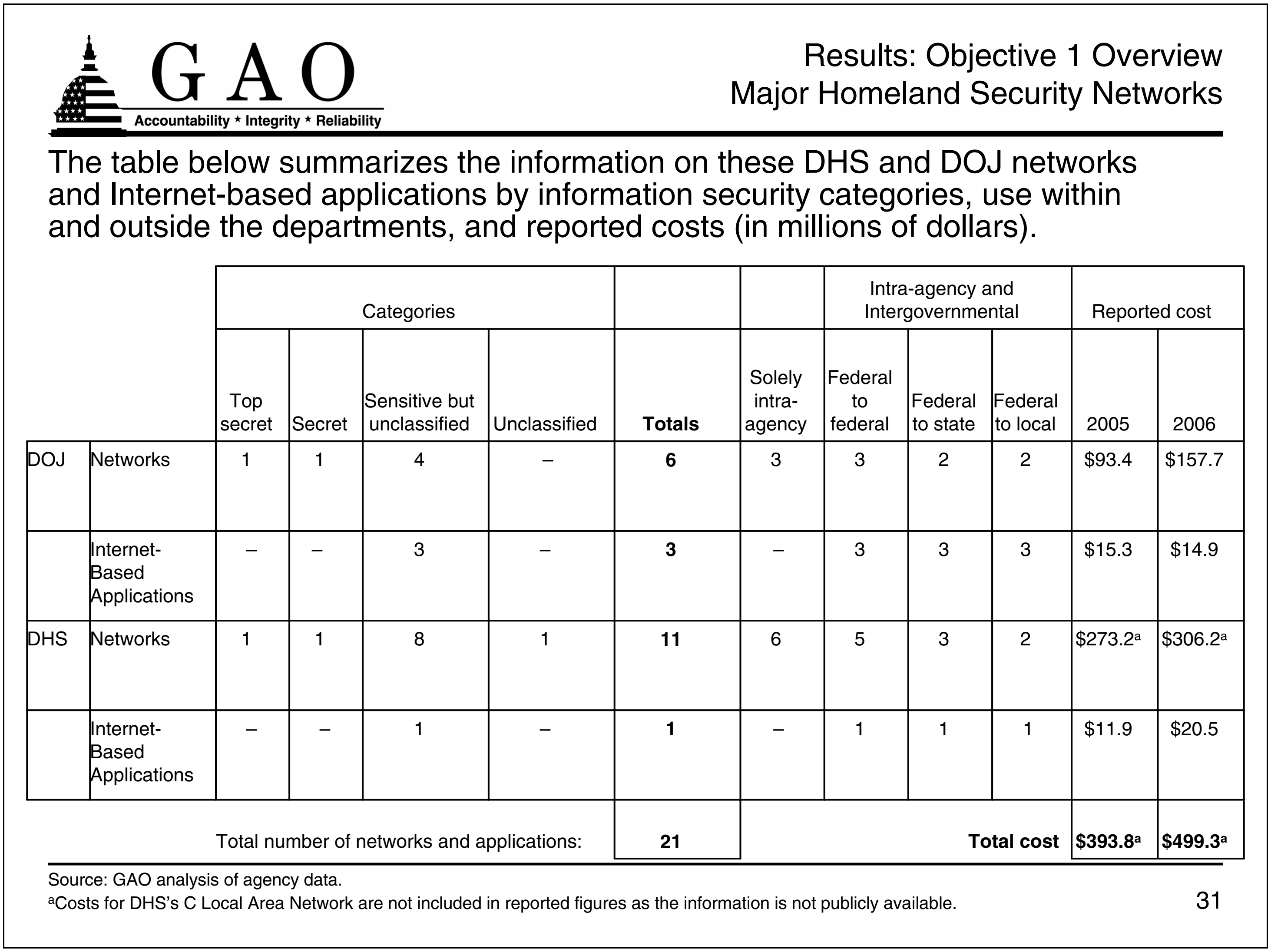
GAO
Accountability * Integrity * Reliability

Results: Objective 1 Overview
Major Homeland Security Networks

These federal networks and agency applications are used in some cases solely within their respective agency, while others are also used by other federal agencies, as well as state and local governments and private sector entities. Specifically, of the 17 federal networks, 9 are used solely within their agency, 8 are used both within their agency and by other federal agencies, 5 are used by state governments, and 4 are used by local governments. All of the Internet-based applications are used by other federal agencies and by state and local governments.

As reported by the DHS and DOJ, the total cost to develop, operate, and maintain these networks and applications in fiscal years 2005 and 2006 is $893.1 million. Of this total,

- networks account for $830.5 million, and
- applications account for $62.6 million.



GAO
Accountability * Integrity * Reliability

Results: Objective 1 Overview
Major Homeland Security Networks

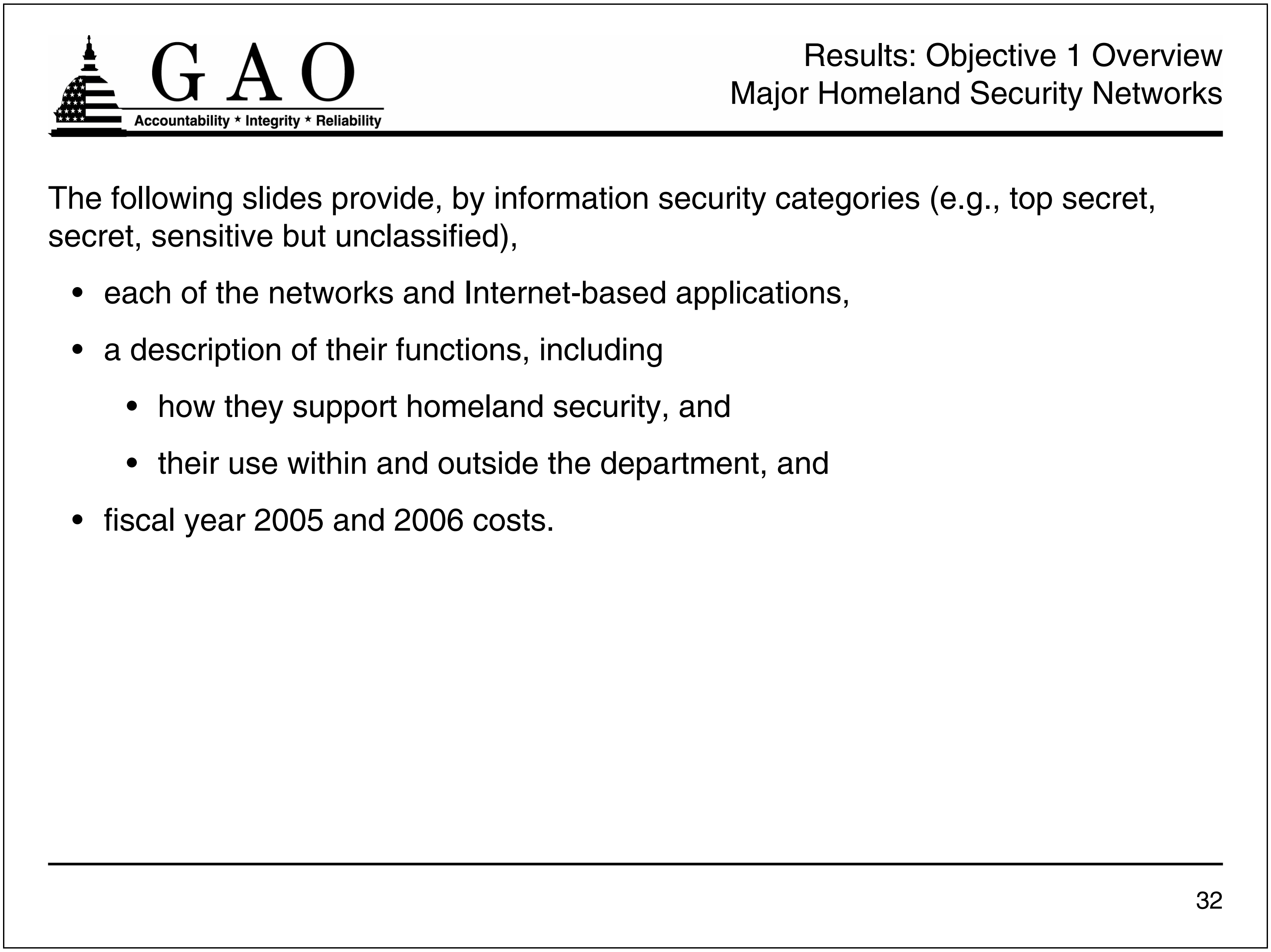
The table below summarizes the information on these DHS and DOJ networks and Internet-based applications by information security categories, use within and outside the departments, and reported costs (in millions of dollars).

		Categories						Intra-agency and Intergovernmental			Reported cost	
		Top secret	Secret	Sensitive but unclassified	Unclassified	**Totals**	Solely intra-agency	Federal to federal	Federal to state	Federal to local	2005	2006
DOJ	Networks	1	1	4	–	**6**	3	3	2	2	$93.4	$157.7
	Internet-Based Applications	–	–	3	–	**3**	–	3	3	3	$15.3	$14.9
DHS	Networks	1	1	8	1	**11**	6	5	3	2	$273.2[a]	$306.2[a]
	Internet-Based Applications	–	–	1	–	**1**	–	1	1	1	$11.9	$20.5
		Total number of networks and applications:				**21**				**Total cost**	**$393.8[a]**	**$499.3[a]**

Source: GAO analysis of agency data.

[a] Costs for DHS's C Local Area Network are not included in reported figures as the information is not publicly available.

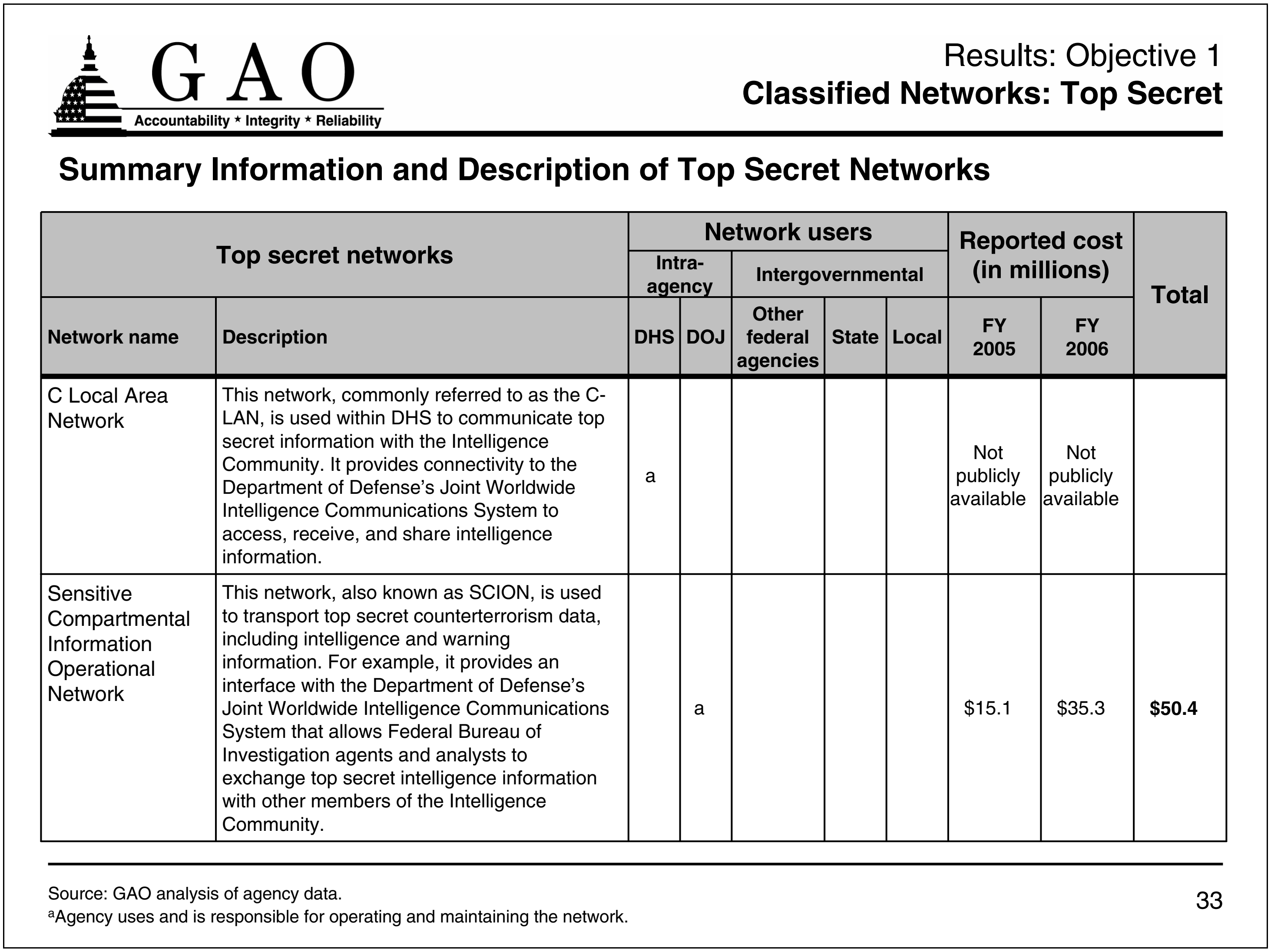
31



Results: Objective 1 Overview
Major Homeland Security Networks

The following slides provide, by information security categories (e.g., top secret, secret, sensitive but unclassified),

- each of the networks and Internet-based applications,
- a description of their functions, including
  - how they support homeland security, and
  - their use within and outside the department, and
- fiscal year 2005 and 2006 costs.



GAO
Accountability * Integrity * Reliability

Results: Objective 1
Classified Networks: Top Secret

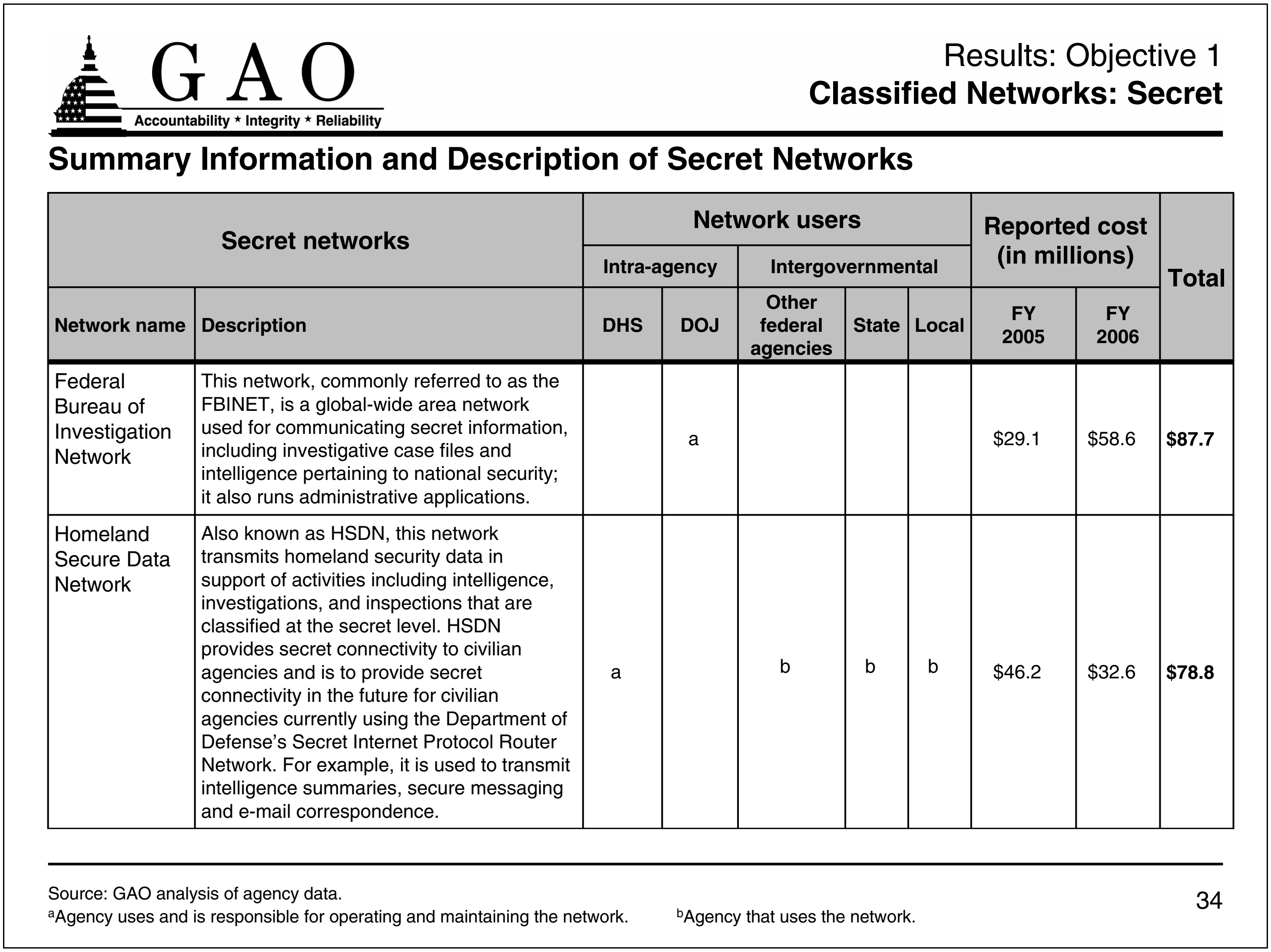
Summary Information and Description of Top Secret Networks

Top secret networks		Network users					Reported cost (in millions)		Total
		Intra-agency		Intergovernmental					
Network name	**Description**	**DHS**	**DOJ**	**Other federal agencies**	**State**	**Local**	**FY 2005**	**FY 2006**	
C Local Area Network	This network, commonly referred to as the C-LAN, is used within DHS to communicate top secret information with the Intelligence Community. It provides connectivity to the Department of Defense's Joint Worldwide Intelligence Communications System to access, receive, and share intelligence information.	a					Not publicly available	Not publicly available	
Sensitive Compartmental Information Operational Network	This network, also known as SCION, is used to transport top secret counterterrorism data, including intelligence and warning information. For example, it provides an interface with the Department of Defense's Joint Worldwide Intelligence Communications System that allows Federal Bureau of Investigation agents and analysts to exchange top secret intelligence information with other members of the Intelligence Community.		a				$15.1	$35.3	**$50.4**

Source: GAO analysis of agency data.

[a] Agency uses and is responsible for operating and maintaining the network.

33



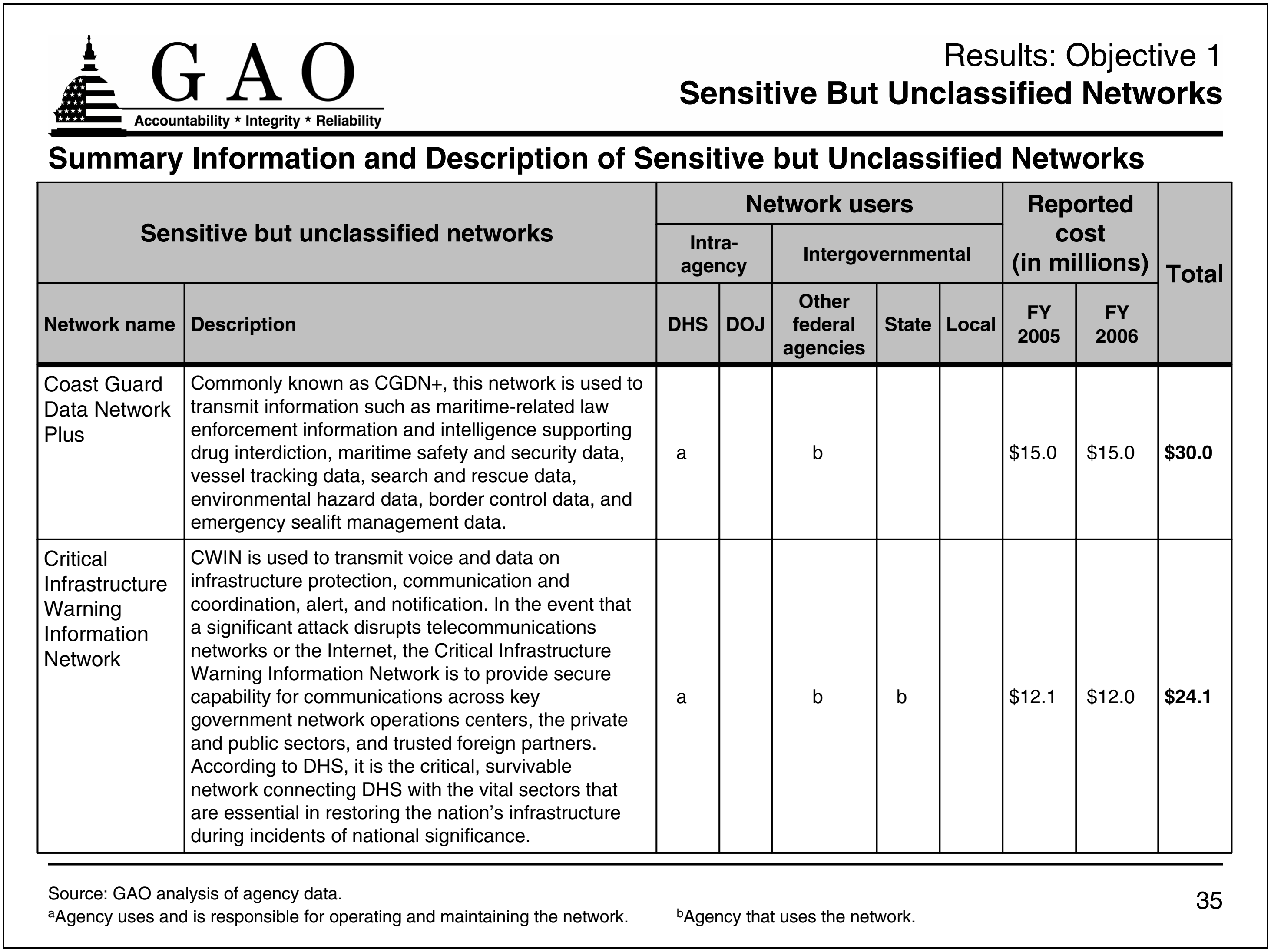
GAO
Accountability * Integrity * Reliability

Results: Objective 1
Classified Networks: Secret

Summary Information and Description of Secret Networks

Secret networks		Network users					Reported cost (in millions)		Total
		Intra-agency		Intergovernmental					
Network name	Description	DHS	DOJ	Other federal agencies	State	Local	FY 2005	FY 2006	
Federal Bureau of Investigation Network	This network, commonly referred to as the FBINET, is a global-wide area network used for communicating secret information, including investigative case files and intelligence pertaining to national security; it also runs administrative applications.		a				$29.1	$58.6	**$87.7**
Homeland Secure Data Network	Also known as HSDN, this network transmits homeland security data in support of activities including intelligence, investigations, and inspections that are classified at the secret level. HSDN provides secret connectivity to civilian agencies and is to provide secret connectivity in the future for civilian agencies currently using the Department of Defense's Secret Internet Protocol Router Network. For example, it is used to transmit intelligence summaries, secure messaging and e-mail correspondence.	a		b	b	b	$46.2	$32.6	**$78.8**

Source: GAO analysis of agency data.
[a]Agency uses and is responsible for operating and maintaining the network. [b]Agency that uses the network.



GAO
Accountability * Integrity * Reliability

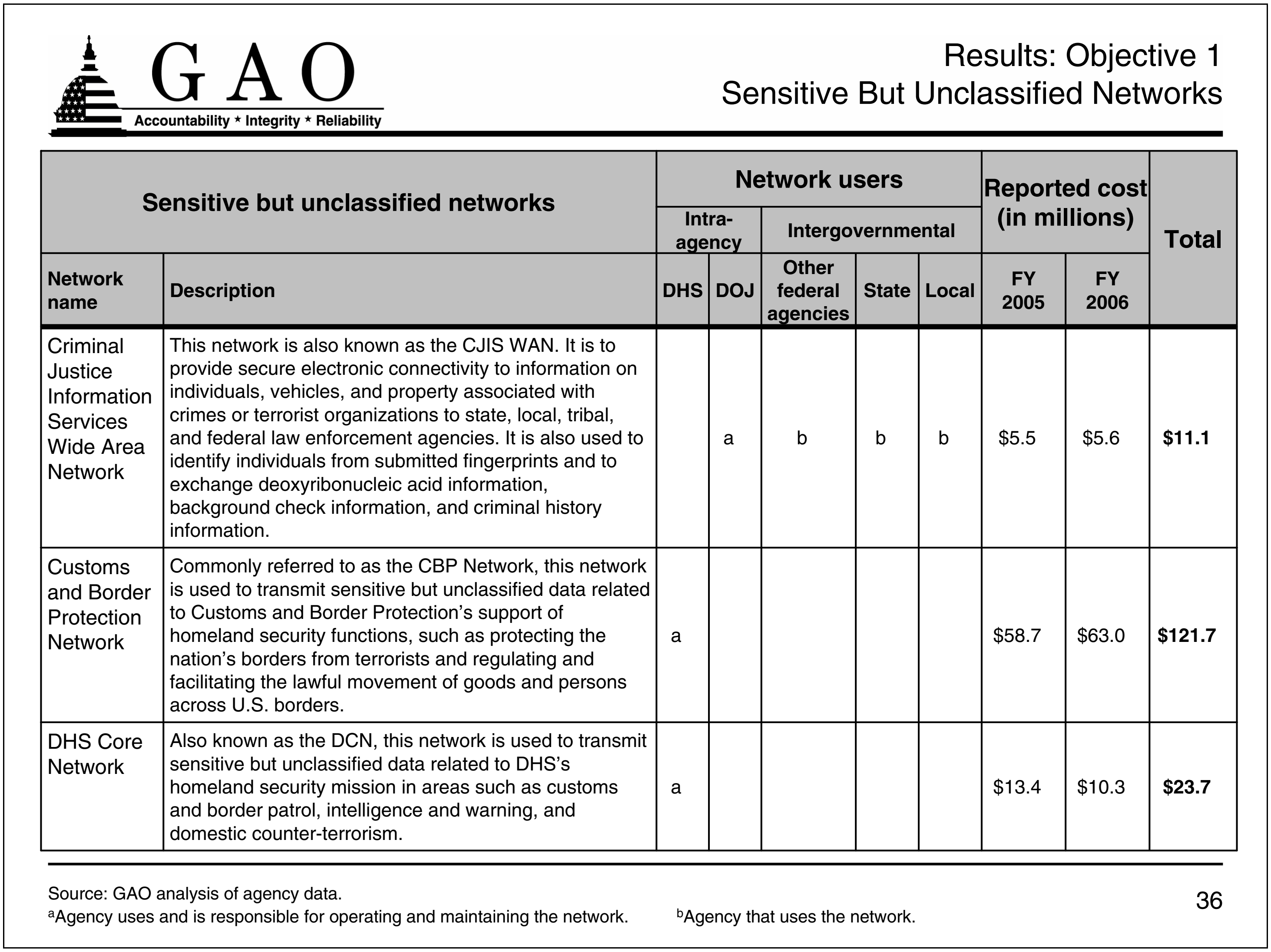
Results: Objective 1
Sensitive But Unclassified Networks

Summary Information and Description of Sensitive but Unclassified Networks

Sensitive but unclassified networks		Network users					Reported cost (in millions)		Total
		Intra-agency		Intergovernmental					
Network name	**Description**	**DHS**	**DOJ**	**Other federal agencies**	**State**	**Local**	**FY 2005**	**FY 2006**	
Coast Guard Data Network Plus	Commonly known as CGDN+, this network is used to transmit information such as maritime-related law enforcement information and intelligence supporting drug interdiction, maritime safety and security data, vessel tracking data, search and rescue data, environmental hazard data, border control data, and emergency sealift management data.	a		b			$15.0	$15.0	**$30.0**
Critical Infrastructure Warning Information Network	CWIN is used to transmit voice and data on infrastructure protection, communication and coordination, alert, and notification. In the event that a significant attack disrupts telecommunications networks or the Internet, the Critical Infrastructure Warning Information Network is to provide secure capability for communications across key government network operations centers, the private and public sectors, and trusted foreign partners. According to DHS, it is the critical, survivable network connecting DHS with the vital sectors that are essential in restoring the nation's infrastructure during incidents of national significance.	a		b	b		$12.1	$12.0	**$24.1**

Source: GAO analysis of agency data.
[a]Agency uses and is responsible for operating and maintaining the network. [b]Agency that uses the network.

35



GAO
Accountability * Integrity * Reliability

Results: Objective 1
Sensitive But Unclassified Networks

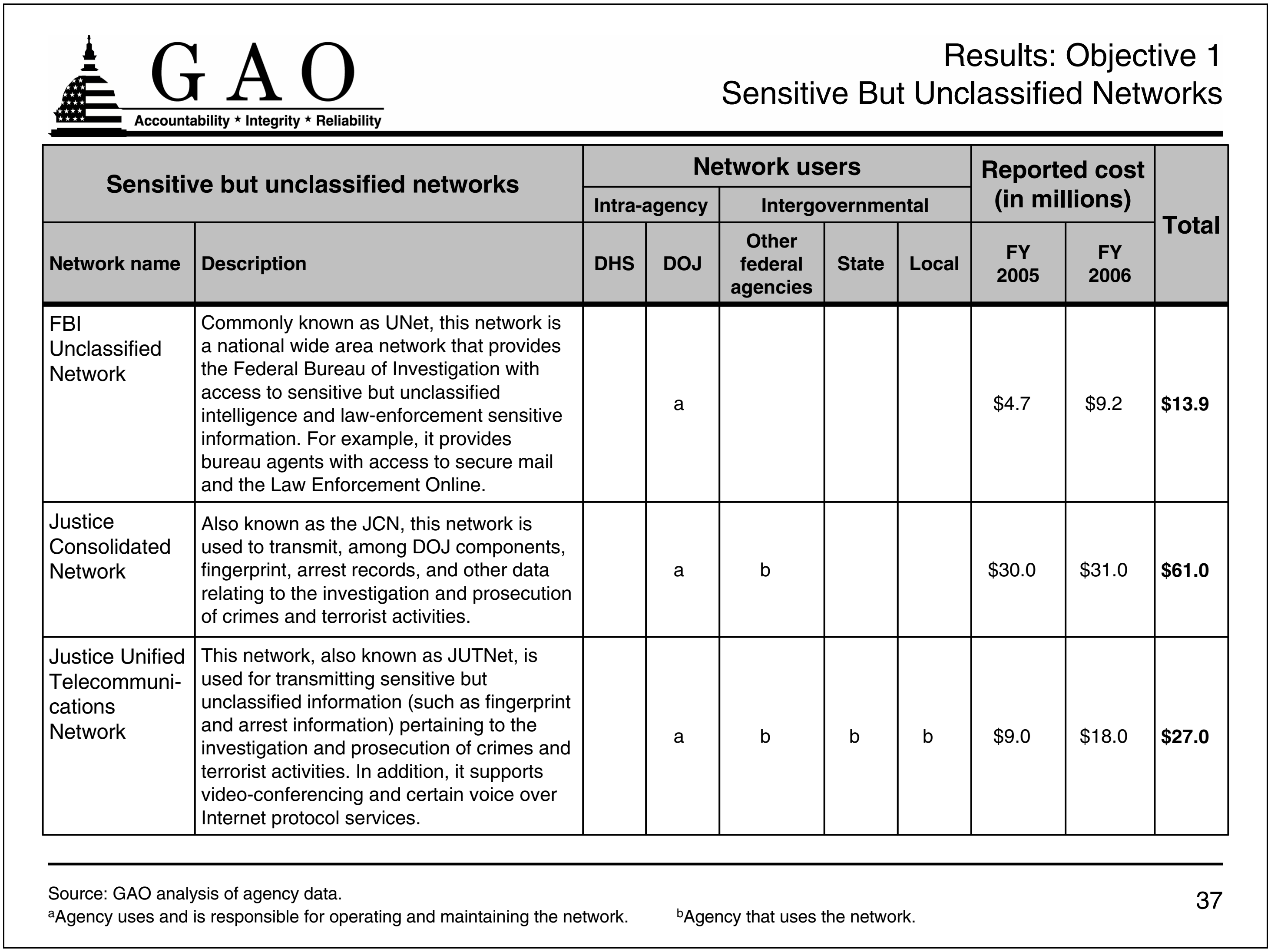
Sensitive but unclassified networks		Network users					Reported cost (in millions)		Total
		Intra-agency		Intergovernmental					
Network name	Description	DHS	DOJ	Other federal agencies	State	Local	FY 2005	FY 2006	
Criminal Justice Information Services Wide Area Network	This network is also known as the CJIS WAN. It is to provide secure electronic connectivity to information on individuals, vehicles, and property associated with crimes or terrorist organizations to state, local, tribal, and federal law enforcement agencies. It is also used to identify individuals from submitted fingerprints and to exchange deoxyribonucleic acid information, background check information, and criminal history information.		a	b	b	b	$5.5	$5.6	**$11.1**
Customs and Border Protection Network	Commonly referred to as the CBP Network, this network is used to transmit sensitive but unclassified data related to Customs and Border Protection's support of homeland security functions, such as protecting the nation's borders from terrorists and regulating and facilitating the lawful movement of goods and persons across U.S. borders.	a					$58.7	$63.0	**$121.7**
DHS Core Network	Also known as the DCN, this network is used to transmit sensitive but unclassified data related to DHS's homeland security mission in areas such as customs and border patrol, intelligence and warning, and domestic counter-terrorism.	a					$13.4	$10.3	**$23.7**

Source: GAO analysis of agency data.

[a] Agency uses and is responsible for operating and maintaining the network.

[b] Agency that uses the network.

36



GAO
Accountability * Integrity * Reliability

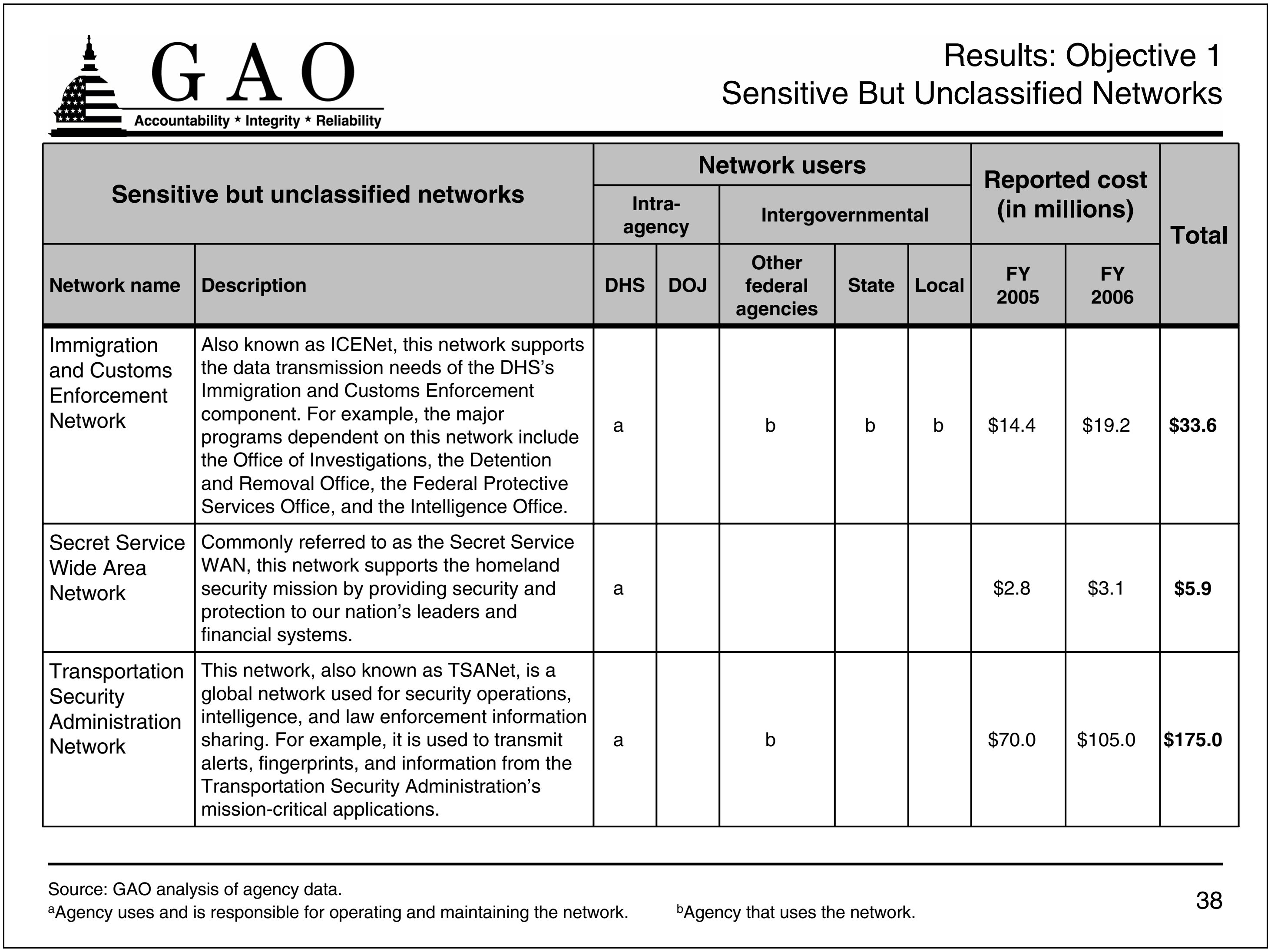
Results: Objective 1
Sensitive But Unclassified Networks

Sensitive but unclassified networks		Network users					Reported cost (in millions)		Total
		Intra-agency		Intergovernmental					
Network name	Description	DHS	DOJ	Other federal agencies	State	Local	FY 2005	FY 2006	
FBI Unclassified Network	Commonly known as UNet, this network is a national wide area network that provides the Federal Bureau of Investigation with access to sensitive but unclassified intelligence and law-enforcement sensitive information. For example, it provides bureau agents with access to secure mail and the Law Enforcement Online.		a				$4.7	$9.2	**$13.9**
Justice Consolidated Network	Also known as the JCN, this network is used to transmit, among DOJ components, fingerprint, arrest records, and other data relating to the investigation and prosecution of crimes and terrorist activities.		a	b			$30.0	$31.0	**$61.0**
Justice Unified Telecommunications Network	This network, also known as JUTNet, is used for transmitting sensitive but unclassified information (such as fingerprint and arrest information) pertaining to the investigation and prosecution of crimes and terrorist activities. In addition, it supports video-conferencing and certain voice over Internet protocol services.		a	b	b	b	$9.0	$18.0	**$27.0**

Source: GAO analysis of agency data.

[a] Agency uses and is responsible for operating and maintaining the network. [b] Agency that uses the network.

37



GAO
Accountability * Integrity * Reliability

Results: Objective 1 Sensitive But Unclassified Networks

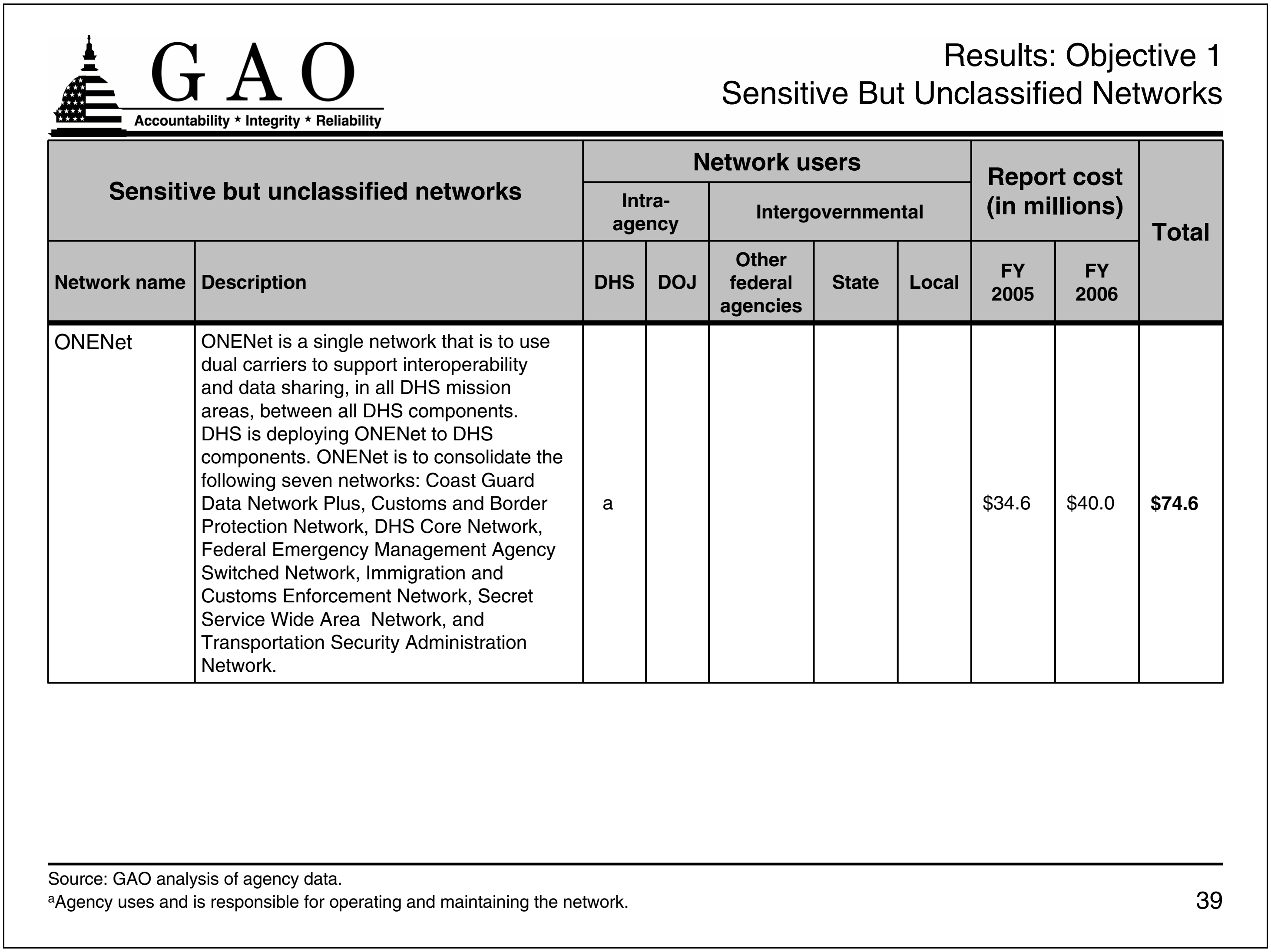
Sensitive but unclassified networks		Network users					Reported cost (in millions)		Total
		Intra-agency		Intergovernmental					
Network name	**Description**	**DHS**	**DOJ**	**Other federal agencies**	**State**	**Local**	**FY 2005**	**FY 2006**	
Immigration and Customs Enforcement Network	Also known as ICENet, this network supports the data transmission needs of the DHS's Immigration and Customs Enforcement component. For example, the major programs dependent on this network include the Office of Investigations, the Detention and Removal Office, the Federal Protective Services Office, and the Intelligence Office.	a		b	b	b	$14.4	$19.2	**$33.6**
Secret Service Wide Area Network	Commonly referred to as the Secret Service WAN, this network supports the homeland security mission by providing security and protection to our nation's leaders and financial systems.	a					$2.8	$3.1	**$5.9**
Transportation Security Administration Network	This network, also known as TSANet, is a global network used for security operations, intelligence, and law enforcement information sharing. For example, it is used to transmit alerts, fingerprints, and information from the Transportation Security Administration's mission-critical applications.	a		b			$70.0	$105.0	**$175.0**

Source: GAO analysis of agency data.

[a] Agency uses and is responsible for operating and maintaining the network.

[b] Agency that uses the network.

38



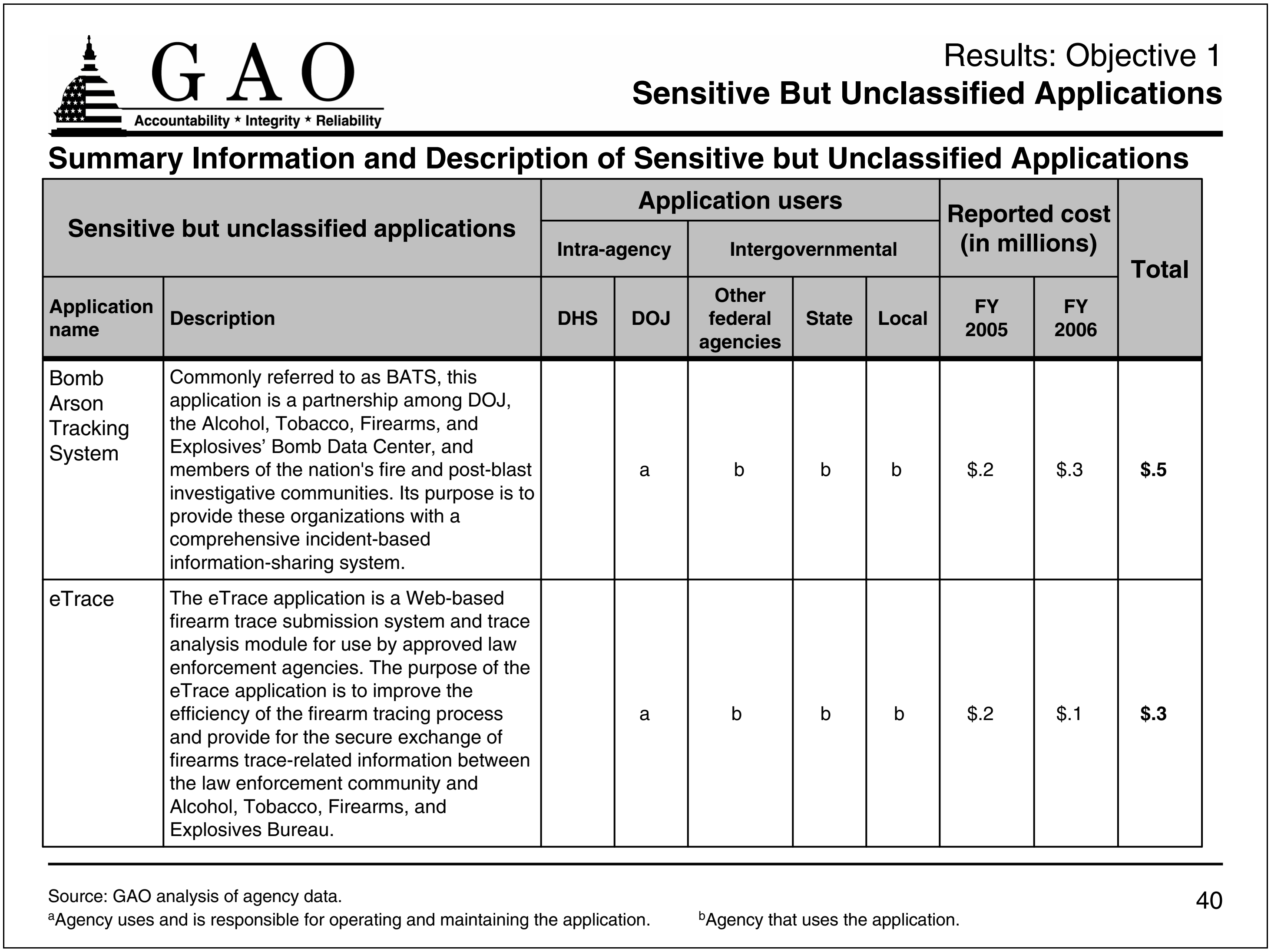
GAO
Accountability * Integrity * Reliability

Results: Objective 1
Sensitive But Unclassified Networks

Sensitive but unclassified networks		Network users					Report cost (in millions)		Total
		Intra-agency		Intergovernmental					
Network name	Description	DHS	DOJ	Other federal agencies	State	Local	FY 2005	FY 2006	
ONENet	ONENet is a single network that is to use dual carriers to support interoperability and data sharing, in all DHS mission areas, between all DHS components. DHS is deploying ONENet to DHS components. ONENet is to consolidate the following seven networks: Coast Guard Data Network Plus, Customs and Border Protection Network, DHS Core Network, Federal Emergency Management Agency Switched Network, Immigration and Customs Enforcement Network, Secret Service Wide Area Network, and Transportation Security Administration Network.	a					$34.6	$40.0	**$74.6**

Source: GAO analysis of agency data.

[a] Agency uses and is responsible for operating and maintaining the network.



GAO
Accountability * Integrity * Reliability

Results: Objective 1
Sensitive But Unclassified Applications

Summary Information and Description of Sensitive but Unclassified Applications

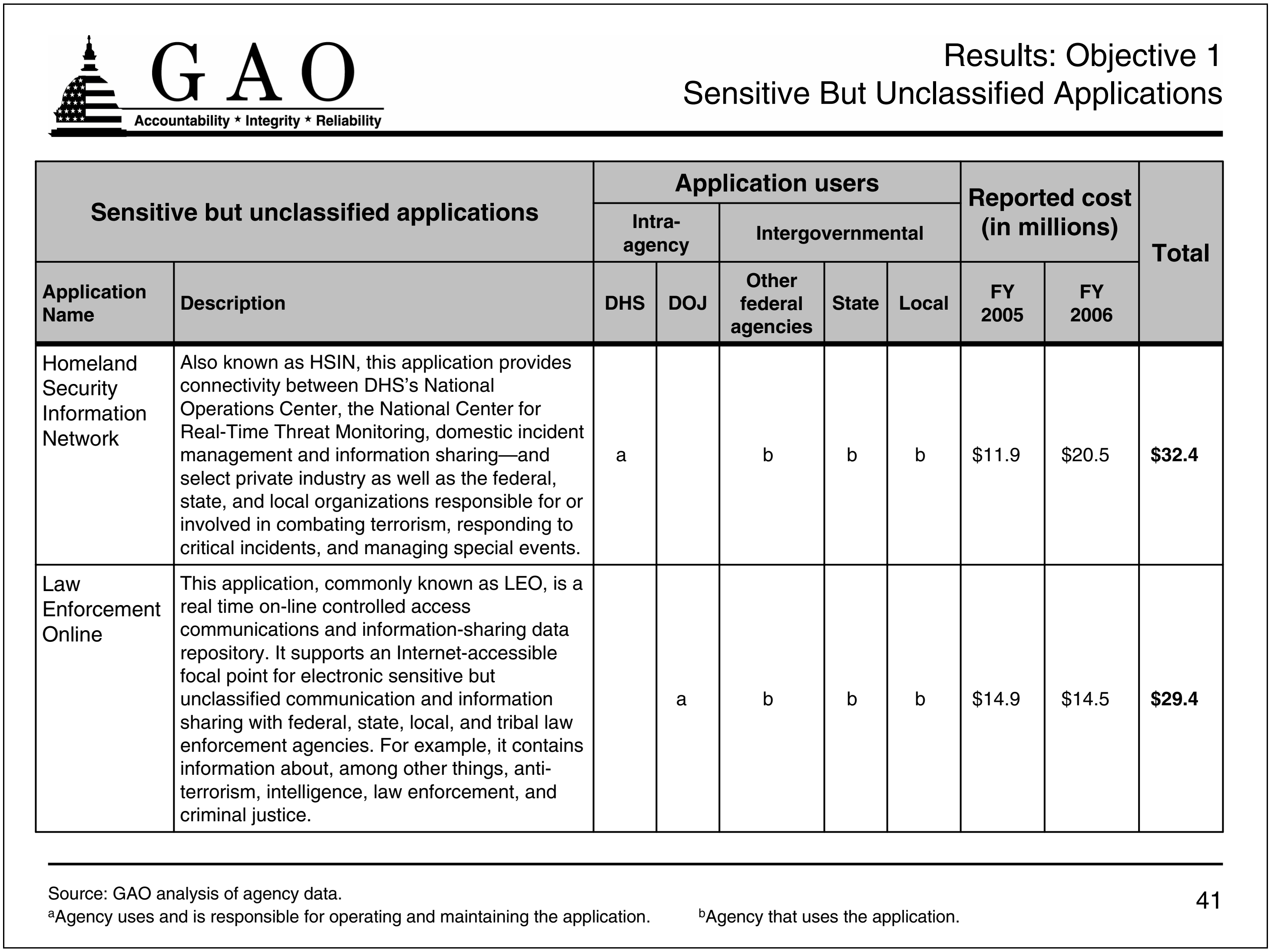
Sensitive but unclassified applications		Application users					Reported cost (in millions)		Total
		Intra-agency		Intergovernmental					
Application name	Description	DHS	DOJ	Other federal agencies	State	Local	FY 2005	FY 2006	
Bomb Arson Tracking System	Commonly referred to as BATS, this application is a partnership among DOJ, the Alcohol, Tobacco, Firearms, and Explosives' Bomb Data Center, and members of the nation's fire and post-blast investigative communities. Its purpose is to provide these organizations with a comprehensive incident-based information-sharing system.		a	b	b	b	$.2	$.3	**$.5**
eTrace	The eTrace application is a Web-based firearm trace submission system and trace analysis module for use by approved law enforcement agencies. The purpose of the eTrace application is to improve the efficiency of the firearm tracing process and provide for the secure exchange of firearms trace-related information between the law enforcement community and Alcohol, Tobacco, Firearms, and Explosives Bureau.		a	b	b	b	$.2	$.1	**$.3**

Source: GAO analysis of agency data.

[a] Agency uses and is responsible for operating and maintaining the application.

[b] Agency that uses the application.

40



GAO
Accountability * Integrity * Reliability

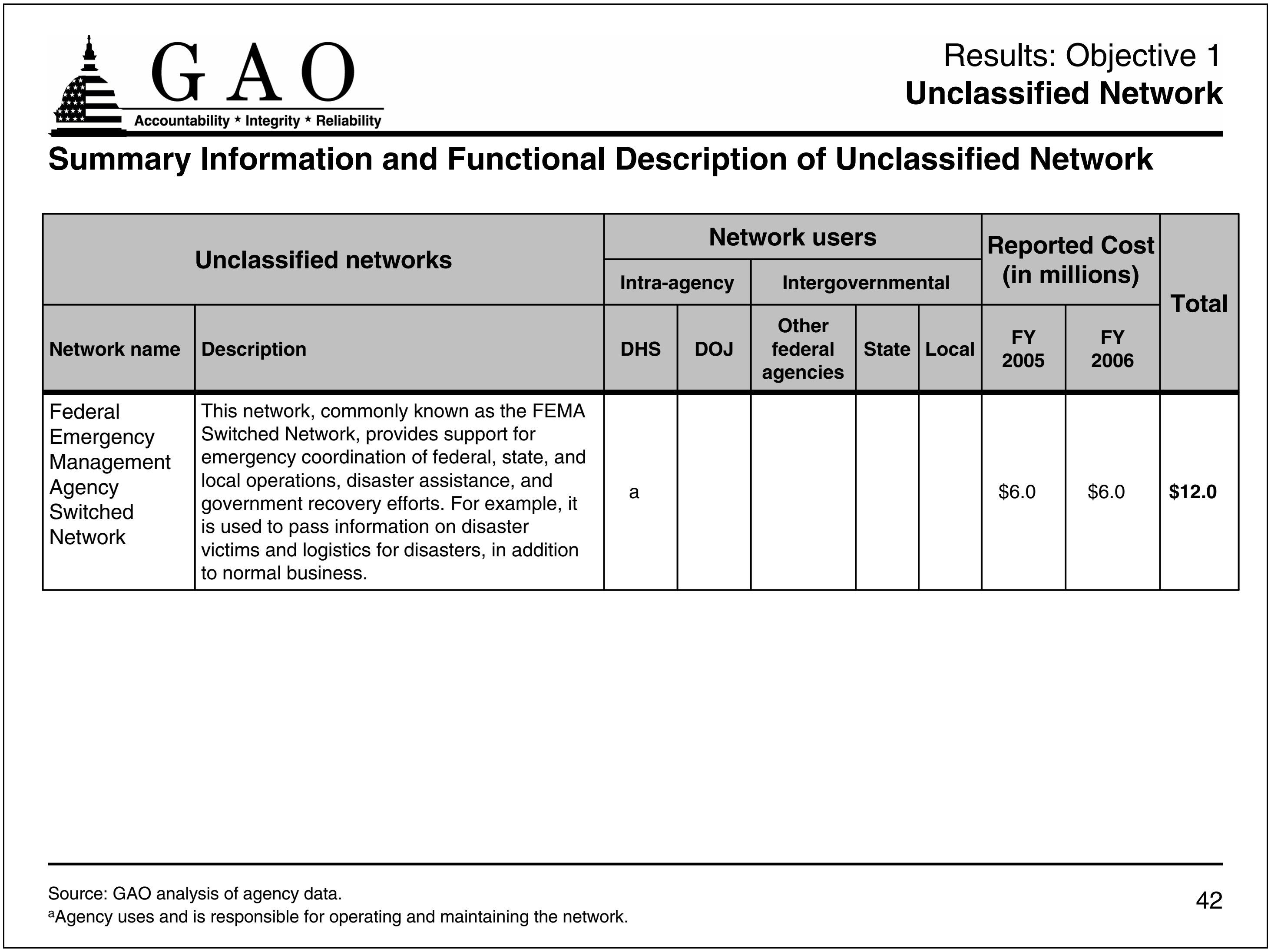
Results: Objective 1
Sensitive But Unclassified Applications

Sensitive but unclassified applications		Application users					Reported cost (in millions)		Total
		Intra-agency		Intergovernmental					
Application Name	**Description**	**DHS**	**DOJ**	**Other federal agencies**	**State**	**Local**	**FY 2005**	**FY 2006**	
Homeland Security Information Network	Also known as HSIN, this application provides connectivity between DHS's National Operations Center, the National Center for Real-Time Threat Monitoring, domestic incident management and information sharing—and select private industry as well as the federal, state, and local organizations responsible for or involved in combating terrorism, responding to critical incidents, and managing special events.	a		b	b	b	$11.9	$20.5	**$32.4**
Law Enforcement Online	This application, commonly known as LEO, is a real time on-line controlled access communications and information-sharing data repository. It supports an Internet-accessible focal point for electronic sensitive but unclassified communication and information sharing with federal, state, local, and tribal law enforcement agencies. For example, it contains information about, among other things, anti-terrorism, intelligence, law enforcement, and criminal justice.		a	b	b	b	$14.9	$14.5	**$29.4**

Source: GAO analysis of agency data.

[a] Agency uses and is responsible for operating and maintaining the application.

[b] Agency that uses the application.



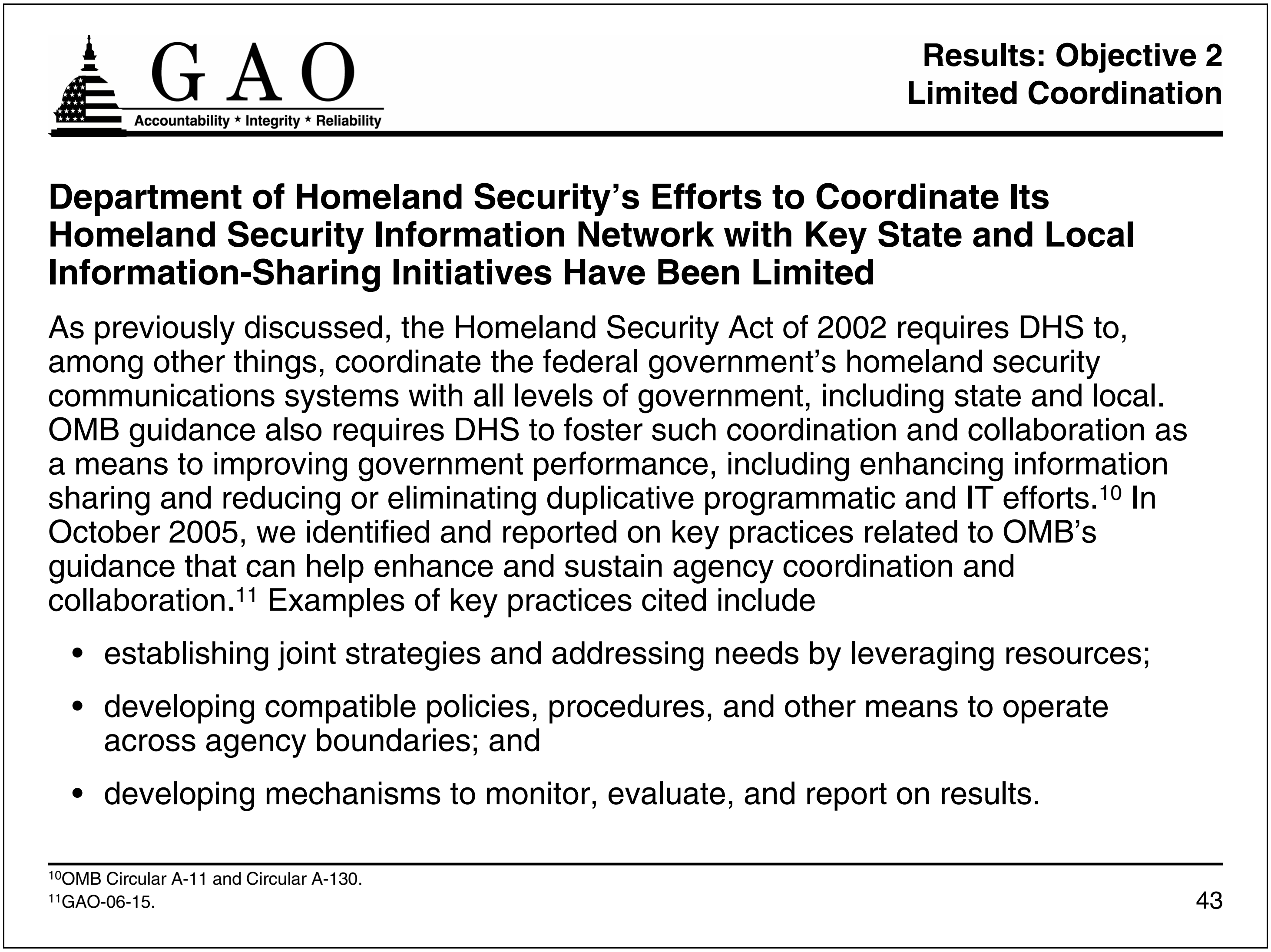
GAO Accountability * Integrity * Reliability

Results: Objective 1
Unclassified Network

Summary Information and Functional Description of Unclassified Network

Unclassified networks		Network users					Reported Cost (in millions)		Total
		Intra-agency		Intergovernmental					
Network name	Description	DHS	DOJ	Other federal agencies	State	Local	FY 2005	FY 2006	
Federal Emergency Management Agency Switched Network	This network, commonly known as the FEMA Switched Network, provides support for emergency coordination of federal, state, and local operations, disaster assistance, and government recovery efforts. For example, it is used to pass information on disaster victims and logistics for disasters, in addition to normal business.	a					$6.0	$6.0	**$12.0**

Source: GAO analysis of agency data.
[a]Agency uses and is responsible for operating and maintaining the network.



GAO
Accountability * Integrity * Reliability

Results: Objective 2
Limited Coordination

Department of Homeland Security's Efforts to Coordinate Its Homeland Security Information Network with Key State and Local Information-Sharing Initiatives Have Been Limited

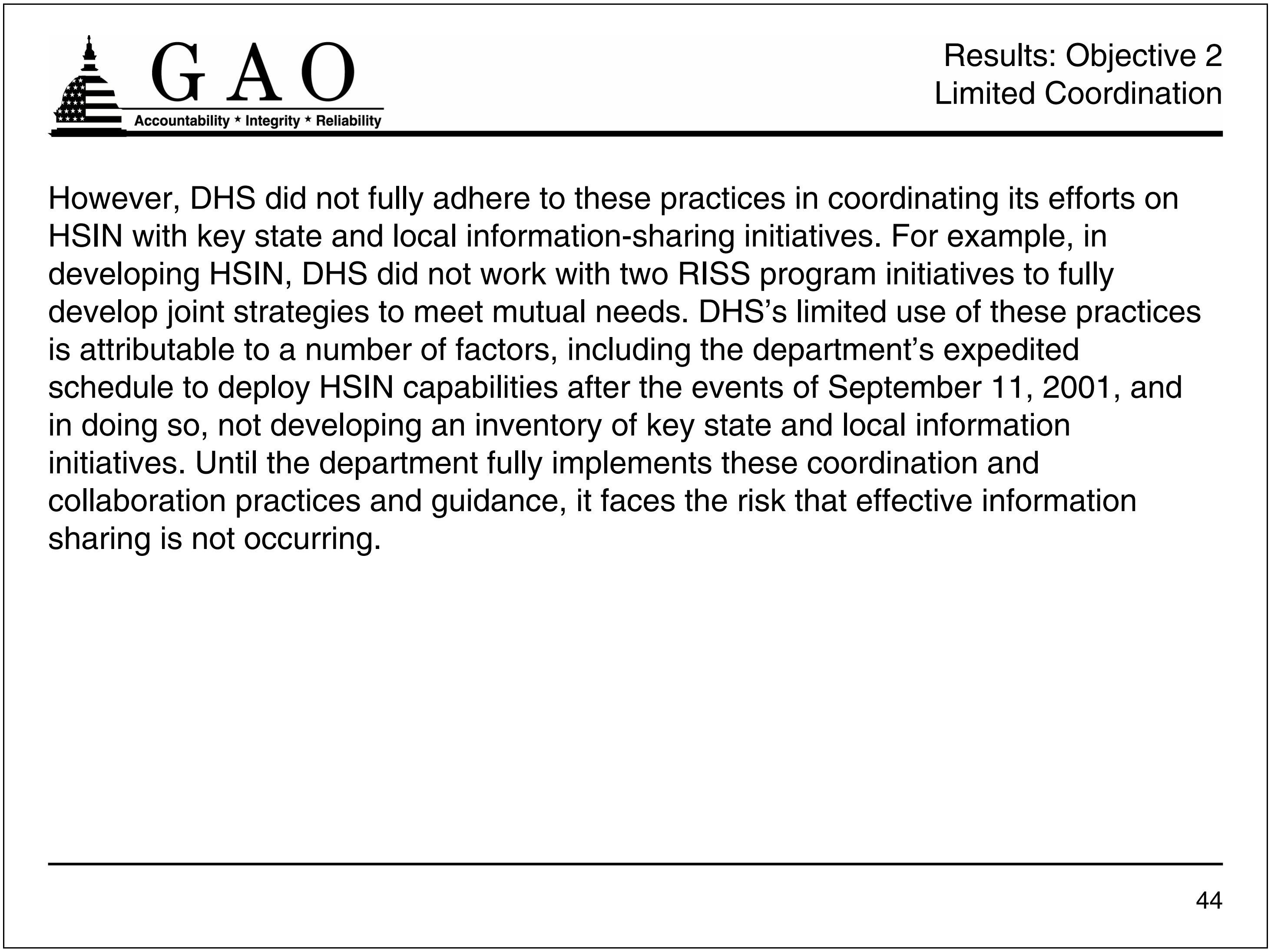
As previously discussed, the Homeland Security Act of 2002 requires DHS to, among other things, coordinate the federal government's homeland security communications systems with all levels of government, including state and local. OMB guidance also requires DHS to foster such coordination and collaboration as a means to improving government performance, including enhancing information sharing and reducing or eliminating duplicative programmatic and IT efforts.[10] In October 2005, we identified and reported on key practices related to OMB's guidance that can help enhance and sustain agency coordination and collaboration.[11] Examples of key practices cited include

- establishing joint strategies and addressing needs by leveraging resources;
- developing compatible policies, procedures, and other means to operate across agency boundaries; and
- developing mechanisms to monitor, evaluate, and report on results.

[10] OMB Circular A-11 and Circular A-130.

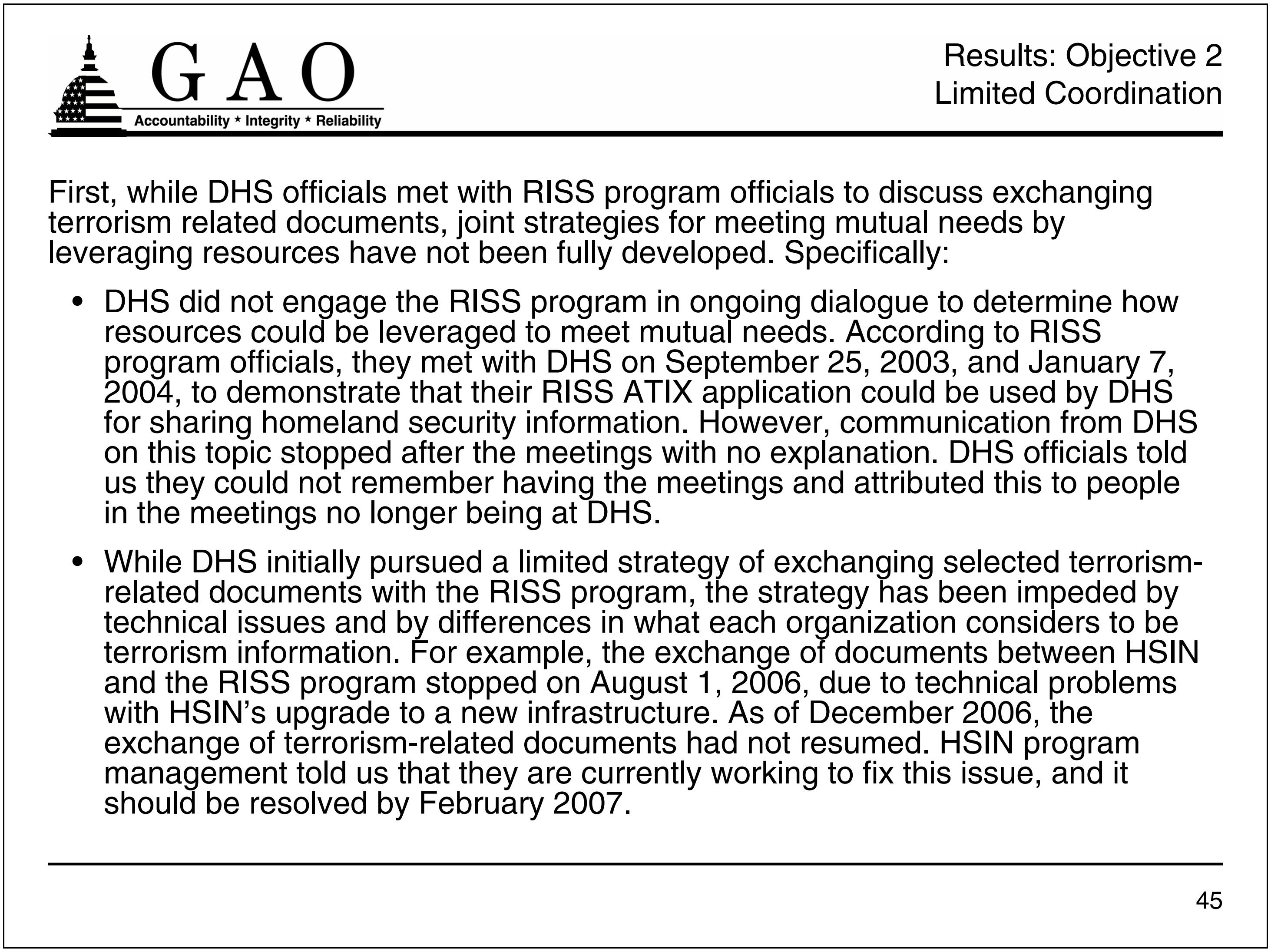
[11] GAO-06-15.

43



Results: Objective 2
Limited Coordination

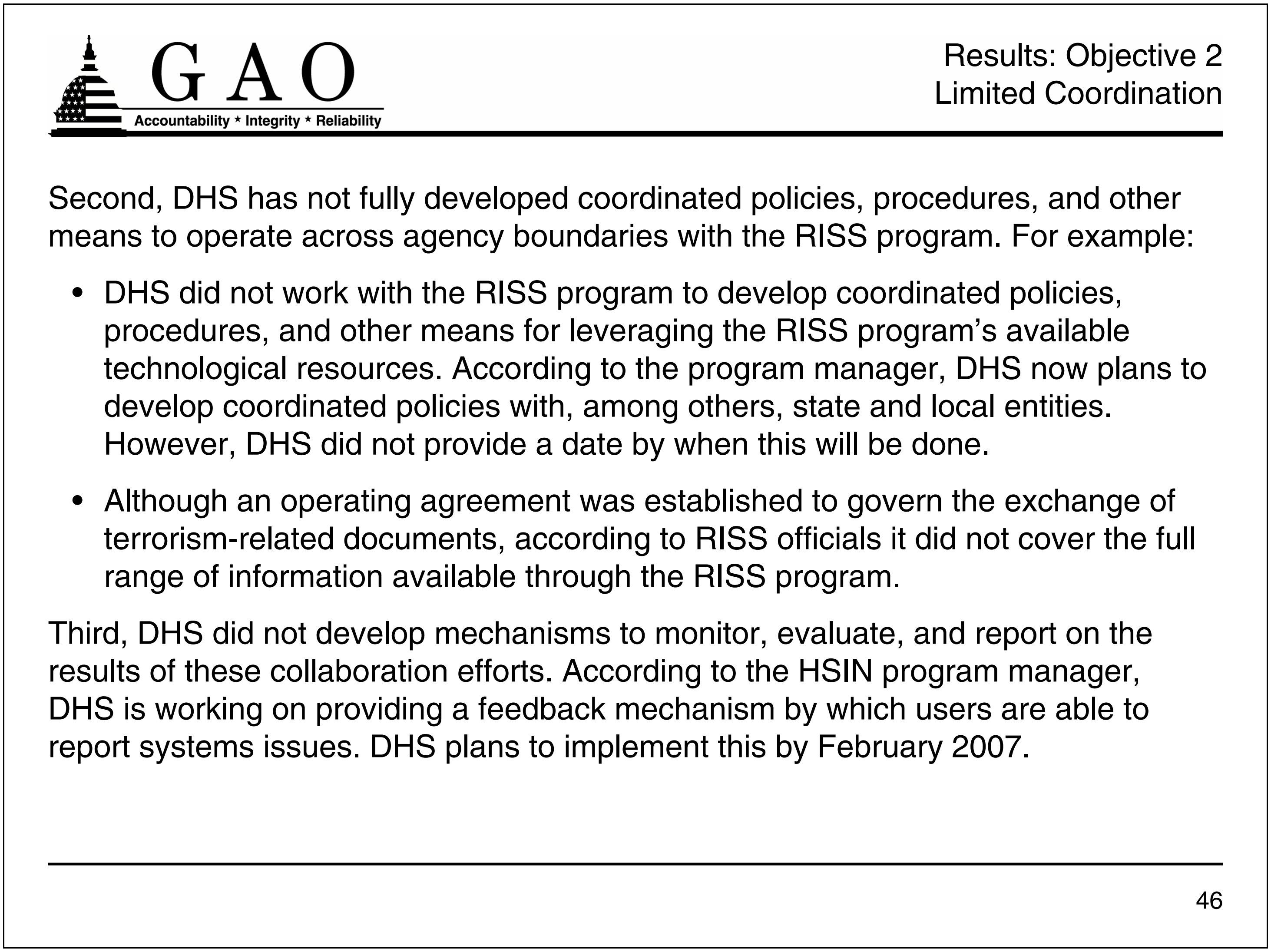
However, DHS did not fully adhere to these practices in coordinating its efforts on HSIN with key state and local information-sharing initiatives. For example, in developing HSIN, DHS did not work with two RISS program initiatives to fully develop joint strategies to meet mutual needs. DHS's limited use of these practices is attributable to a number of factors, including the department's expedited schedule to deploy HSIN capabilities after the events of September 11, 2001, and in doing so, not developing an inventory of key state and local information initiatives. Until the department fully implements these coordination and collaboration practices and guidance, it faces the risk that effective information sharing is not occurring.



Results: Objective 2
Limited Coordination

First, while DHS officials met with RISS program officials to discuss exchanging terrorism related documents, joint strategies for meeting mutual needs by leveraging resources have not been fully developed. Specifically:

- DHS did not engage the RISS program in ongoing dialogue to determine how resources could be leveraged to meet mutual needs. According to RISS program officials, they met with DHS on September 25, 2003, and January 7, 2004, to demonstrate that their RISS ATIX application could be used by DHS for sharing homeland security information. However, communication from DHS on this topic stopped after the meetings with no explanation. DHS officials told us they could not remember having the meetings and attributed this to people in the meetings no longer being at DHS.
- While DHS initially pursued a limited strategy of exchanging selected terrorism-related documents with the RISS program, the strategy has been impeded by technical issues and by differences in what each organization considers to be terrorism information. For example, the exchange of documents between HSIN and the RISS program stopped on August 1, 2006, due to technical problems with HSIN's upgrade to a new infrastructure. As of December 2006, the exchange of terrorism-related documents had not resumed. HSIN program management told us that they are currently working to fix this issue, and it should be resolved by February 2007.



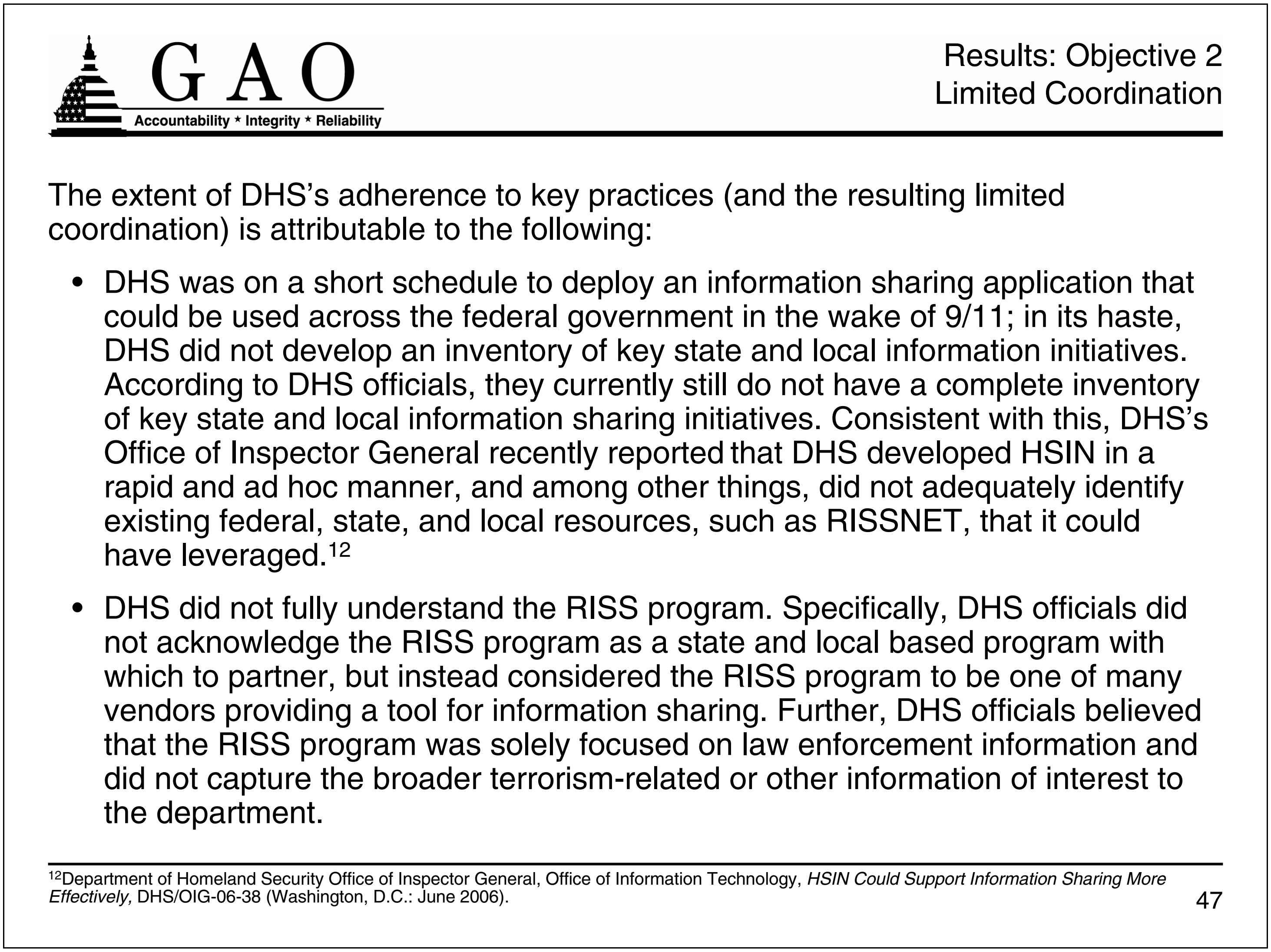
GAO
Accountability * Integrity * Reliability

Results: Objective 2
Limited Coordination

Second, DHS has not fully developed coordinated policies, procedures, and other means to operate across agency boundaries with the RISS program. For example:

- DHS did not work with the RISS program to develop coordinated policies, procedures, and other means for leveraging the RISS program's available technological resources. According to the program manager, DHS now plans to develop coordinated policies with, among others, state and local entities. However, DHS did not provide a date by when this will be done.
- Although an operating agreement was established to govern the exchange of terrorism-related documents, according to RISS officials it did not cover the full range of information available through the RISS program.

Third, DHS did not develop mechanisms to monitor, evaluate, and report on the results of these collaboration efforts. According to the HSIN program manager, DHS is working on providing a feedback mechanism by which users are able to report systems issues. DHS plans to implement this by February 2007.



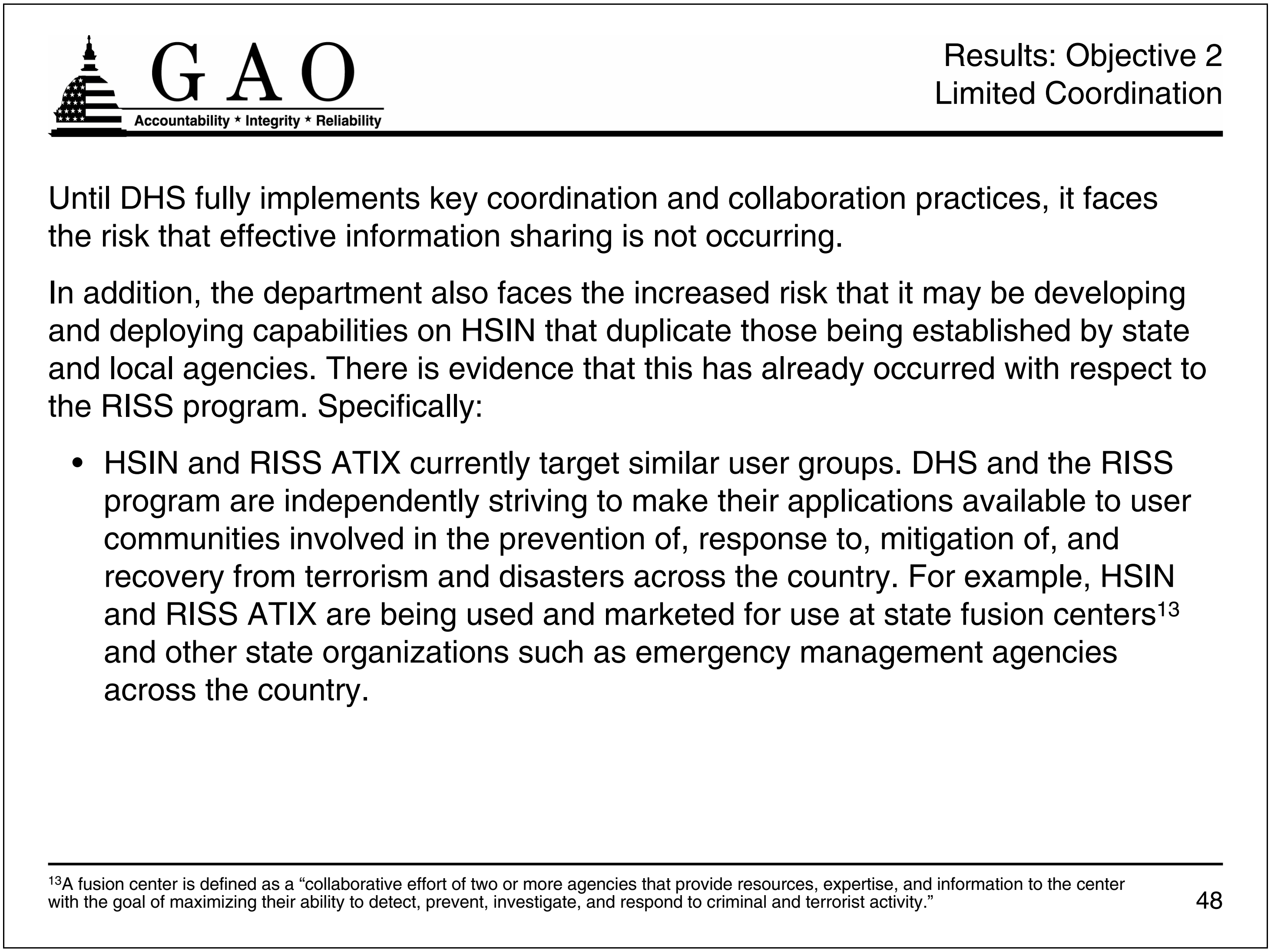
GAO Accountability * Integrity * Reliability

Results: Objective 2
Limited Coordination

The extent of DHS's adherence to key practices (and the resulting limited coordination) is attributable to the following:

- DHS was on a short schedule to deploy an information sharing application that could be used across the federal government in the wake of 9/11; in its haste, DHS did not develop an inventory of key state and local information initiatives. According to DHS officials, they currently still do not have a complete inventory of key state and local information sharing initiatives. Consistent with this, DHS's Office of Inspector General recently reported that DHS developed HSIN in a rapid and ad hoc manner, and among other things, did not adequately identify existing federal, state, and local resources, such as RISSNET, that it could have leveraged.[12]
- DHS did not fully understand the RISS program. Specifically, DHS officials did not acknowledge the RISS program as a state and local based program with which to partner, but instead considered the RISS program to be one of many vendors providing a tool for information sharing. Further, DHS officials believed that the RISS program was solely focused on law enforcement information and did not capture the broader terrorism-related or other information of interest to the department.

[12] Department of Homeland Security Office of Inspector General, Office of Information Technology, *HSIN Could Support Information Sharing More Effectively,* DHS/OIG-06-38 (Washington, D.C.: June 2006).



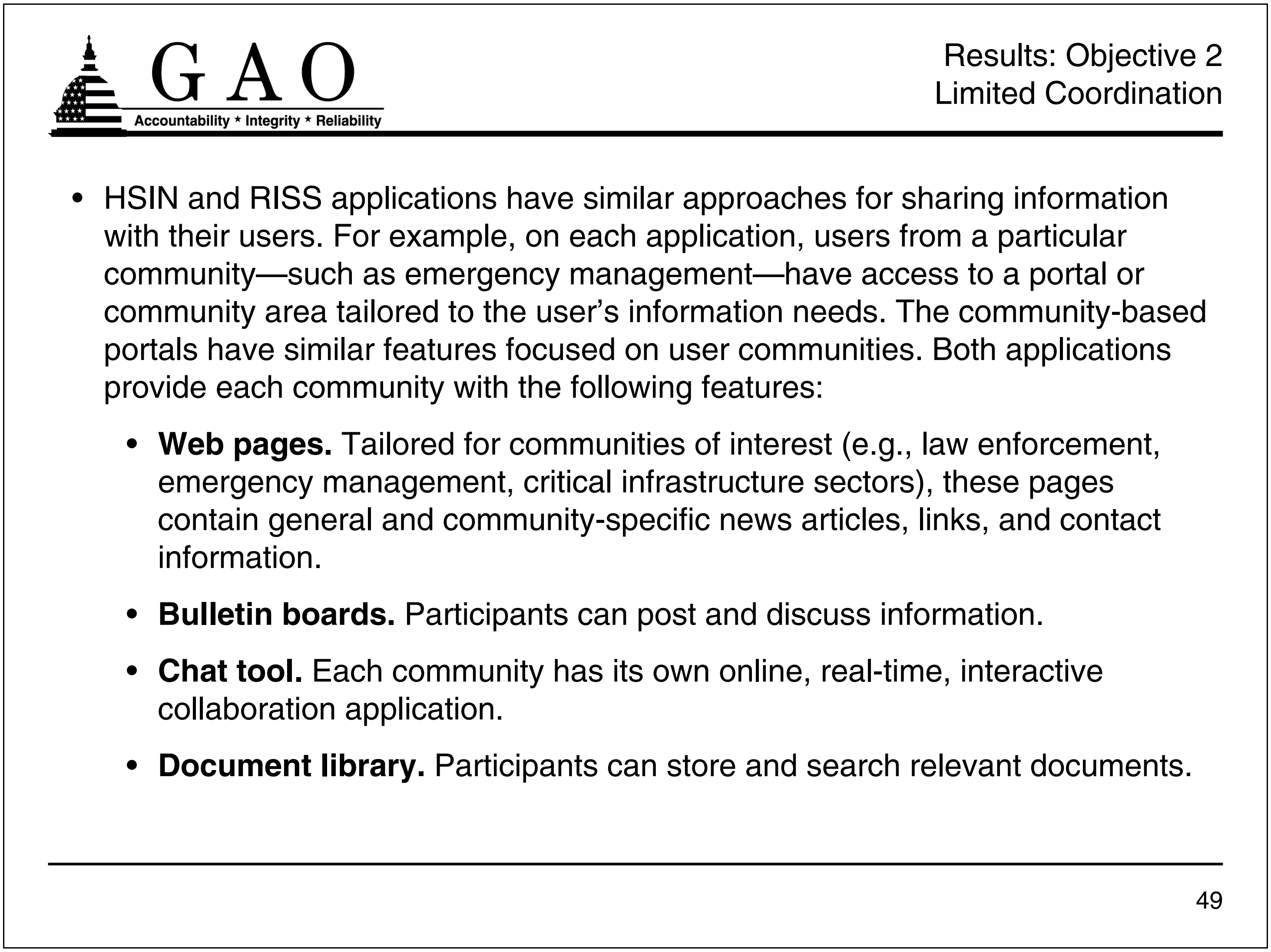
Results: Objective 2
Limited Coordination

Until DHS fully implements key coordination and collaboration practices, it faces the risk that effective information sharing is not occurring.

In addition, the department also faces the increased risk that it may be developing and deploying capabilities on HSIN that duplicate those being established by state and local agencies. There is evidence that this has already occurred with respect to the RISS program. Specifically:

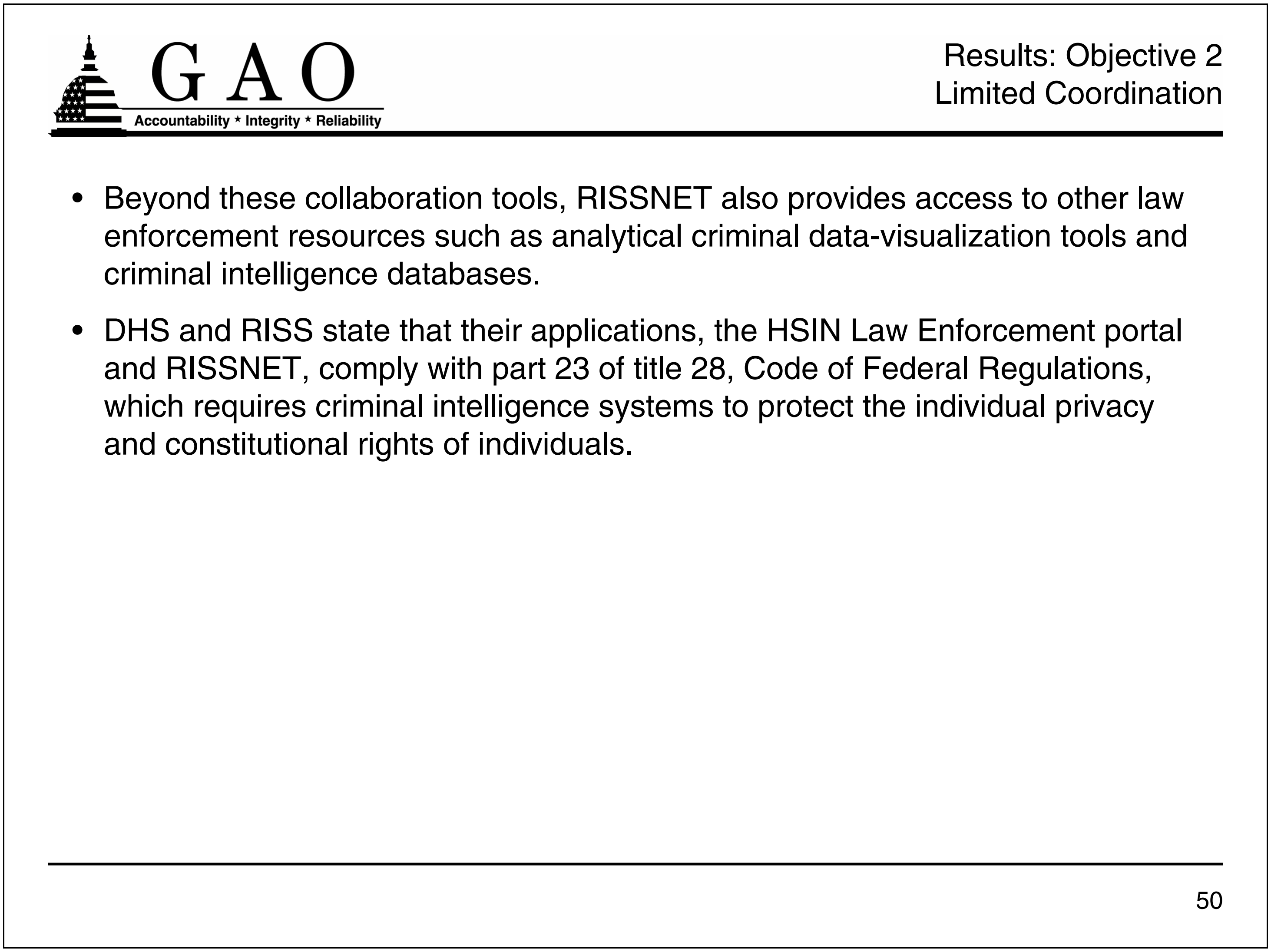
- HSIN and RISS ATIX currently target similar user groups. DHS and the RISS program are independently striving to make their applications available to user communities involved in the prevention of, response to, mitigation of, and recovery from terrorism and disasters across the country. For example, HSIN and RISS ATIX are being used and marketed for use at state fusion centers[13] and other state organizations such as emergency management agencies across the country.

[13] A fusion center is defined as a “collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.”



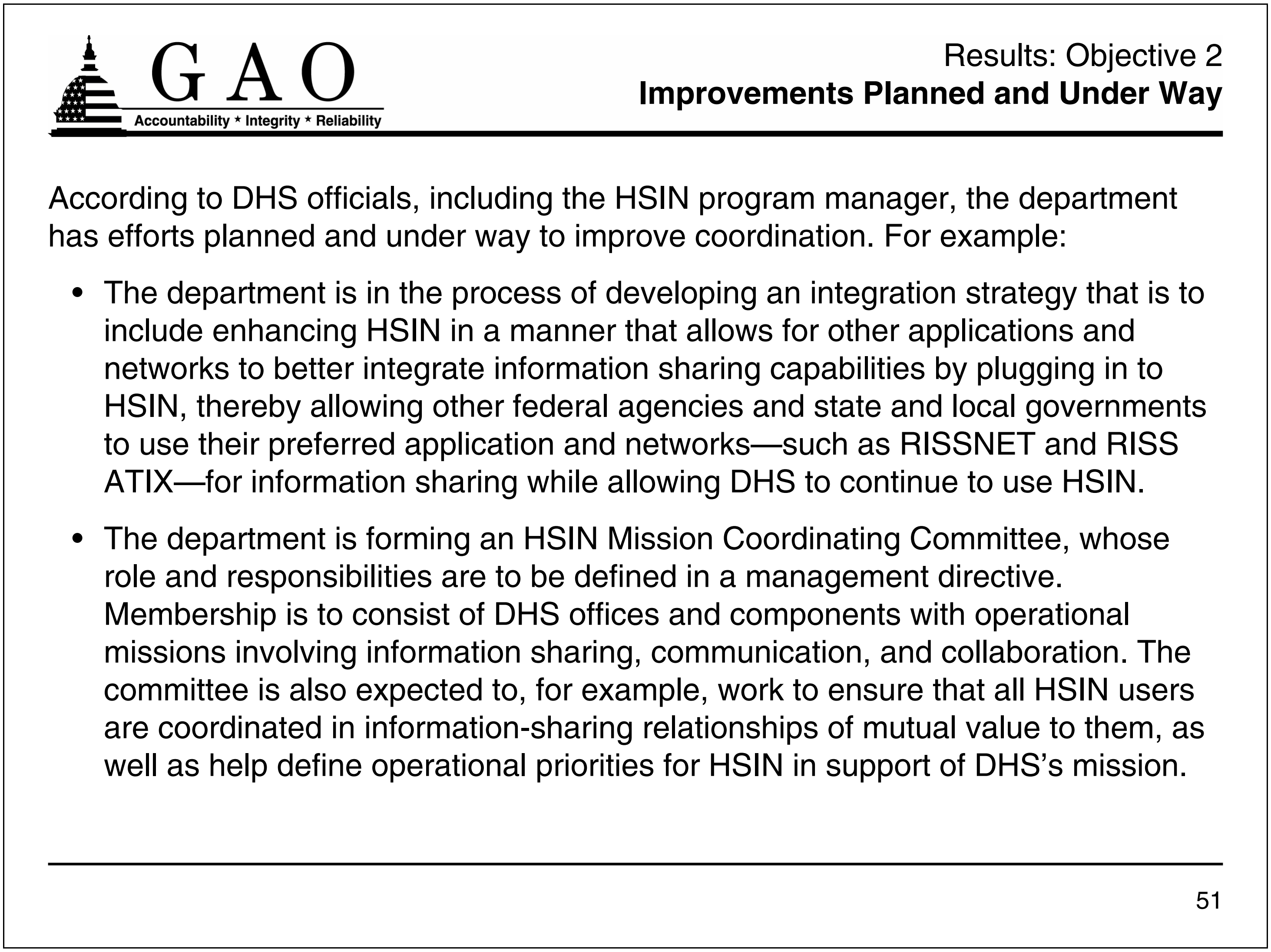
Results: Objective 2
Limited Coordination

- HSIN and RISS applications have similar approaches for sharing information with their users. For example, on each application, users from a particular community—such as emergency management—have access to a portal or community area tailored to the user’s information needs. The community-based portals have similar features focused on user communities. Both applications provide each community with the following features:
  - **Web pages.** Tailored for communities of interest (e.g., law enforcement, emergency management, critical infrastructure sectors), these pages contain general and community-specific news articles, links, and contact information.
  - **Bulletin boards.** Participants can post and discuss information.
  - **Chat tool.** Each community has its own online, real-time, interactive collaboration application.
  - **Document library.** Participants can store and search relevant documents.



Results: Objective 2
Limited Coordination

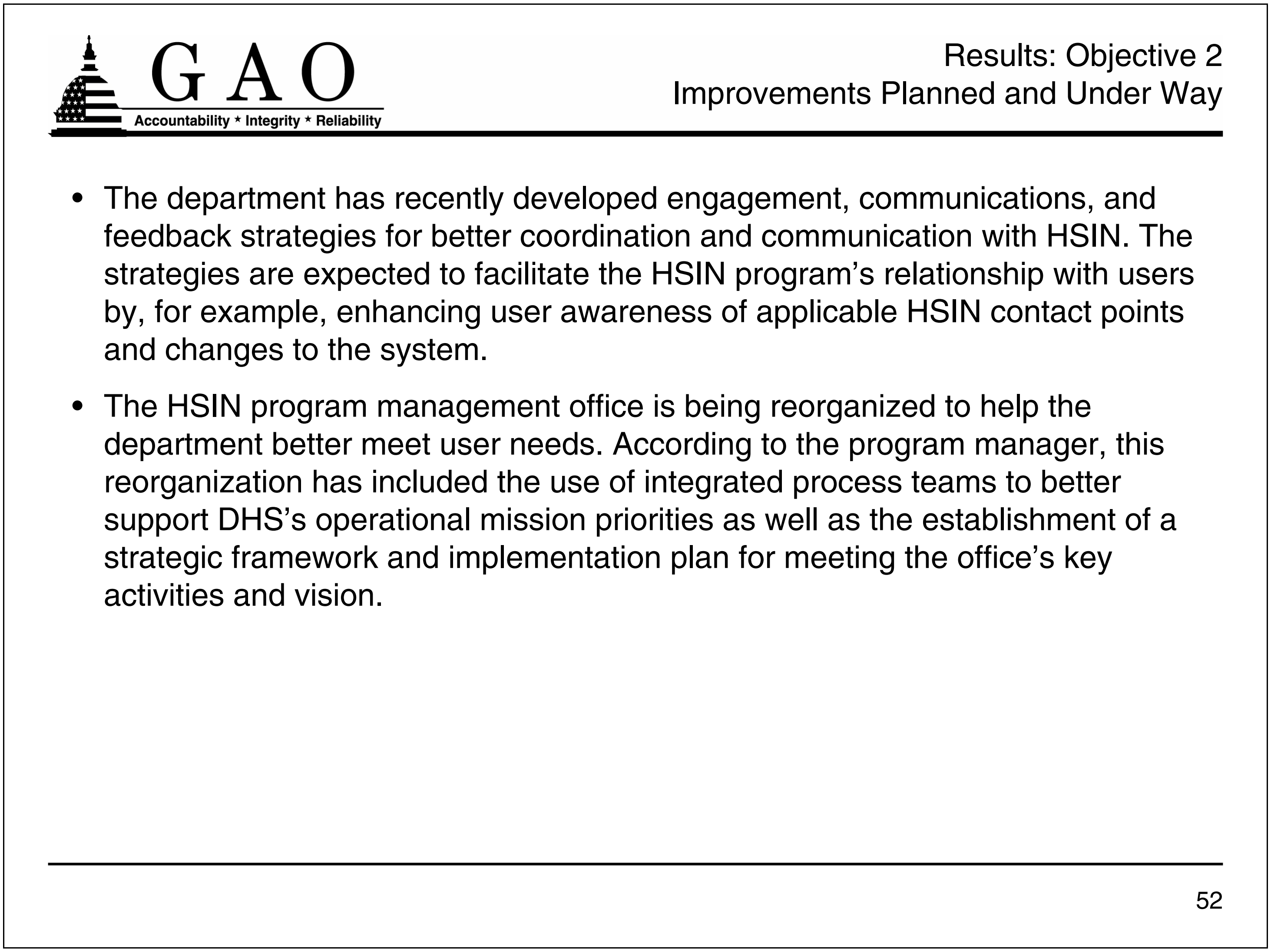
- Beyond these collaboration tools, RISSNET also provides access to other law enforcement resources such as analytical criminal data-visualization tools and criminal intelligence databases.
- DHS and RISS state that their applications, the HSIN Law Enforcement portal and RISSNET, comply with part 23 of title 28, Code of Federal Regulations, which requires criminal intelligence systems to protect the individual privacy and constitutional rights of individuals.



Results: Objective 2
Improvements Planned and Under Way

According to DHS officials, including the HSIN program manager, the department has efforts planned and under way to improve coordination. For example:

- The department is in the process of developing an integration strategy that is to include enhancing HSIN in a manner that allows for other applications and networks to better integrate information sharing capabilities by plugging in to HSIN, thereby allowing other federal agencies and state and local governments to use their preferred application and networks—such as RISSNET and RISS ATIX—for information sharing while allowing DHS to continue to use HSIN.
- The department is forming an HSIN Mission Coordinating Committee, whose role and responsibilities are to be defined in a management directive. Membership is to consist of DHS offices and components with operational missions involving information sharing, communication, and collaboration. The committee is also expected to, for example, work to ensure that all HSIN users are coordinated in information-sharing relationships of mutual value to them, as well as help define operational priorities for HSIN in support of DHS's mission.

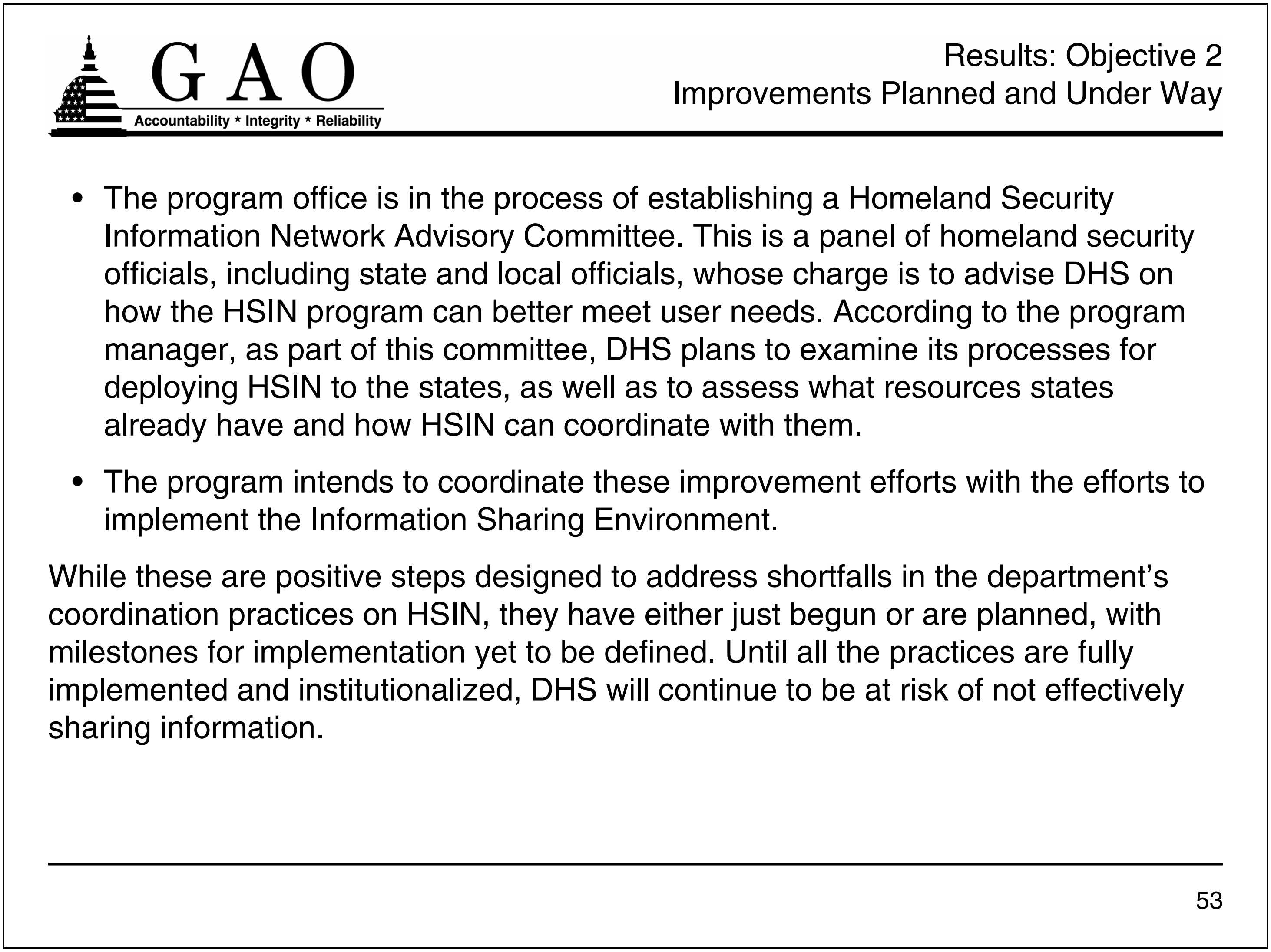


GAO
Accountability * Integrity * Reliability

Results: Objective 2
Improvements Planned and Under Way

- The department has recently developed engagement, communications, and feedback strategies for better coordination and communication with HSIN. The strategies are expected to facilitate the HSIN program's relationship with users by, for example, enhancing user awareness of applicable HSIN contact points and changes to the system.
- The HSIN program management office is being reorganized to help the department better meet user needs. According to the program manager, this reorganization has included the use of integrated process teams to better support DHS's operational mission priorities as well as the establishment of a strategic framework and implementation plan for meeting the office's key activities and vision.

52



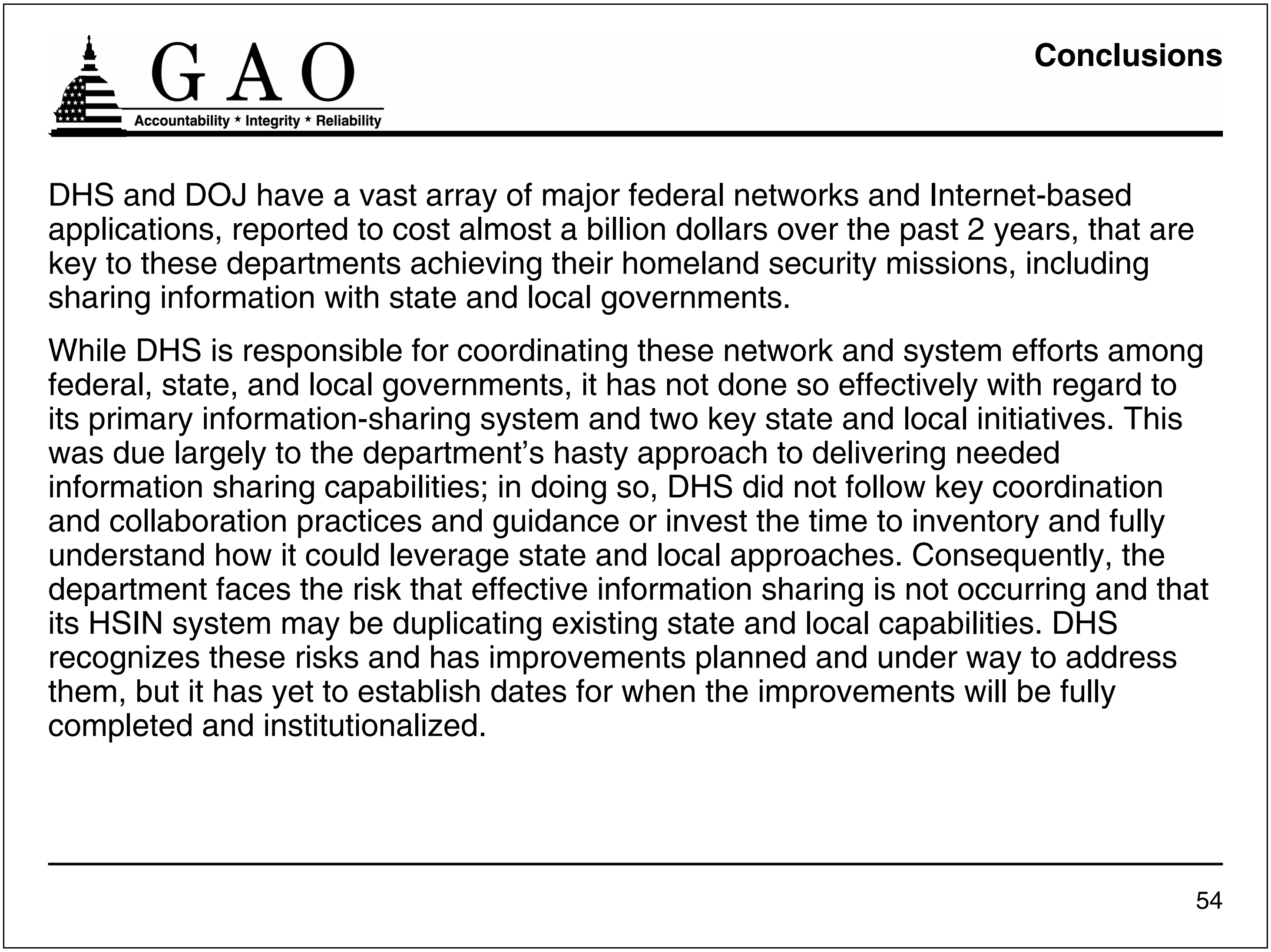
GAO
Accountability * Integrity * Reliability

Results: Objective 2
Improvements Planned and Under Way

- The program office is in the process of establishing a Homeland Security Information Network Advisory Committee. This is a panel of homeland security officials, including state and local officials, whose charge is to advise DHS on how the HSIN program can better meet user needs. According to the program manager, as part of this committee, DHS plans to examine its processes for deploying HSIN to the states, as well as to assess what resources states already have and how HSIN can coordinate with them.
- The program intends to coordinate these improvement efforts with the efforts to implement the Information Sharing Environment.

While these are positive steps designed to address shortfalls in the department’s coordination practices on HSIN, they have either just begun or are planned, with milestones for implementation yet to be defined. Until all the practices are fully implemented and institutionalized, DHS will continue to be at risk of not effectively sharing information.

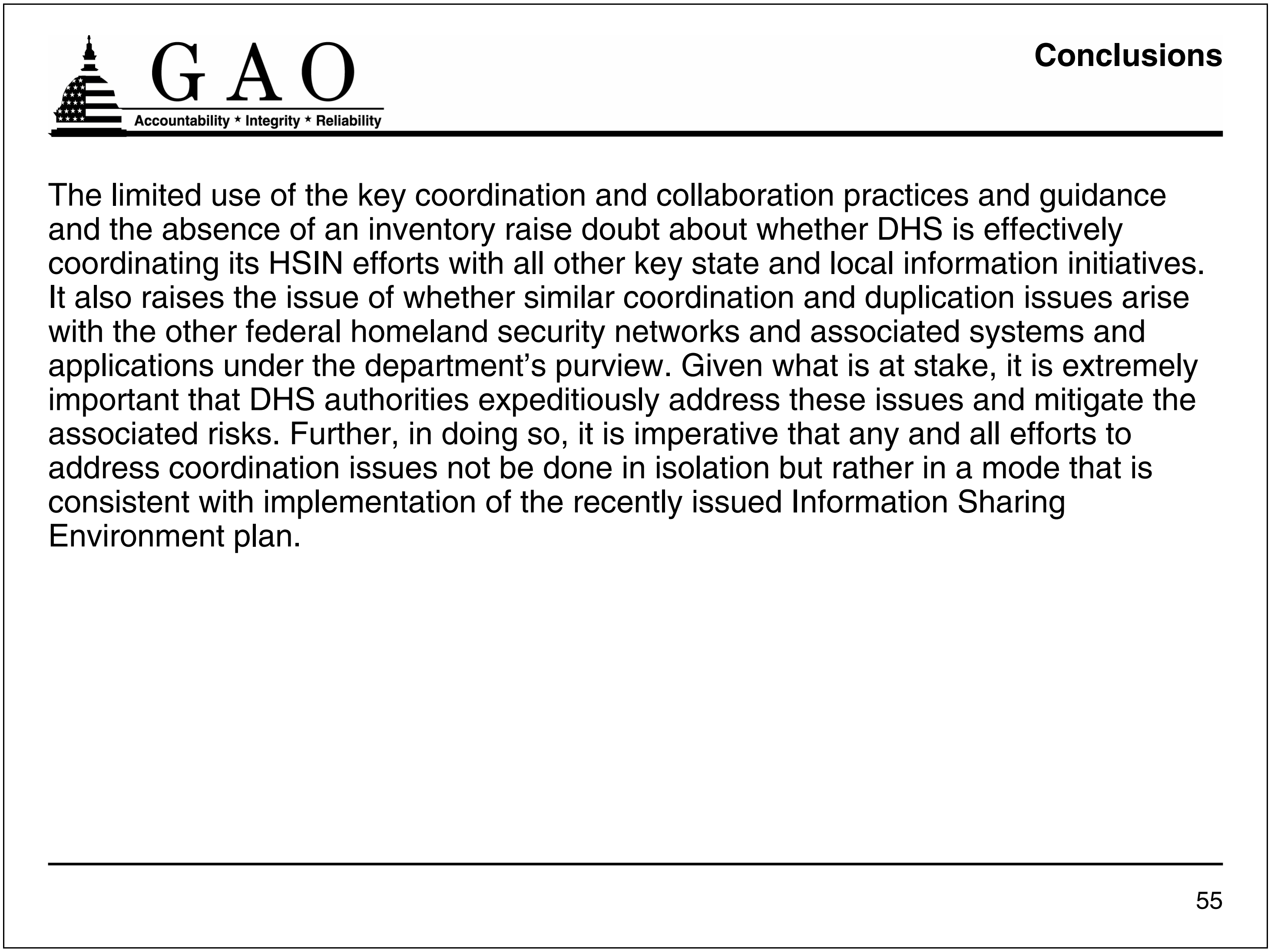
53



Conclusions

DHS and DOJ have a vast array of major federal networks and Internet-based applications, reported to cost almost a billion dollars over the past 2 years, that are key to these departments achieving their homeland security missions, including sharing information with state and local governments.

While DHS is responsible for coordinating these network and system efforts among federal, state, and local governments, it has not done so effectively with regard to its primary information-sharing system and two key state and local initiatives. This was due largely to the department's hasty approach to delivering needed information sharing capabilities; in doing so, DHS did not follow key coordination and collaboration practices and guidance or invest the time to inventory and fully understand how it could leverage state and local approaches. Consequently, the department faces the risk that effective information sharing is not occurring and that its HSIN system may be duplicating existing state and local capabilities. DHS recognizes these risks and has improvements planned and under way to address them, but it has yet to establish dates for when the improvements will be fully completed and institutionalized.

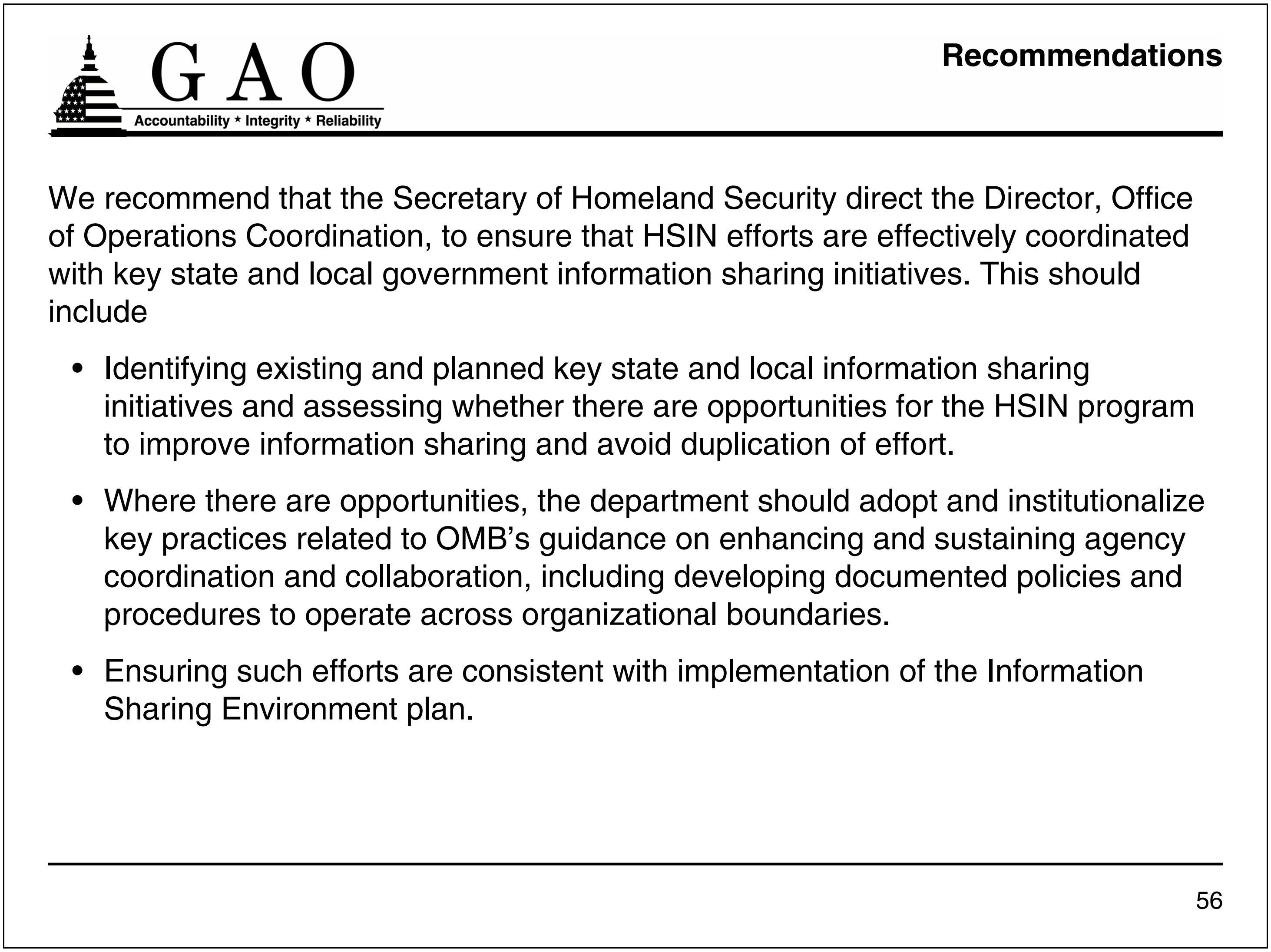


GAO
Accountability * Integrity * Reliability

Conclusions

The limited use of the key coordination and collaboration practices and guidance and the absence of an inventory raise doubt about whether DHS is effectively coordinating its HSIN efforts with all other key state and local information initiatives. It also raises the issue of whether similar coordination and duplication issues arise with the other federal homeland security networks and associated systems and applications under the department's purview. Given what is at stake, it is extremely important that DHS authorities expeditiously address these issues and mitigate the associated risks. Further, in doing so, it is imperative that any and all efforts to address coordination issues not be done in isolation but rather in a mode that is consistent with implementation of the recently issued Information Sharing Environment plan.

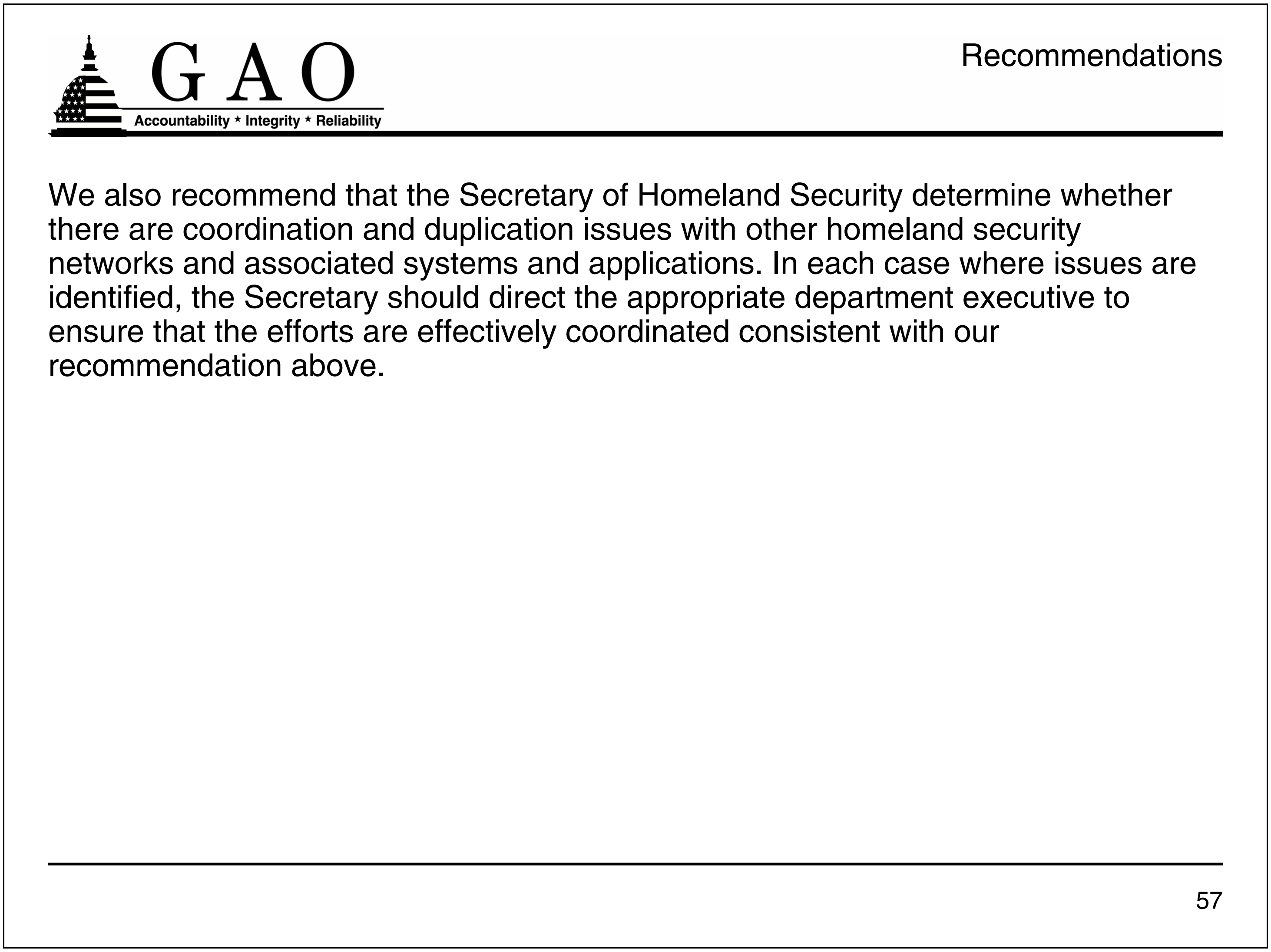
55



Recommendations

We recommend that the Secretary of Homeland Security direct the Director, Office of Operations Coordination, to ensure that HSIN efforts are effectively coordinated with key state and local government information sharing initiatives. This should include

- Identifying existing and planned key state and local information sharing initiatives and assessing whether there are opportunities for the HSIN program to improve information sharing and avoid duplication of effort.
- Where there are opportunities, the department should adopt and institutionalize key practices related to OMB's guidance on enhancing and sustaining agency coordination and collaboration, including developing documented policies and procedures to operate across organizational boundaries.
- Ensuring such efforts are consistent with implementation of the Information Sharing Environment plan.

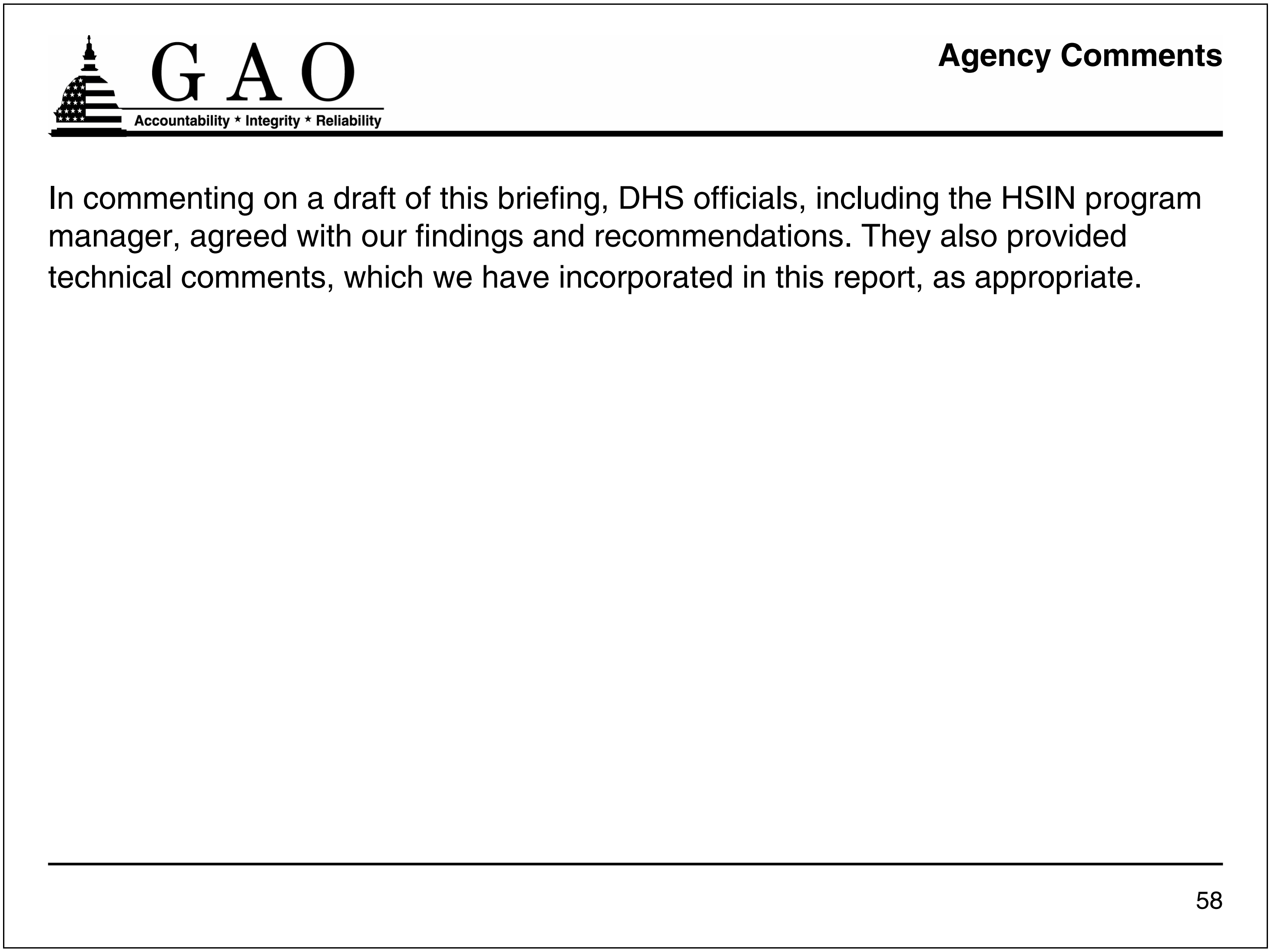


GAO
Accountability * Integrity * Reliability

Recommendations

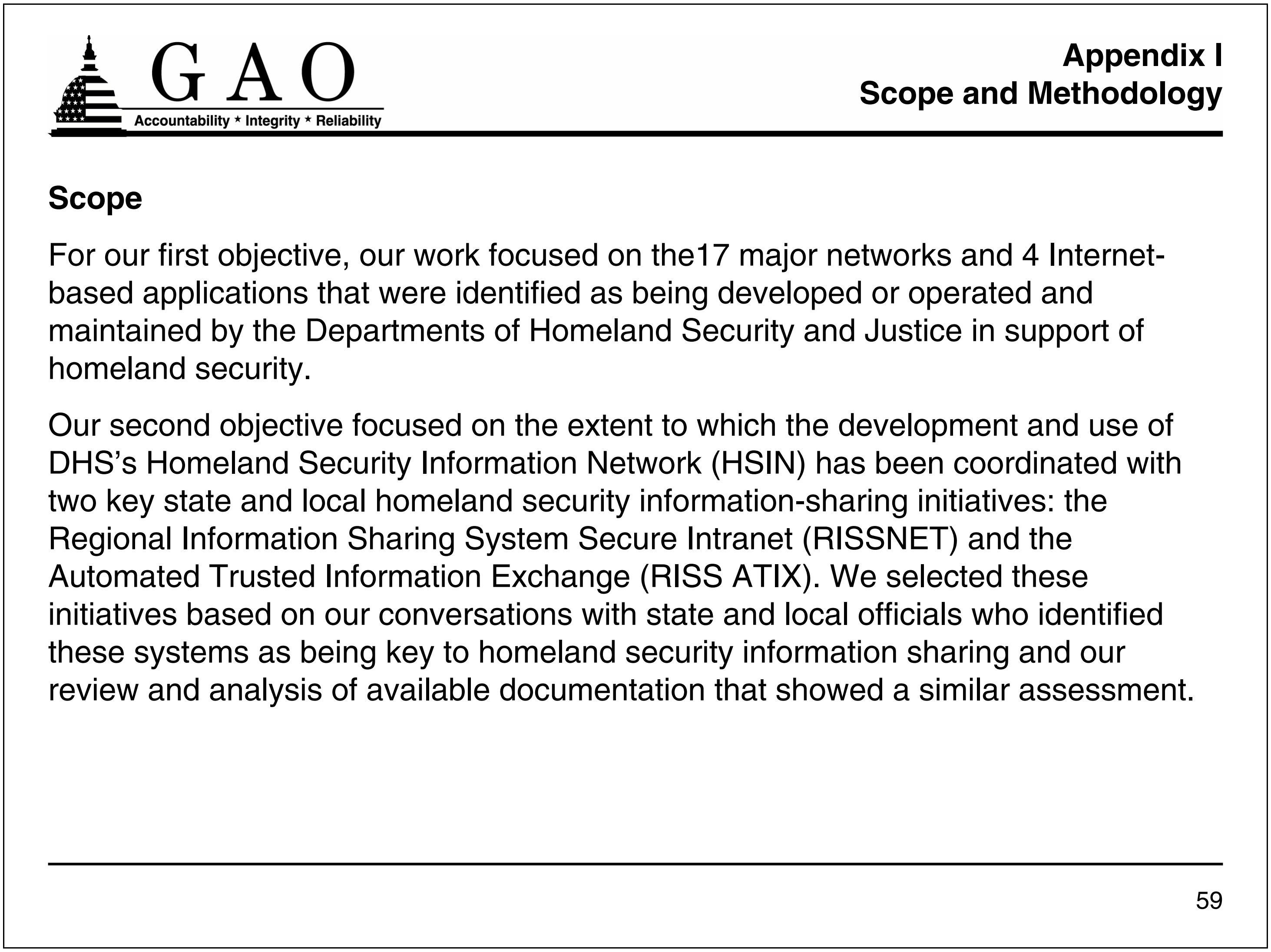
We also recommend that the Secretary of Homeland Security determine whether there are coordination and duplication issues with other homeland security networks and associated systems and applications. In each case where issues are identified, the Secretary should direct the appropriate department executive to ensure that the efforts are effectively coordinated consistent with our recommendation above.

57



Agency Comments

In commenting on a draft of this briefing, DHS officials, including the HSIN program manager, agreed with our findings and recommendations. They also provided technical comments, which we have incorporated in this report, as appropriate.



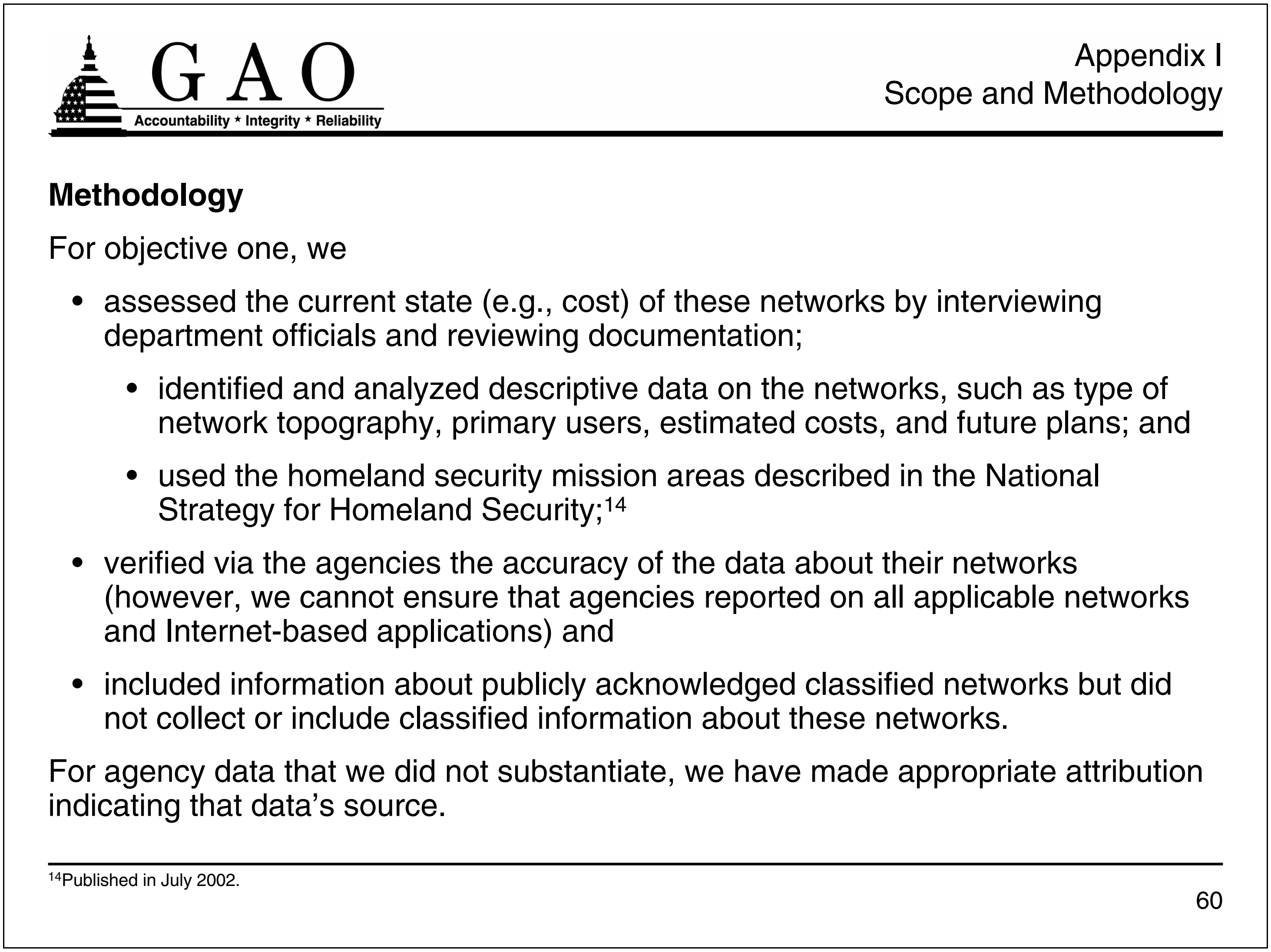
GAO
Accountability * Integrity * Reliability

Appendix I
Scope and Methodology

Scope

For our first objective, our work focused on the17 major networks and 4 Internet-based applications that were identified as being developed or operated and maintained by the Departments of Homeland Security and Justice in support of homeland security.

Our second objective focused on the extent to which the development and use of DHS's Homeland Security Information Network (HSIN) has been coordinated with two key state and local homeland security information-sharing initiatives: the Regional Information Sharing System Secure Intranet (RISSNET) and the Automated Trusted Information Exchange (RISS ATIX). We selected these initiatives based on our conversations with state and local officials who identified these systems as being key to homeland security information sharing and our review and analysis of available documentation that showed a similar assessment.



GAO
Accountability * Integrity * Reliability

Appendix I
Scope and Methodology

Methodology

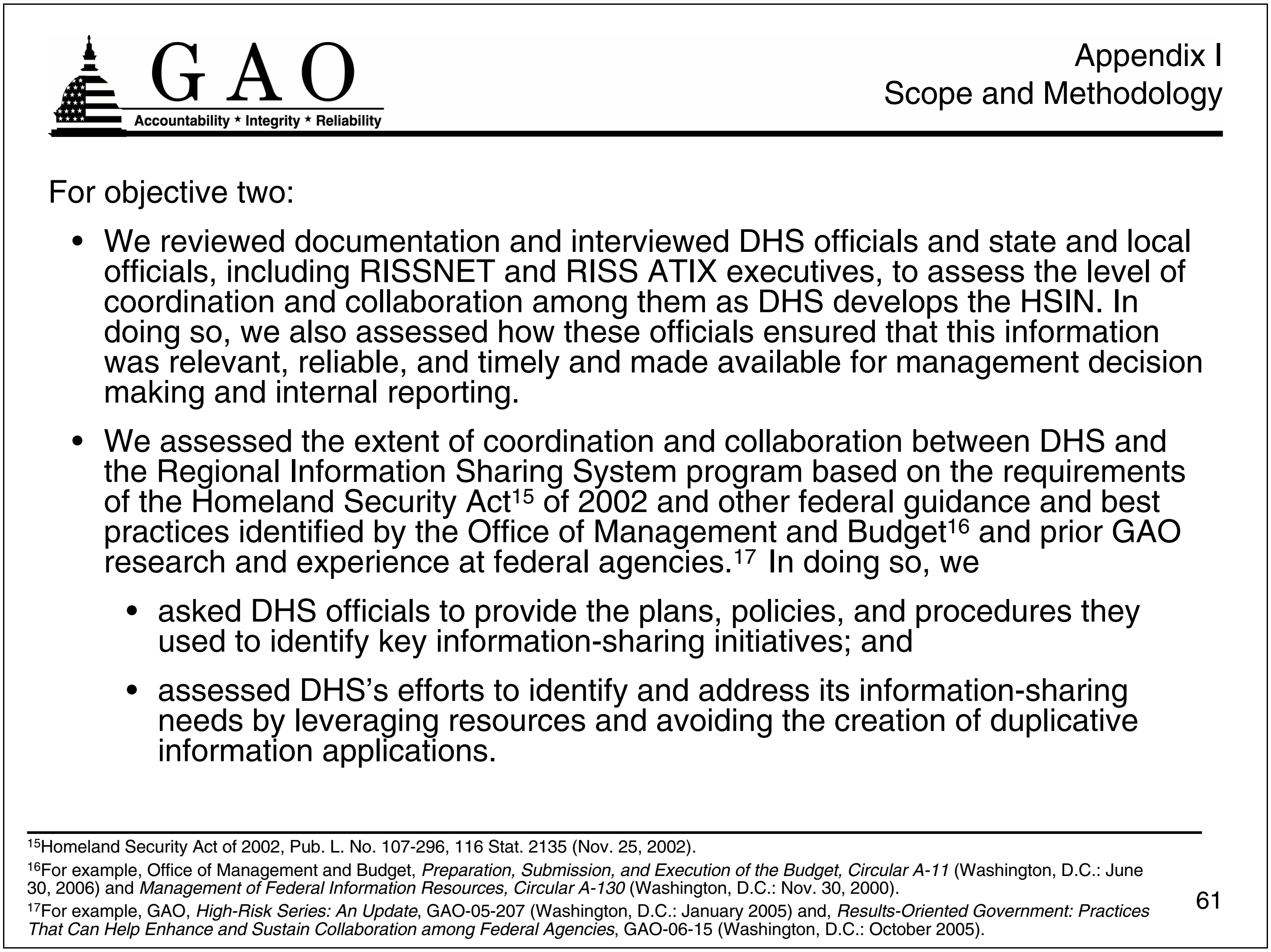
For objective one, we

- assessed the current state (e.g., cost) of these networks by interviewing department officials and reviewing documentation;
  - identified and analyzed descriptive data on the networks, such as type of network topography, primary users, estimated costs, and future plans; and
  - used the homeland security mission areas described in the National Strategy for Homeland Security;[14]
- verified via the agencies the accuracy of the data about their networks (however, we cannot ensure that agencies reported on all applicable networks and Internet-based applications) and
- included information about publicly acknowledged classified networks but did not collect or include classified information about these networks.

For agency data that we did not substantiate, we have made appropriate attribution indicating that data's source.

[14] Published in July 2002.

60



Appendix I
Scope and Methodology

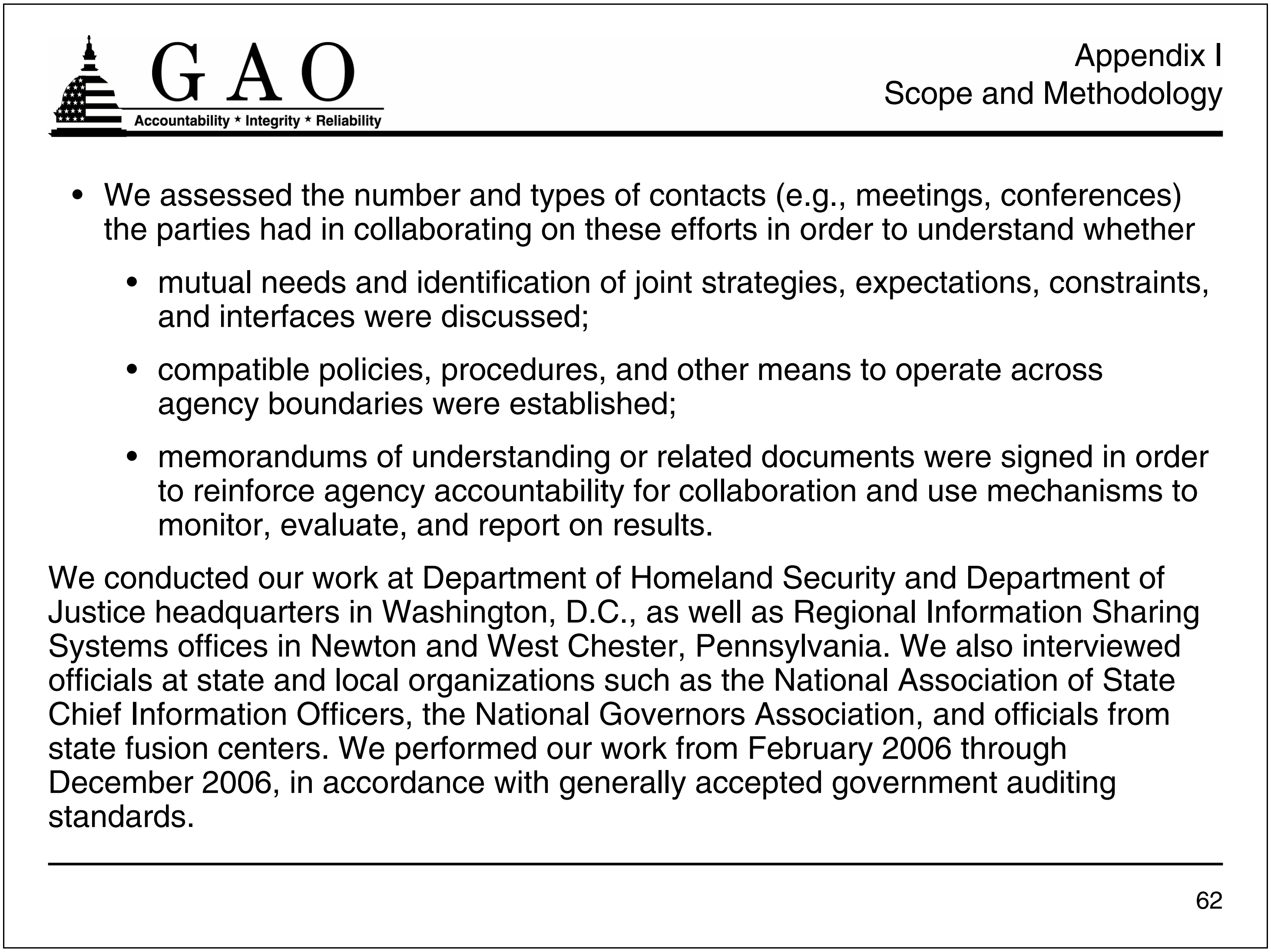
For objective two:

- We reviewed documentation and interviewed DHS officials and state and local officials, including RISSNET and RISS ATIX executives, to assess the level of coordination and collaboration among them as DHS develops the HSIN. In doing so, we also assessed how these officials ensured that this information was relevant, reliable, and timely and made available for management decision making and internal reporting.
- We assessed the extent of coordination and collaboration between DHS and the Regional Information Sharing System program based on the requirements of the Homeland Security Act[15] of 2002 and other federal guidance and best practices identified by the Office of Management and Budget[16] and prior GAO research and experience at federal agencies.[17] In doing so, we
  - asked DHS officials to provide the plans, policies, and procedures they used to identify key information-sharing initiatives; and
  - assessed DHS's efforts to identify and address its information-sharing needs by leveraging resources and avoiding the creation of duplicative information applications.

[15] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (Nov. 25, 2002).

[16] For example, Office of Management and Budget, *Preparation, Submission, and Execution of the Budget, Circular A-11* (Washington, D.C.: June 30, 2006) and *Management of Federal Information Resources, Circular A-130* (Washington, D.C.: Nov. 30, 2000).

[17] For example, GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005) and, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: October 2005).

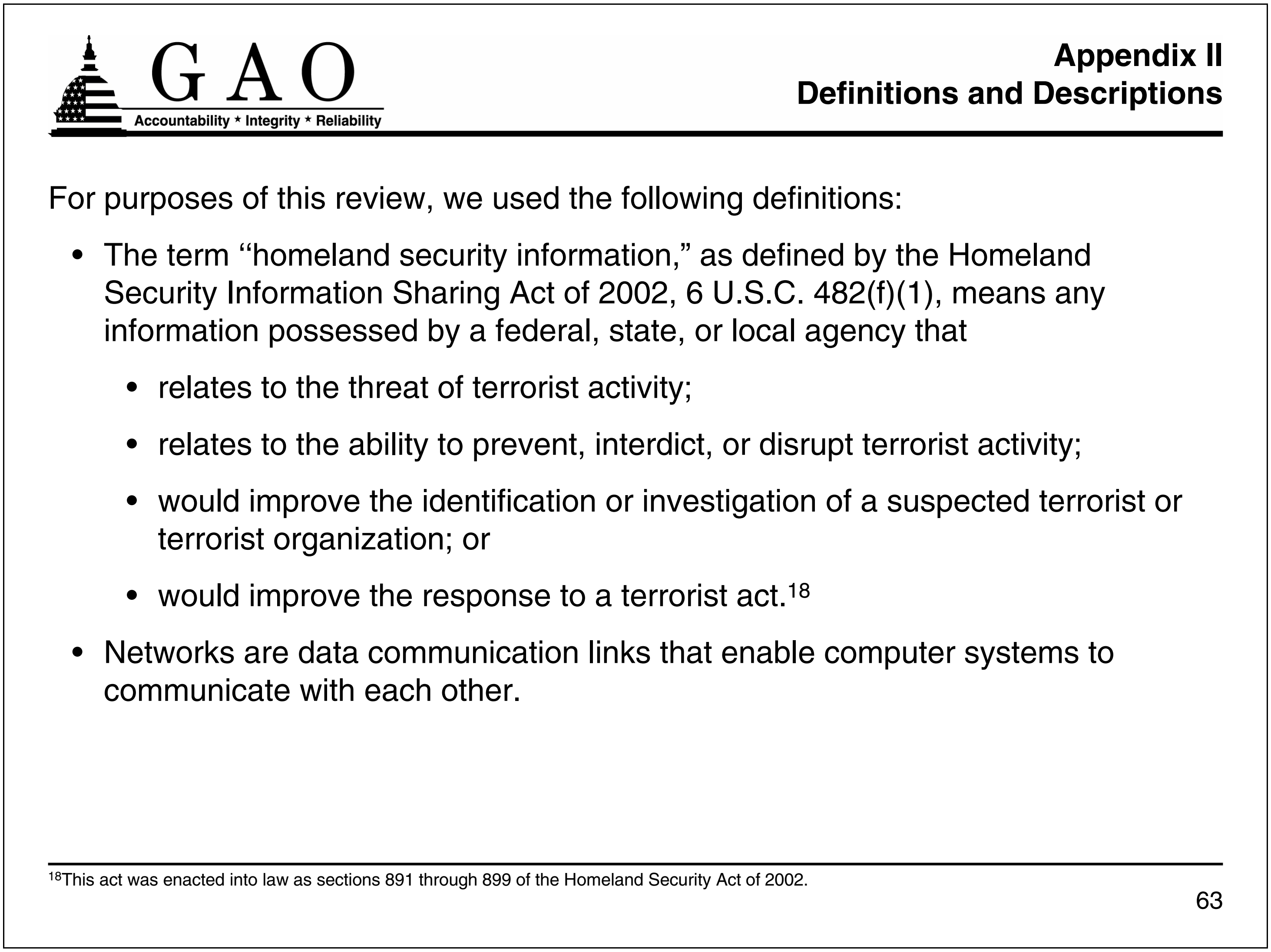


GAO Accountability * Integrity * Reliability

Appendix I
Scope and Methodology

- We assessed the number and types of contacts (e.g., meetings, conferences) the parties had in collaborating on these efforts in order to understand whether
  - mutual needs and identification of joint strategies, expectations, constraints, and interfaces were discussed;
  - compatible policies, procedures, and other means to operate across agency boundaries were established;
  - memorandums of understanding or related documents were signed in order to reinforce agency accountability for collaboration and use mechanisms to monitor, evaluate, and report on results.

We conducted our work at Department of Homeland Security and Department of Justice headquarters in Washington, D.C., as well as Regional Information Sharing Systems offices in Newton and West Chester, Pennsylvania. We also interviewed officials at state and local organizations such as the National Association of State Chief Information Officers, the National Governors Association, and officials from state fusion centers. We performed our work from February 2006 through December 2006, in accordance with generally accepted government auditing standards.



GAO
Accountability * Integrity * Reliability

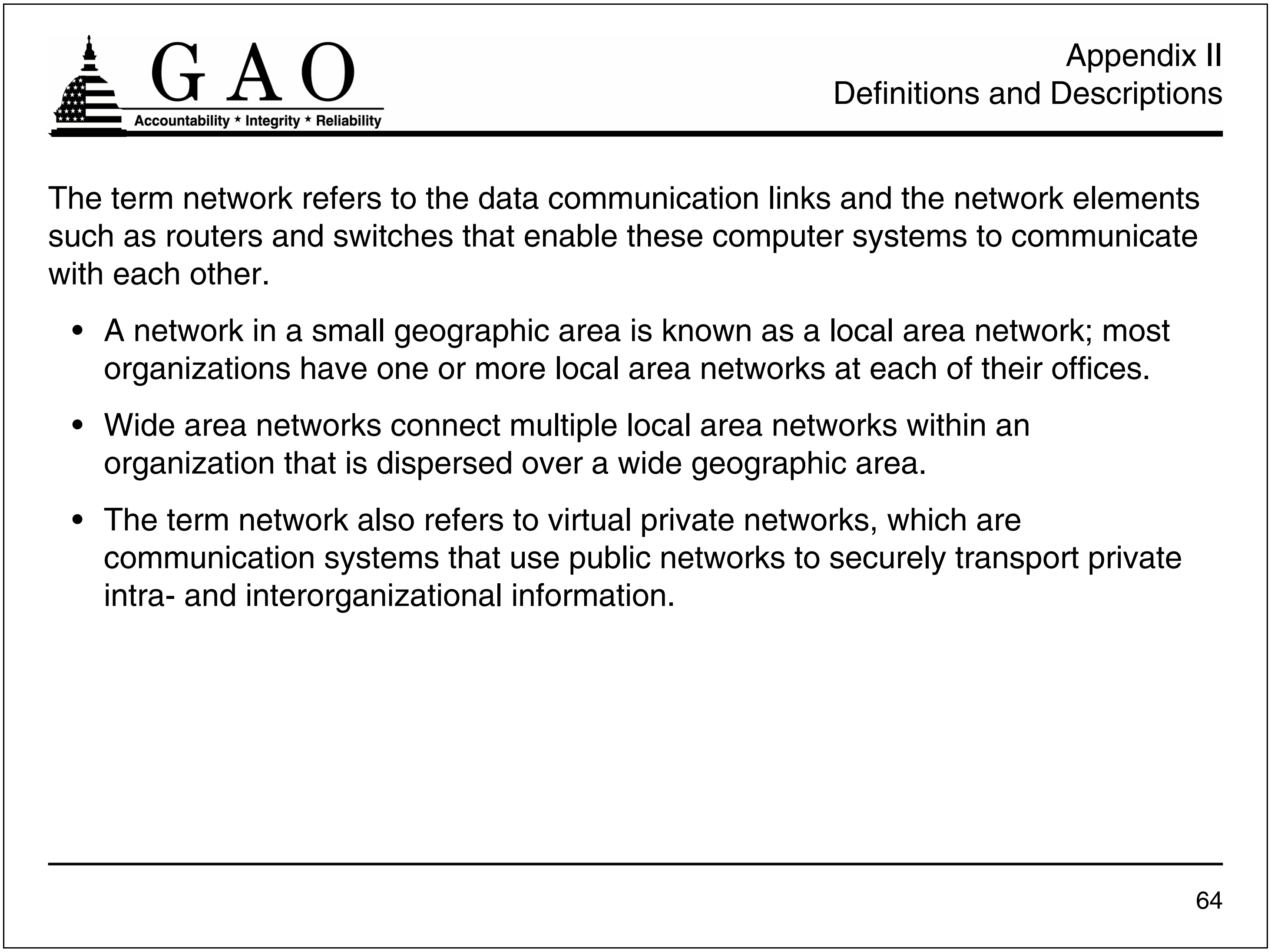
Appendix II
Definitions and Descriptions

For purposes of this review, we used the following definitions:

- The term ‘‘homeland security information,” as defined by the Homeland Security Information Sharing Act of 2002, 6 U.S.C. 482(f)(1), means any information possessed by a federal, state, or local agency that
  - relates to the threat of terrorist activity;
  - relates to the ability to prevent, interdict, or disrupt terrorist activity;
  - would improve the identification or investigation of a suspected terrorist or terrorist organization; or
  - would improve the response to a terrorist act.[18]
- Networks are data communication links that enable computer systems to communicate with each other.

[18] This act was enacted into law as sections 891 through 899 of the Homeland Security Act of 2002.

63



Appendix II
Definitions and Descriptions

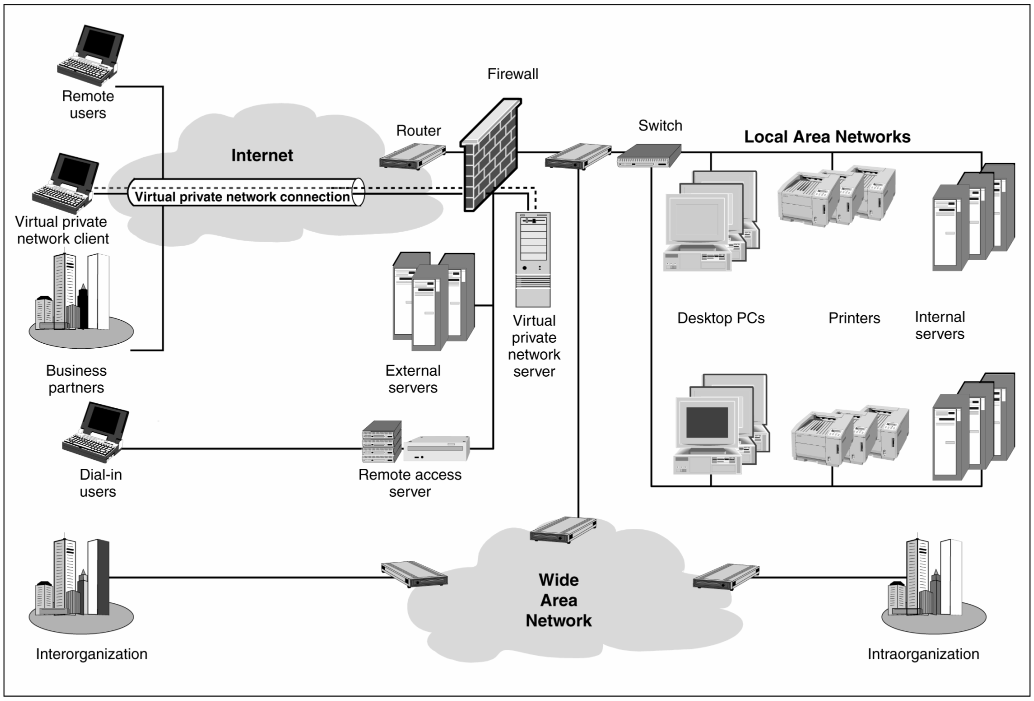
The term network refers to the data communication links and the network elements such as routers and switches that enable these computer systems to communicate with each other.

- A network in a small geographic area is known as a local area network; most organizations have one or more local area networks at each of their offices.
- Wide area networks connect multiple local area networks within an organization that is dispersed over a wide geographic area.
- The term network also refers to virtual private networks, which are communication systems that use public networks to securely transport private intra- and interorganizational information.

GAO
Accountability * Integrity * Reliability

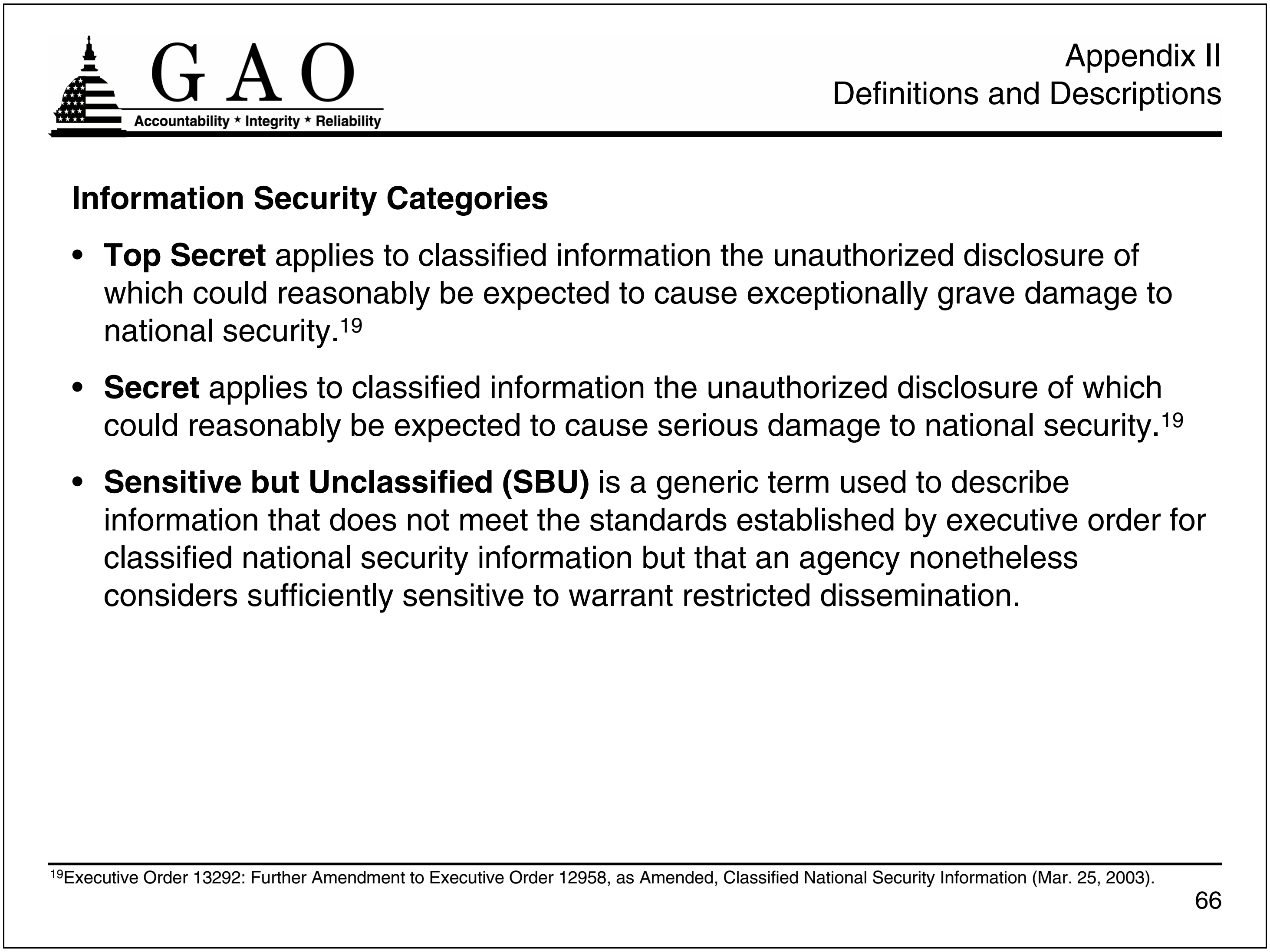
Appendix II
Definitions and Descriptions

Computer systems are connected to local area networks and wide area networks and are often connected to the Internet.



Source: GAO analysis and Art Explosion (clip art).

65



Appendix II
Definitions and Descriptions

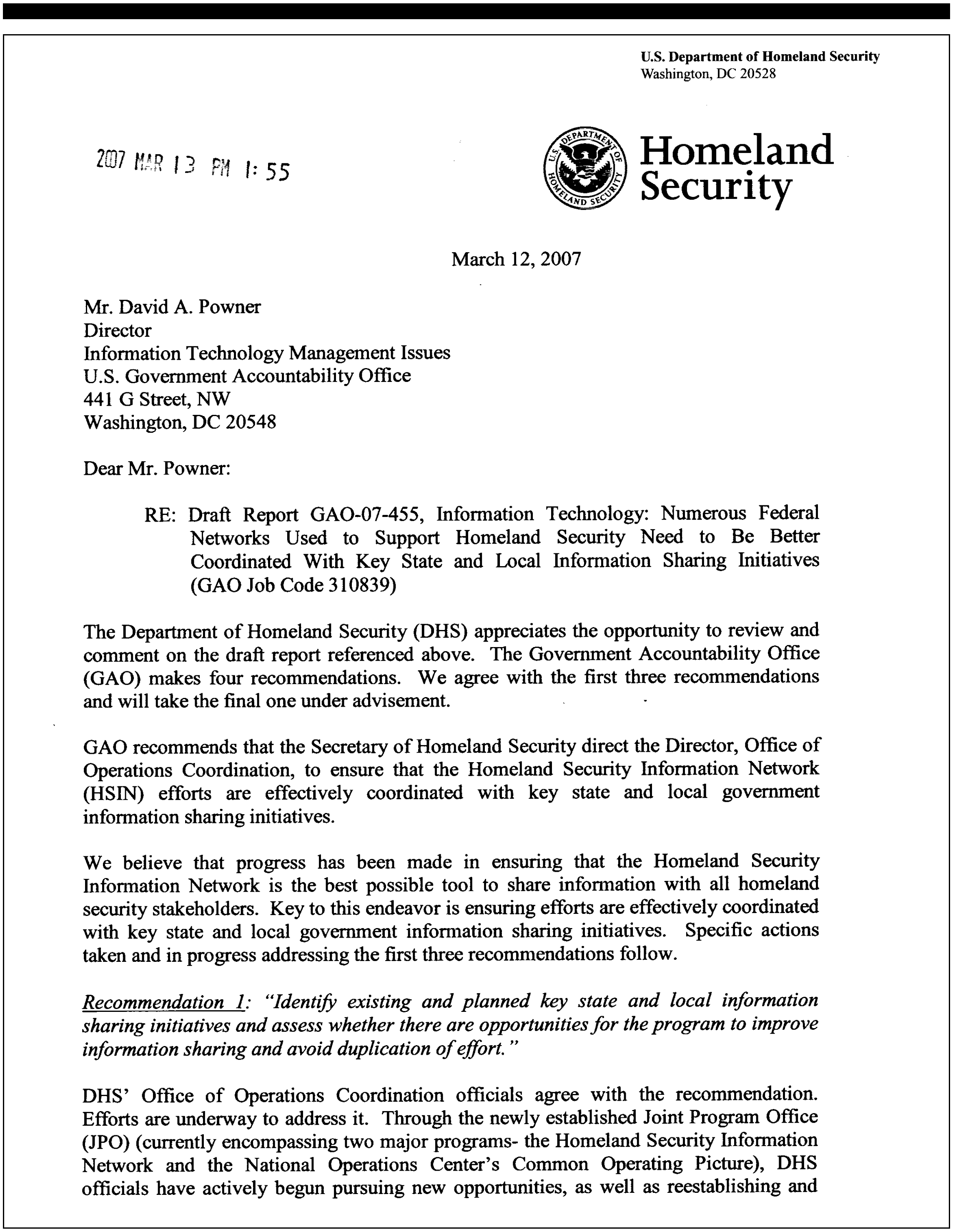
Information Security Categories

- **Top Secret** applies to classified information the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to national security.[19]
- **Secret** applies to classified information the unauthorized disclosure of which could reasonably be expected to cause serious damage to national security.[19]
- **Sensitive but Unclassified (SBU)** is a generic term used to describe information that does not meet the standards established by executive order for classified national security information but that an agency nonetheless considers sufficiently sensitive to warrant restricted dissemination.

[19] Executive Order 13292: Further Amendment to Executive Order 12958, as Amended, Classified National Security Information (Mar. 25, 2003).

Appendix II

Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

2007 MAR 13 PM 1:55

Homeland
Security

March 12, 2007

Mr. David A. Powner
Director
Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Powner:

RE: Draft Report GAO-07-455, Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated With Key State and Local Information Sharing Initiatives (GAO Job Code 310839)

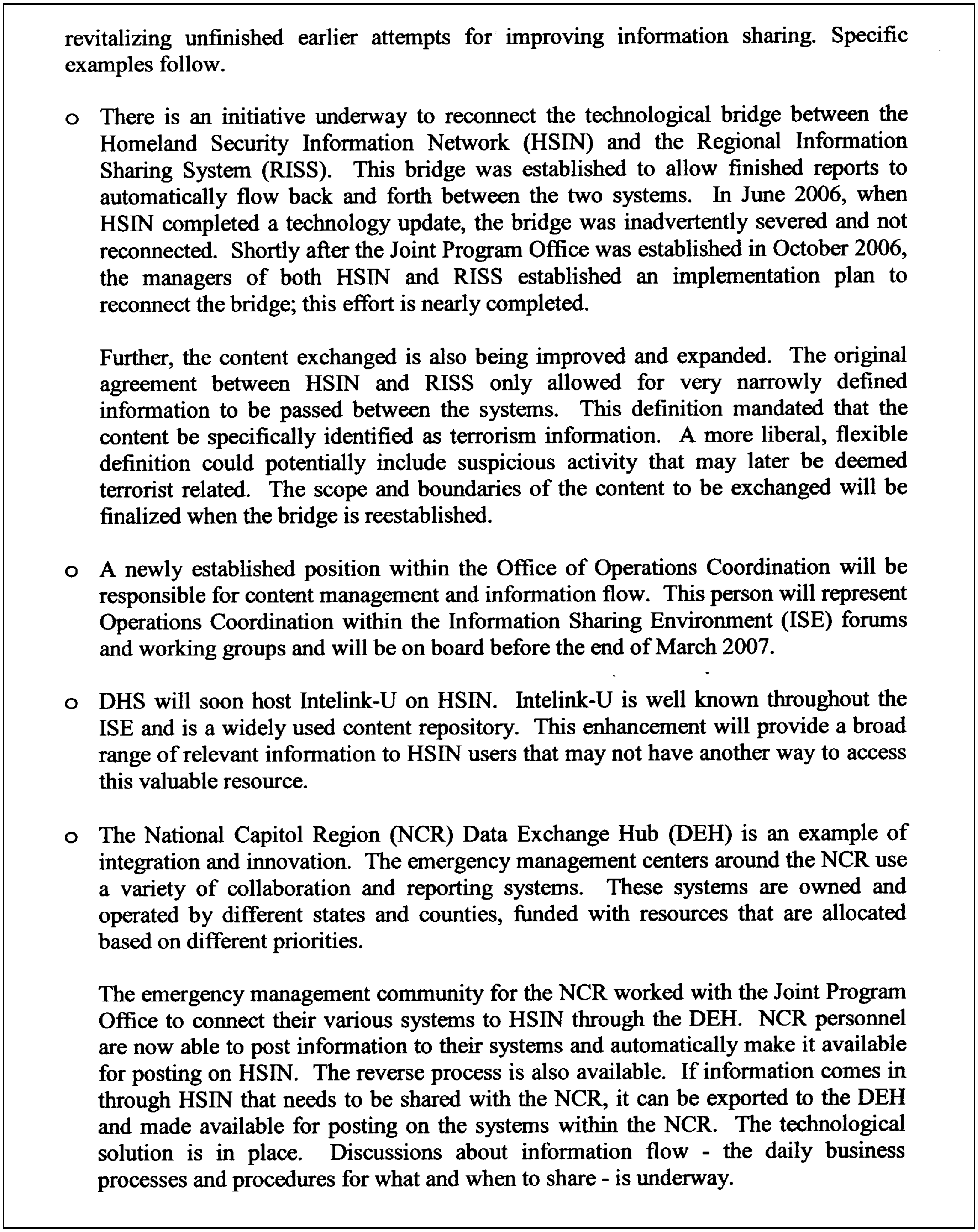
The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the draft report referenced above. The Government Accountability Office (GAO) makes four recommendations. We agree with the first three recommendations and will take the final one under advisement.

GAO recommends that the Secretary of Homeland Security direct the Director, Office of Operations Coordination, to ensure that the Homeland Security Information Network (HSIN) efforts are effectively coordinated with key state and local government information sharing initiatives.

We believe that progress has been made in ensuring that the Homeland Security Information Network is the best possible tool to share information with all homeland security stakeholders. Key to this endeavor is ensuring efforts are effectively coordinated with key state and local government information sharing initiatives. Specific actions taken and in progress addressing the first three recommendations follow.

<u>Recommendation 1</u>: *"Identify existing and planned key state and local information sharing initiatives and assess whether there are opportunities for the program to improve information sharing and avoid duplication of effort."*

DHS' Office of Operations Coordination officials agree with the recommendation. Efforts are underway to address it. Through the newly established Joint Program Office (JPO) (currently encompassing two major programs- the Homeland Security Information Network and the National Operations Center's Common Operating Picture), DHS officials have actively begun pursuing new opportunities, as well as reestablishing and



revitalizing unfinished earlier attempts for improving information sharing. Specific examples follow.

- There is an initiative underway to reconnect the technological bridge between the Homeland Security Information Network (HSIN) and the Regional Information Sharing System (RISS). This bridge was established to allow finished reports to automatically flow back and forth between the two systems. In June 2006, when HSIN completed a technology update, the bridge was inadvertently severed and not reconnected. Shortly after the Joint Program Office was established in October 2006, the managers of both HSIN and RISS established an implementation plan to reconnect the bridge; this effort is nearly completed.

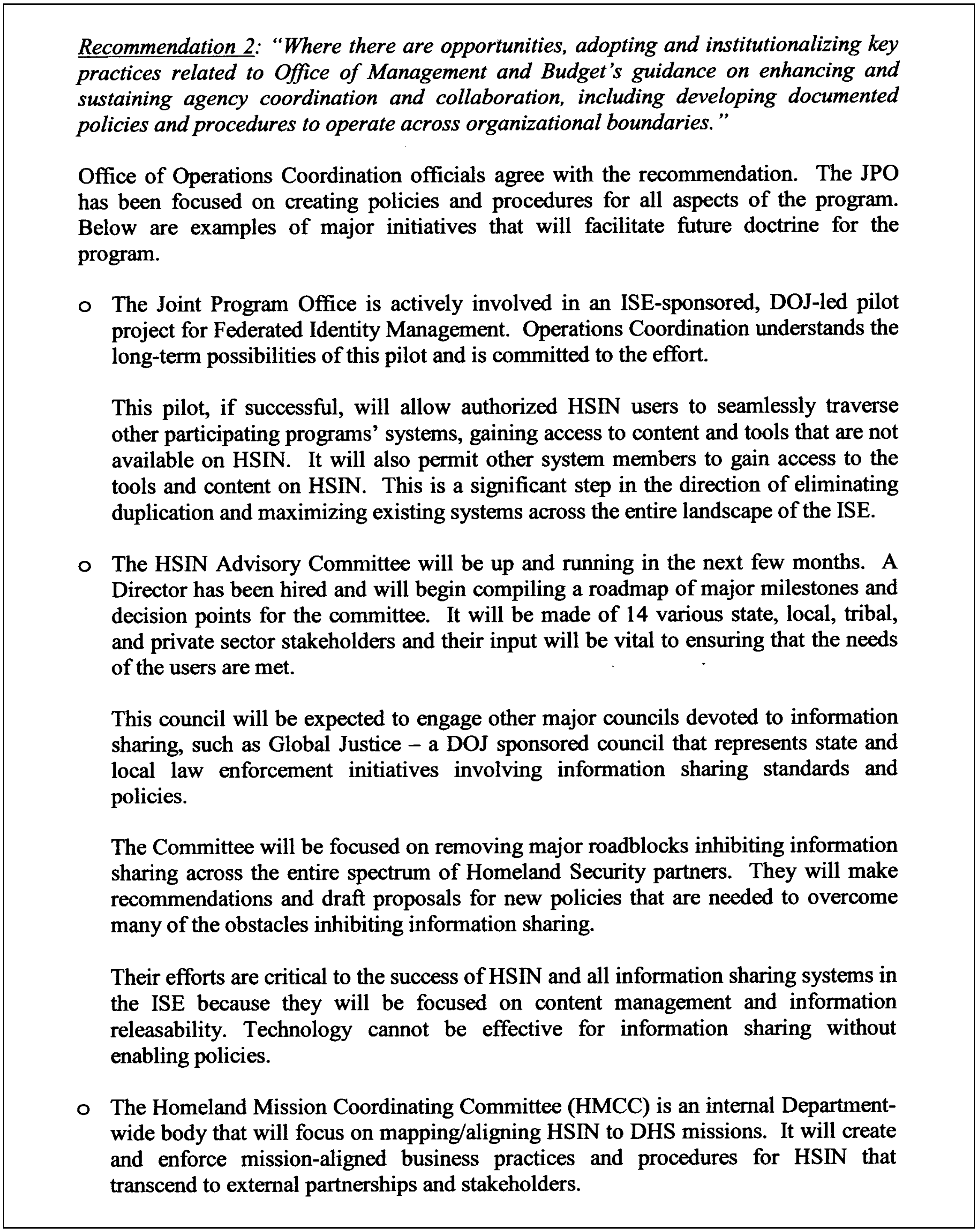
  Further, the content exchanged is also being improved and expanded. The original agreement between HSIN and RISS only allowed for very narrowly defined information to be passed between the systems. This definition mandated that the content be specifically identified as terrorism information. A more liberal, flexible definition could potentially include suspicious activity that may later be deemed terrorist related. The scope and boundaries of the content to be exchanged will be finalized when the bridge is reestablished.

- A newly established position within the Office of Operations Coordination will be responsible for content management and information flow. This person will represent Operations Coordination within the Information Sharing Environment (ISE) forums and working groups and will be on board before the end of March 2007.

- DHS will soon host Intelink-U on HSIN. Intelink-U is well known throughout the ISE and is a widely used content repository. This enhancement will provide a broad range of relevant information to HSIN users that may not have another way to access this valuable resource.

- The National Capitol Region (NCR) Data Exchange Hub (DEH) is an example of integration and innovation. The emergency management centers around the NCR use a variety of collaboration and reporting systems. These systems are owned and operated by different states and counties, funded with resources that are allocated based on different priorities.

  The emergency management community for the NCR worked with the Joint Program Office to connect their various systems to HSIN through the DEH. NCR personnel are now able to post information to their systems and automatically make it available for posting on HSIN. The reverse process is also available. If information comes in through HSIN that needs to be shared with the NCR, it can be exported to the DEH and made available for posting on the systems within the NCR. The technological solution is in place. Discussions about information flow - the daily business processes and procedures for what and when to share - is underway.



<u>Recommendation 2</u>: *"Where there are opportunities, adopting and institutionalizing key practices related to Office of Management and Budget's guidance on enhancing and sustaining agency coordination and collaboration, including developing documented policies and procedures to operate across organizational boundaries."*

Office of Operations Coordination officials agree with the recommendation. The JPO has been focused on creating policies and procedures for all aspects of the program. Below are examples of major initiatives that will facilitate future doctrine for the program.

- The Joint Program Office is actively involved in an ISE-sponsored, DOJ-led pilot project for Federated Identity Management. Operations Coordination understands the long-term possibilities of this pilot and is committed to the effort.

  This pilot, if successful, will allow authorized HSIN users to seamlessly traverse other participating programs' systems, gaining access to content and tools that are not available on HSIN. It will also permit other system members to gain access to the tools and content on HSIN. This is a significant step in the direction of eliminating duplication and maximizing existing systems across the entire landscape of the ISE.

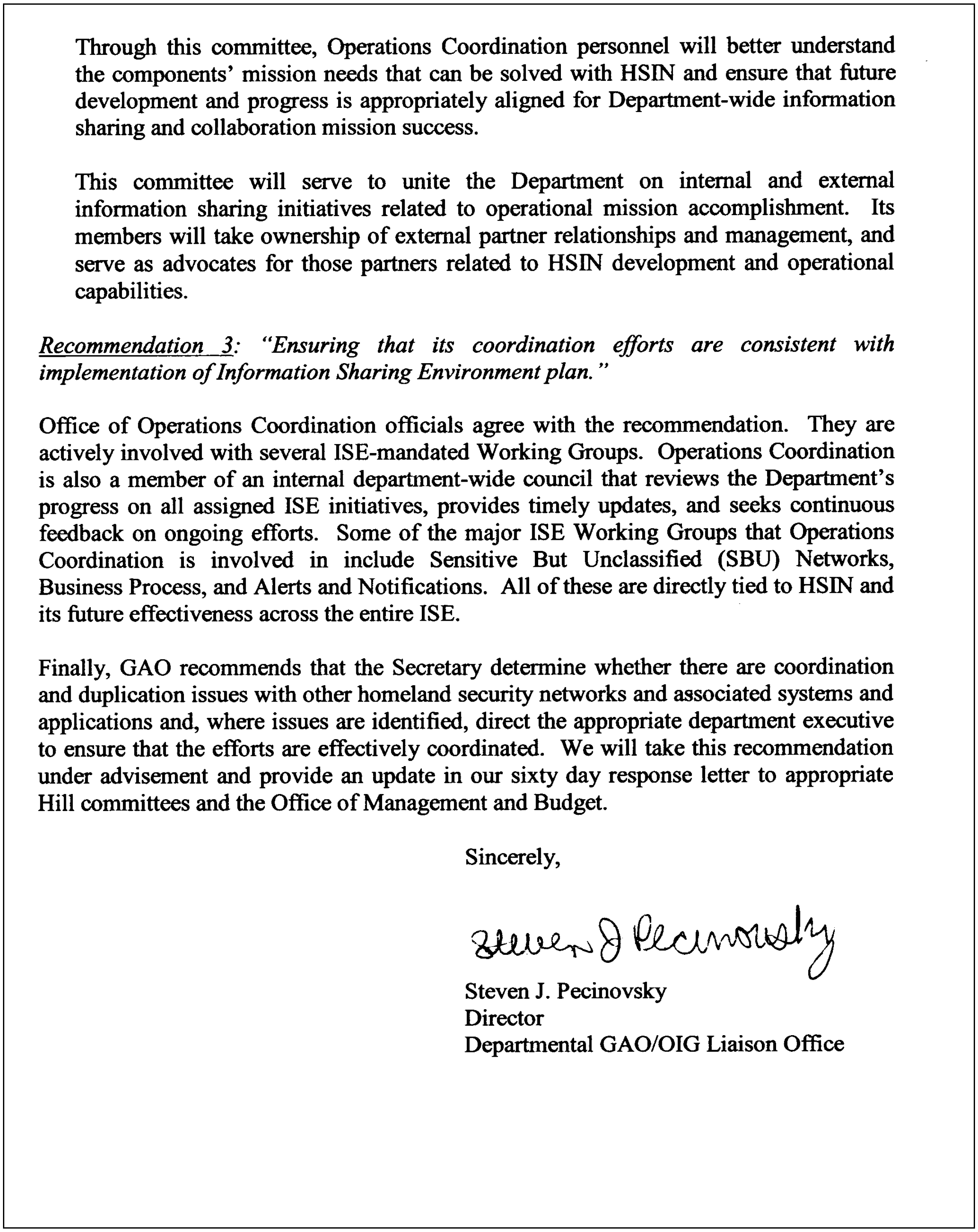
- The HSIN Advisory Committee will be up and running in the next few months. A Director has been hired and will begin compiling a roadmap of major milestones and decision points for the committee. It will be made of 14 various state, local, tribal, and private sector stakeholders and their input will be vital to ensuring that the needs of the users are met.

  This council will be expected to engage other major councils devoted to information sharing, such as Global Justice – a DOJ sponsored council that represents state and local law enforcement initiatives involving information sharing standards and policies.

  The Committee will be focused on removing major roadblocks inhibiting information sharing across the entire spectrum of Homeland Security partners. They will make recommendations and draft proposals for new policies that are needed to overcome many of the obstacles inhibiting information sharing.

  Their efforts are critical to the success of HSIN and all information sharing systems in the ISE because they will be focused on content management and information releasability. Technology cannot be effective for information sharing without enabling policies.

- The Homeland Mission Coordinating Committee (HMCC) is an internal Department-wide body that will focus on mapping/aligning HSIN to DHS missions. It will create and enforce mission-aligned business practices and procedures for HSIN that transcend to external partnerships and stakeholders.



Through this committee, Operations Coordination personnel will better understand the components' mission needs that can be solved with HSIN and ensure that future development and progress is appropriately aligned for Department-wide information sharing and collaboration mission success.

This committee will serve to unite the Department on internal and external information sharing initiatives related to operational mission accomplishment. Its members will take ownership of external partner relationships and management, and serve as advocates for those partners related to HSIN development and operational capabilities.

Recommendation 3: *"Ensuring that its coordination efforts are consistent with implementation of Information Sharing Environment plan."*

Office of Operations Coordination officials agree with the recommendation. They are actively involved with several ISE-mandated Working Groups. Operations Coordination is also a member of an internal department-wide council that reviews the Department's progress on all assigned ISE initiatives, provides timely updates, and seeks continuous feedback on ongoing efforts. Some of the major ISE Working Groups that Operations Coordination is involved in include Sensitive But Unclassified (SBU) Networks, Business Process, and Alerts and Notifications. All of these are directly tied to HSIN and its future effectiveness across the entire ISE.

Finally, GAO recommends that the Secretary determine whether there are coordination and duplication issues with other homeland security networks and associated systems and applications and, where issues are identified, direct the appropriate department executive to ensure that the efforts are effectively coordinated. We will take this recommendation under advisement and provide an update in our sixty day response letter to appropriate Hill committees and the Office of Management and Budget.

Sincerely,

Steven J Pecinovsky

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

GAO Contact and Staff Acknowledgments

GAO Contact

David A. Powner at (202) 512-9286 or pownerd@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following also made key contributions to this report: Gary Mountjoy, Assistant Director; Barbara Collier; Joseph Cruz; Matthew Grote; Joanne Landesman; and Lori Martinez.

GAO's Mission

The Government Accountability 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 GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

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. Government Accountability 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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON ♻ RECYCLED PAPER