



March 2015

LIBRARY OF CONGRESS

Strong Leadership Needed to Address Serious Information Technology Management Weaknesses

GAO Highlights

Highlights of [GAO-15-315](#), a report to congressional committees

Why GAO Did This Study

The Library of Congress is the world's largest library, whose mission is to make its resources available and useful to Congress and the American public. In carrying out its mission, the Library increasingly relies on IT systems, particularly in light of the ways that digital technology has changed the way information is created, shared, and preserved.

The House Appropriations Committee report accompanying the 2015 legislative branch appropriations bill required GAO to conduct a review of IT management at the Library. GAO's objectives focused on the extent to which the Library has established and implemented key IT practices and requirements in, among other areas: (1) strategic planning, (2) governance and investment management, (3) information security and privacy, (4) service management, and (5) leadership. To carry out its work, GAO reviewed Library regulations, policies, procedures, plans, and other relevant documentation for each area and interviewed key Library officials.

What GAO Recommends

GAO is recommending that the Library expeditiously hire a permanent CIO. GAO is also making 30 other recommendations to the Library aimed at establishing and implementing key IT management practices. The Library generally agreed with GAO's recommendations and described planned and ongoing actions to address them.

View [GAO-15-315](#). For more information, contact Joel C. Willemssen at (202) 512-6253 or willemssenj@gao.gov.

March 2015

LIBRARY OF CONGRESS

Strong Leadership Needed to Address Serious Information Technology Management Weaknesses

What GAO Found

The Library of Congress has established policies and procedures for managing its information technology (IT) resources, but significant weaknesses across several areas have hindered their effectiveness:

Strategic planning: The Library does not have an IT strategic plan that is aligned with the overall agency strategic plan and establishes goals, measures, and strategies. This leaves the Library without a clear direction for its use of IT.

Investment management: Although the Library obligated at least \$119 million on IT for fiscal year 2014, it is not effectively managing its investments. To its credit, the Library has established structures for managing IT investments—including a review board and a process for selecting investments. However, the board does not review all key investments, and its roles and responsibilities are not always clearly defined. Additionally, the Library does not have a complete process for tracking its IT spending or an accurate inventory of its assets. For example, while the inventory identifies over 18,000 computers currently in use, officials stated that the Library has fewer than 6,500. Until the Library addresses these weaknesses, its ability to make informed decisions will be impaired.

Information security and privacy: The Library assigned roles and responsibilities and developed policies and procedures for securing its information and systems. However, its implementation of key security and privacy management controls was uneven. For example, the Library's system inventory did not include all key systems. Additionally, the Library did not always fully define and test security controls for its systems, remediate weaknesses in a timely manner, and assess the risks to the privacy of personal information in its systems. Such deficiencies also contributed to weaknesses in technical security controls, putting the Library's systems and information at risk of compromise.

Service management: The Library's Information Technology Services (ITS) division is primarily responsible for providing IT services to the agency's operating units. While ITS has catalogued these services, it has not fully developed agreements with the other units specifying expected levels of performance. Further, the other units were often not satisfied with these services, which has contributed to them independently pursuing their own IT activities. This in turn has resulted in units purchasing unnecessary hardware and software, maintaining separate e-mail environments, and managing overlapping or duplicative IT activities.

Leadership: The Library does not have the leadership needed to address these IT management weaknesses. For example, the agency's chief information officer (CIO) position does not have adequate authority over or oversight of the Library's IT. Additionally, the Library has not had a permanent CIO since 2012 and has had five temporary CIOs in the interim.

In January 2015, at the conclusion of GAO's review, officials stated that the Library plans to draft an IT strategic plan within 90 days and hire a permanent CIO. If it follows through on these plans, the Library will be in a stronger position to address its IT management weaknesses and more effectively support its mission.

Contents

Letter		1
	Background	4
	Library's Approach to IT Lacks Key Planning Practices to Effectively Guide Efforts	21
	Library Is Not Effectively Managing the Selection and Oversight of IT Investments	27
	Library of Congress Has Not Fully Established and Implemented Key IT Acquisition Practices	38
	Security and Privacy Weaknesses Threaten Information and Systems That Support the Library's Mission	49
	Library Has Not Ensured That IT Services Are Supporting Organizational Needs, Resulting in Inconsistent Satisfaction with Services and Duplicative or Overlapping Efforts	73
	Library Lacks Strong Leadership Needed to Address Its IT Management Weaknesses	89
	Conclusions	94
	Recommendations	96
	Agency Comments and Our Evaluation	100
Appendix I	Objectives, Scope, and Methodology	102
Appendix II	Comments from the Library of Congress	123
Appendix III	GAO Contact and Staff Acknowledgments	127
Tables		
	Table 1: Information Technology Staff at the Library of Congress, as of September 2014	11
	Table 2: Information Technology-Related Spending at the Library of Congress, Fiscal Year 2014 Obligations	12
	Table 3: GAO Summary Assessment of ITS's Cost-Estimating Guidance	44
	Table 4: GAO Summary Assessment of ITS's Scheduling Guidance	47
	Table 5: POA&M Status for Selected Systems, as of December 2014	60

Table 6: ITS Customer Satisfaction Survey Results	78
Table 7: Examples of Key Commodity IT Purchased by Individual Service Units in the Past 3 Years	82
Table 8: IT Activities Performed by Library Service Units	84
Table 9: IT Staff Salaries by Service Unit, Fiscal Year 2014	86

Figure

Figure 1: Simplified Library of Congress Organizational Chart	7
---	---

Abbreviations

CIO	chief information officer
CISO	chief information security officer
CMMI-ACQ	Capability Maturity Model® Integration for Acquisition
CRS	Congressional Research Service
eCO	Electronic Copyright Office
FAME	Facility and Asset Management Enterprise
FITARA	Federal Information Technology Acquisition Reform Act
FEDLINK	Federal Library and Information Network
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
IG	inspector general
IT	information technology
ITS	Information Technology Services
ITSC	IT Steering Committee
LCR	Library of Congress Regulation
NIST	National Institute of Standards and Technology
NLS	National Library Service for the Blind and Physically Handicapped
OSEP	Office of Security and Emergency Preparedness
OSI	Office of Strategic Initiatives
OSO	Office of Support Operations
PICS/NIOSS	Production Information & Control System/NLS Integrated Operations Support System
PII	personally identifiable information
POA&M	plan of action and milestones
SEI	Software Engineering Institute
SP	Special Publication
SLA	service-level agreement
SYMIN II	System Management Information Network II

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



March 31, 2015

The Honorable Shelley Moore Capito
Chairman
The Honorable Brian Schatz
Ranking Member
Subcommittee on the Legislative Branch
Committee on Appropriations
United States Senate

The Honorable Tom Graves
Chairman
The Honorable Debbie Wasserman Schultz
Ranking Member
Subcommittee on the Legislative Branch
Committee on Appropriations
House of Representatives

The Library of Congress is the United States' oldest federal cultural institution and plays an important role in the life of the nation. Since its founding in 1800 as mainly a reference and lending library for members of Congress, it has grown to include the world's largest library, with a mission to support the Congress in fulfilling its constitutional duties and to further the progress of knowledge and creativity for the benefit of the American people. In addition to maintaining its collection of books, recordings, photographs, maps, manuscripts, and other items, the Library provides research and policy analysis to members of Congress and their staff. Further, since the late 19th century, the Library of Congress has been home to the U.S. Copyright Office, which is responsible for administering and sustaining an effective national copyright system.

As technology has advanced and the needs of its users have evolved, the Library has increasingly relied on information technology (IT) to carry out its mission, and these changes have required it to reexamine how it will accomplish its mission in the future. Digital technology is fundamentally changing how information is created, shared, and preserved, while the Internet has changed the public's expectations about access to information. For example, the public no longer has to physically visit a library to obtain free access to many of its collection items.

To help ensure the effective management of the Library's IT resources, the House Appropriations Committee report accompanying the fiscal year

2015 legislative branch appropriations bill required GAO to review the actions taken by the Library to manage the IT supporting its programs and operations. Our specific objectives for this review were to assess the extent to which the Library (1) addressed in its strategic planning the IT and related resources required to meet its goals and objectives; (2) established an IT governance structure to manage the selection, control, and evaluation of IT investments; (3) used key IT acquisition and development best practices; (4) established programs for ensuring the information security and privacy protection of its information and information systems; (5) used best practices for managing IT services; and (6) has a chief information officer (CIO) with authority to exercise control and oversight of IT management functions.

To address our objectives, we compared Library policies, procedures, and implementation in the six IT-management-related areas with federal laws and guidance and with key practices identified by industry and GAO—many of which the Library has embraced.¹ Specifically, we did the following:

- Reviewed Library strategic planning documents, including its agency-wide strategic plan, draft IT-specific strategic plan, enterprise architecture documentation, and human capital plan to determine if the Library's planning for IT was aligned with the strategic goals of the agency, whether it had developed an enterprise architecture that described its current and planned business process and IT environment, and whether it had identified skills needed to achieve its goals and any gaps it needed to fill.
- Reviewed Library policies, procedures, and other documentation for IT investment management, including documentation relating to the activities of its IT Steering Committee and other oversight bodies, and compared them to recognized practices for establishing a disciplined, repeatable process for IT investment management. We further examined documentation related to three selected investments undergoing the Library's investment management process to assess

¹As a legislative branch agency, the Library is not required to follow most federal IT management laws and guidance, which generally only apply to executive branch agencies. However, the Library has modeled its related policies and procedures on many executive branch principles and requirements. Thus, we used relevant federal laws and guidance to inform our evaluation of Library policies, procedures, and practices, but did not evaluate the Library for compliance with such requirements.

the information that was used to select and oversee these investments.² We also reviewed Library spending data, including its annual expenditures on IT, and information on its inventory of investments and assets, to determine if these were comprehensive.

- Examined Library policies and procedures to determine if they reflected best practices for selected key acquisition areas—risk management, requirements development, cost estimation, and scheduling. We also reviewed documentation for the three selected investments to determine the extent to which they had implemented these practices.
- Assessed Library policies, procedures, and other documentation related to its information security and privacy programs against relevant federal guidance. To do so, we selected nine information systems across the Library to determine the extent to which the Library had implemented management controls in key areas related to information security and privacy.³ We also conducted testing to determine whether appropriate technical security controls had been applied. Further, we visited Library data center facilities in the greater Washington, D.C., area to assess physical, environmental, and other controls intended to protect the assets at these facilities.
- Examined policies and documentation for managing IT services across the Library to determine if they supported the needs of the organization. This included reviewing a service catalog and service-level agreements developed by the Library's central IT organization—ITS—for services it provides to other units within the Library. We also conducted a customer satisfaction survey of other units to determine their level of satisfaction with ITS's service and sent a structured

²The three selected investments are Facility Asset Management Enterprise (FAME), Momentum Upgrade and Migration, and Twitter Research Access.

³The nine systems we reviewed were the ITS Library of Congress Data Network, Office of Security and Emergency Preparedness Physical Security Network, Congressional Research Service Enterprise Infrastructure General Support System, Information Technology Services Application Hosting Environment, Information Technology Services Library of Congress Office Automation System, Copyright Electronic Copyright Office, Library Services System Management Information Network II, National Library Service for the Blind and Physically Handicapped Production Information and Control System/Integrated Operations Support System, and Office of the Chief Financial Officer Momentum.

questionnaire to each service unit to identify potentially duplicative IT activities across the Library.

- Reviewed policies outlining the responsibilities of the CIO and other key officials, and reviewed documentation to determine if these officials were carrying out their responsibilities for effective leadership of IT management.

For each objective, we also interviewed key officials with responsibilities for IT management at the Library. These included the Librarian of Congress, the former Deputy Librarian, the former acting CIO, the head of ITS, the Chief Information Security Officer, heads of the various service units, and IT staff at the service units, among others.

We conducted this performance audit from April 2014 to March 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Additional details on our objectives, scope, and methodology can be found in appendix I.

Background

Established in 1800, the Library of Congress is the nation's oldest federal cultural institution and serves as the research arm of Congress. Its mission is to support Congress in fulfilling its constitutional duties and to further the progress of knowledge and creativity for the benefit of the American people.

The Library of Congress is the largest library in the world, with more than 158 million items on approximately 838 miles of bookshelves. The collections include more than 36 million books and other print materials, 3.5 million recordings, 13.7 million photographs, 5.5 million maps, 6.7 million pieces of sheet music, and 69 million manuscripts.

The Library receives some 15,000 items each working day and adds approximately 12,000 items to its collections daily. These items are received through a variety of sources, including the copyright registration process, as the Library is home to the U.S. Copyright Office. Materials are also acquired through gift, purchase, other government agencies (state, local, and federal), Cataloging in Publication (a pre-publication arrangement with publishers), and exchange with libraries in the United States and abroad. Items not selected for the collections or other internal

purposes are used in the Library's national and international exchange programs. Through these exchanges the Library acquires material that would not be available otherwise. The remaining items not selected for collections or exchange programs are made available to other federal agencies and are then available for donation to educational institutions, public bodies, and nonprofit tax-exempt organizations in the United States.

The Library collaborates with external communities nationally and internationally through, among other things, activities relating to preservation, research, and education. For example, the Library collects, preserves, and makes accessible first-hand accounts of U.S. veterans so that future generations may hear directly from veterans. Additionally, in collaboration with the United Nations Educational Scientific and Cultural Organization, as well as partner libraries and cultural institutions from around the world, the Library established the World Digital Library. This effort makes available on the Internet, free of charge, and in multilingual format significant primary materials from many countries and cultures.⁴ Further, the Library maintains Congress.gov, which is the official website for U.S. federal legislative information.⁵

Organization of the Library

Positioned within the legislative branch, the Library is led by the Librarian of Congress, who is nominated by the President and confirmed by the Senate. There have been 13 Librarians of Congress since the founding of the Library. The Deputy Librarian shares with the Librarian the overall responsibility for governing the Library and has the delegated authority to act on behalf of the Librarian.

The Library encompasses several service and support units, including the following:

- **Office of the Librarian:** The Office of the Librarian has overall management responsibility for the Library and carries out certain executive functions. It includes the Office of the Chief Financial Officer, the Office of the General Counsel, the Congressional Relations Office, the Office of Communications, the Development

⁴The World Digital Library can be found at <http://www.wdl.org/en/>.

⁵<https://www.congress.gov/>.

Office, the Office of Contracts and Grants Management, and the Office of Special Events and Public Programs.

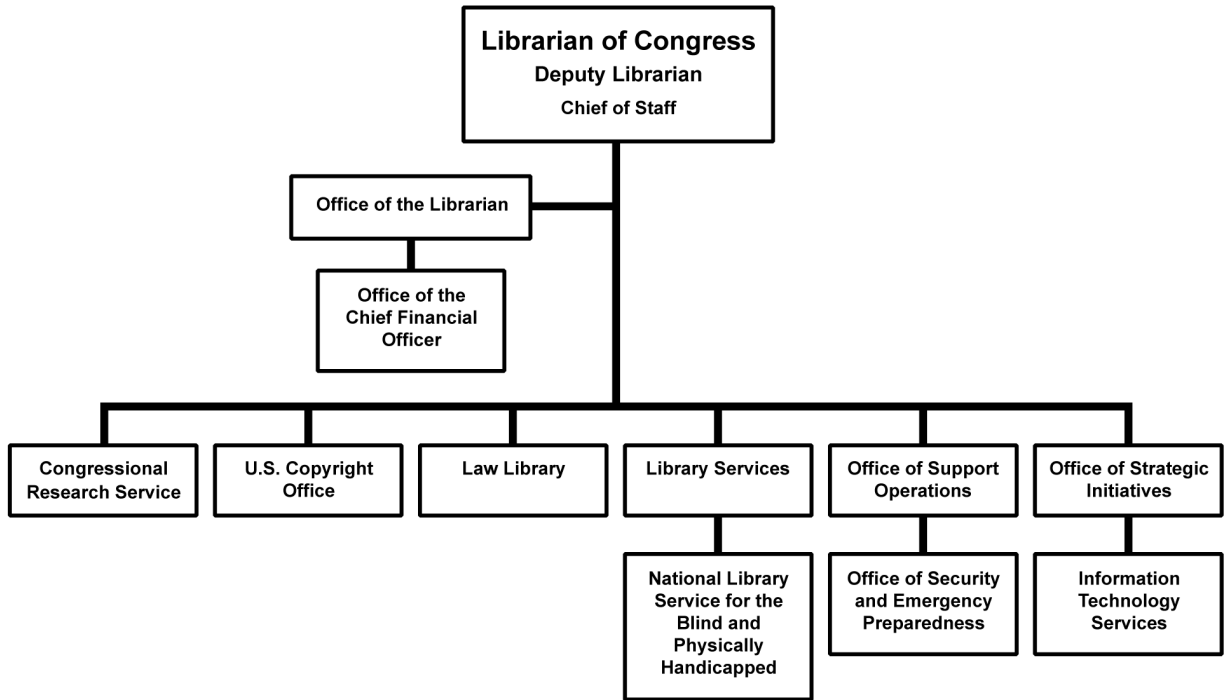
- **Congressional Research Service (CRS):** Established by statute in 1914,⁶ CRS is responsible for providing Congress with nonpartisan legislative research and analysis services. CRS is led by a Director, who is appointed by the Librarian in consultation with the Joint Committee on the Library and serves under the general direction of the Librarian of Congress.
- **United States Copyright Office:** Established by statute in 1897, the Copyright Office is responsible for administering the Copyright Act, including copyright registration, recordation, mandatory deposit, and certain statutory licenses. The office is led by the Register of Copyrights, who is appointed by and serves under the general direction of the Librarian of Congress.
- **Law Library:** Congress established its Law Library in 1832 to provide ready access to reliable legal materials.
- **Library Services:** Library Services develops and preserves the Library's collections, which document the history and creativity of the American people in almost all media and formats and record the world's knowledge in some 470 languages. Library Services also includes the National Library Service for the Blind and Physically Handicapped (NLS), which directs the production of books and magazines in Braille and recorded formats as well as specially designed audio playback equipment. Further, Library Services administers the Library's six overseas offices—located in Brazil, Egypt, India, Indonesia, Kenya, and Pakistan. These offices are tasked with acquiring, cataloging, and preserving collections from developing countries.
- **Office of Strategic Initiatives (OSI):** The mission of OSI is to support the Library's vision and strategy by directing the overall digital strategic planning for the Library and the national program for long-term preservation of digital cultural assets. This office includes ITS, which is to support the Library's IT systems and infrastructure.

⁶First established as the Legislative Reference Service in 1914, Congress renamed the service CRS in 1970 to better reflect its mission—that is, to provide research and policy analysis in support of the legislative process.

- **Office of Support Operations (OSO):** OSO is made up of several offices that provide essential infrastructure services to the entire Library. These include the Office of Opportunity, Inclusiveness, and Compliance; Integrated Support Services; Human Resource Services; and the Office of Security and Emergency Preparedness (OSEP).

Figure 1 provides a simplified depiction of the Library's organization.

Figure 1: Simplified Library of Congress Organizational Chart



Source: Library documentation. | GAO-15-315

An Executive Committee, made up of the heads of the major service units of the Library and chaired by the Librarian, sets overall Library policy and practices, and advises the Librarian.

For fiscal year 2014, the Library was appropriated \$618,776,000 for its operations⁷ and was authorized to maintain 3,746 full-time equivalents.⁸ For fiscal year 2015, the Library was appropriated \$630,853,000,⁹ and, for fiscal year 2016, the Library requested \$666,629,000.¹⁰

Library of Congress IT Environment

Like other federal agencies, the Library relies on a host of IT systems to carry out its mission. These include standard hardware (e.g., desktop and laptop computers, printers, and servers) and software (e.g., e-mail, standard office productivity programs such as word processing and spreadsheet programs, and Internet resources) that Library employees use to carry out their day-to-day work. It also makes use of administrative and business systems, such as accounting, financial planning and budgeting, and human resources systems.

A number of IT systems support Library-wide activities. For example:

- **ITS Library of Congress Data Network:** The ITS Library of Congress Data Network provides network connectivity for Library personnel at Washington, D.C., metropolitan area facilities, with the exception of personnel that rely on the OSEP Physical Security Network.
- **OSEP Physical Security Network:** The OSEP Physical Security Network is the technical infrastructure used for the systems that protect facilities, collections, assets, staff, and visitors. These systems include intrusion alarms, card readers for access control, closed-circuit video cameras, monitors, and recorders.

⁷This included separate appropriations for the Copyright Office (\$51,624,000, which included authorization to obligate up to \$33,444,000 in fees); for CRS (\$105,350,000); and NLS (\$49,750,000).

⁸Full-time equivalents represent the total number of hours worked divided by the number of compensable hours in a full-time schedule.

⁹This included separate appropriations for the Copyright Office (\$54,303,000, which included authorization to obligate up to \$33,582,000 in fees); CRS (\$106,945,000); and NLS (\$50,248,000).

¹⁰This included separate requests for the Copyright Office (\$58,875,000, which included a request for authorization to obligate up to \$35,777,000 in fees); CRS (\$111,956,000); and NLS (\$51,428,000).

-
- **ITS Application Hosting Environment:** The ITS Application Hosting Environment is the technical infrastructure used to support service units' business systems, with the exception of financial business systems and systems used by CRS and OSEP.
 - **ITS Library of Congress Office Automation System:** The ITS Library of Congress Office Automation System is the technical infrastructure used to support file and print services, as well as office automation tools, for Library personnel, with the exception of CRS.
 - **Office of the Chief Financial Officer Momentum:** Momentum is the Library's central financial management system. The U.S. Capitol Police, Congressional Budget Office, Office of Compliance, and Open World Leadership Center also use this system to record and maintain their financial information. This system is hosted on the ITS Financial Hosting Environment.

In addition, the Library's service units have systems that support their various specific missions. For example:

- **Copyright Electronic Copyright Office (eCO):** Members of the public (e.g., authors and other copyright owners) use the eCO system to register basic claims to copyright. The Copyright Office also uses the system to manage the registration process. The ITS Application Hosting Environment hosts the eCO system.
- **CRS Enterprise Infrastructure General Support System:** The CRS Enterprise Infrastructure General Support System is the technical infrastructure (e.g., servers and network devices) used to support CRS applications (e.g., the system used to develop CRS reports), as well as file and print services and office automation tools (e.g., e-mail, word processing, and collaboration tools) for CRS personnel.
- **Library Services System Management Information Network II (SYMINT II):** Library Services uses SYMINT II to manage accounting transactions for the Federal Library and Information Network

(FEDLINK) program.¹¹ This system is hosted on the ITS Financial Hosting Environment, which is used to support financial systems.

- **NLS Production Information & Control System/NLS Integrated Operations Support System (PICS/NIOSS):** NLS uses PICS/NIOSS to manage the process of producing, distributing, and maintaining audiobooks (i.e., the electronic files used to present print information to a reader in audio format). This system is hosted on the ITS Application Hosting environment.

IT Responsibilities

Much of the responsibility for the Library's IT rests with OSI. The office is headed by the Associate Librarian for Strategic Initiatives, who also serves as the Library's CIO. The CIO's responsibilities include coordination of key IT management areas, such as investment management, enterprise architecture, and information security.

Within OSI, ITS has various responsibilities for supporting the Library's IT infrastructure. These include supporting the service units by planning, designing, developing, and maintaining systems and the infrastructure supporting those systems.

As of September 2014, the Library had at least 380 staff dedicated to various IT functions.¹² Most of these (about 250) were in OSI, while the rest were distributed throughout the rest of the organization, with Library Services and CRS having the most IT staff among the other service units. In addition, the Library relies on contractors to fill certain skill gaps, where necessary. Table 1 shows the number of IT staff—excluding contractors—across the agency.

¹¹FEDLINK is a cooperative procurement, accounting, and training program designed to provide customer agencies with access to online databases, periodical subscriptions, books and non-print materials, and other library and information support services. Under the program, the Library has negotiated contracts with commercial suppliers to take advantage of volume discounts.

¹²As discussed in more detail in appendix I, this figure only includes employees whose job title is in the information technology management series (2210). According to a Copyright budget analyst and the Library's Chief Financial Officer, the Library has employees who perform key IT activities, but whose job titles fall outside of the information technology management series.

Table 1: Information Technology Staff at the Library of Congress, as of September 2014

Service unit	Number of IT staff
Copyright Office	17
Congressional Research Service	40
Law Library	7
Library Services	47
Office of the Librarian	14
Office of Support Operations	9
Office of Strategic Initiatives	249
Total	383

Source: GAO analysis of Library data. | GAO-15-315

The Library obligated at least \$119 million for IT during fiscal year 2014.¹³ Of that, about \$46 million was obligated for IT staff salaries, and the other \$73 million was for non-pay obligations (e.g., goods and services).¹⁴ Although OSI accounts for most of the Library's IT spending, other service units also make investments in IT that collectively represent a little less than half of the organization's IT spending. Table 2 shows IT spending across the Library.

¹³As discussed later in this report, this figure is our estimate based on data supplied by Library units and does not reflect all IT obligations made by the Library.

¹⁴Of the approximately \$73 million obligated for non-pay obligations, \$635,993 was funded by gift or trust funds, \$2,517,775 was funded by reimbursable obligations (i.e., financed by offsetting collections credited to an expenditure account in payment for goods and services provided by that account), and \$121,835 was funded by revolving funds (i.e., a fund that conducts continuing cycles of business-like activity, in which the fund charges for the sale of products or services and uses the proceeds to finance its spending).

Table 2: Information Technology-Related Spending at the Library of Congress, Fiscal Year 2014 Obligations

Service unit	Fiscal year 2014 obligations
Copyright Office ^a	\$9,258,413
Congressional Research Service	\$12,355,176
Law Library	\$711,211
Library Services	\$13,203,148
Office of Librarian	\$9,055,839
Office of Strategic Initiatives	\$72,015,569
Office of Support Operations	\$2,545,299
Total	\$119,144,655

Source: GAO analysis of Library financial and human capital data. | GAO-15-315

^aOf the \$9,258,413 that the Copyright Office obligated for IT in fiscal year 2014, \$1,954,565 was obligated for salaries of staff that performed IT work, and the other \$7,303,849 was obligated for IT goods and services. Of the approximately \$7.3 million, \$6,897,532 was funded by fees collected by the office.

Examples of major investments in IT at the Library include the following:

- **Office of the Chief Financial Officer Momentum Upgrade and Migration:** As previously mentioned, Momentum is the Library's financial system. The Library is making additional investments in this system in order to move Momentum to a cloud-based environment. After this effort is completed, the Library plans to migrate the Architect of the Capital's financial management system into the Library's Momentum environment.
- **OSO Facility and Asset Management Enterprise (FAME):** FAME is an existing library business system used to perform facility management functions (e.g., asset, space, and facility management). The system relies on commercial, off-the-shelf software. The Library is investing in additional modules of the underlying software relating to the management of work orders, keys, reservations, event support, and customer service.
- **OSI and Library Services Twitter Research Access:** The Library plans to develop a pilot for making a collection of "tweets" (i.e., brief messages of up to 140 characters in length) from the online social networking service Twitter¹⁵ available for research access. The

¹⁵Twitter is a social networking site that allows users to share and receive tweets.

Library and Twitter signed an agreement that gave the Library, under specific terms and conditions, all public tweets that were made from 2006 through April 2010. The Library and Twitter also agreed that Twitter would provide all public tweets on an ongoing basis under the same terms.

Control over the Library's IT spending lies primarily with each of the individual service units—some of which have their own IT organizations and CIOs. For example:

- **CRS:** The Information Technology and Management Office, which is led by the CRS CIO, is responsible for managing the majority of the IT systems used by CRS staff.
- **Copyright Office:** The Copyright Office of the CIO, which is led by the Copyright CIO, is responsible for maintaining the Copyright Office IT systems.
- **Library Services:** The Automation Planning & Liaison Office within Library Services is responsible for procuring IT hardware, software, and services; managing IT assets; and coordinating with other Library IT organizations.

These organizations are accountable to the heads of their respective service units. For example, the CIO for CRS reports to the Director of CRS, not to the Library of Congress CIO.

Reported Challenges in IT Management at the Library

As GAO and others have highlighted in several reports, the Library has faced long-standing challenges in effectively managing its IT. In 1996, we issued a report on a management review of the Library, covering six major issue areas, including its use of IT.¹⁶ Among other things, the review found that (1) the Library lacked a sufficient strategic focus on information resources management that was linked to its mission objectives; (2) its existing technology infrastructure was not integrated across the Library at a level appropriate to reduce interfaces between systems, lessen the need for maintenance resources, and minimize

¹⁶GAO, *Management Review of the Library of Congress* (Washington, D.C.: May 7, 1996), available online at <http://www.gao.gov/products/156761> (vol. 1) and <http://www.gao.gov/products/156762> (vol. 2). This review was undertaken by Booz-Allen & Hamilton, Inc. on behalf of GAO.

redundant data; (3) technology programs and projects were not managed as investments, with insufficient attention paid to program and project costs, priorities, and performance; and (4) the Library had not decided whether it should continue to build new systems in-house or whether it would be more cost-effective to acquire these capabilities elsewhere. The report recommended a number of actions the Library could take to improve its management of IT in these areas. In commenting on the report, the Library acknowledged the need to link information resources to its mission objectives and re-focus its infrastructure to reflect changes in the technology environment.

The findings in this report were echoed in a review conducted by the National Academy of Sciences and in several reports from the Library's Inspector General (IG). In 2000, the National Academy of Sciences released a report, commissioned by the Library, that examined the need for the Library to develop a digital strategy to cope with the fact that content was increasingly being produced in digital forms.¹⁷ The study found that all Library service units spent money on IT and that this spending was not fully coordinated across the Library. It was unable to quantify this spending because the Library had not established financial accounting for IT. The study concluded that "[s]hadow systems and duplication are the inevitable outcome of such arrangements." Additionally, the study found that strategic direction for IT must come from the office of the Librarian, but that the most senior members of that office—the Librarian of Congress, Deputy Librarian, and Chief of Staff—did not have any specific background or expertise in IT. Further, the report identified a number of findings relating to information security, referring to this issue as "[b]y far the most serious infrastructure problem" at the Library. The study made a number of recommendations, including that the Library (1) establish a Library-wide committee tasked with, among other things, approving significant IT investments; (2) appoint a second Deputy Librarian in order to provide strategic direction for the Library's IT; and (3) address its information security findings.

In March 2009, the Library's IG reported on the agency's IT strategic planning efforts since the issuance of the National Academy report, including the extent to which the Library had implemented the report's

¹⁷National Academy of Sciences, *LC21: A Digital Strategy for the Library of Congress* (Washington, D.C.: National Academy Press, 2000).

recommendations.¹⁸ The report noted that the Library had made many technology improvements, including migrating from mainframe systems, updating the storage architecture, building an alternate computing facility that provides backup for its data centers, building a secure financial hosting environment, and developing a National Institute of Standards and Technology-compliant certification and accreditation process.¹⁹ The report further noted that the Library had standardized internal and external websites, developed digital collections containing more than 300 terabytes of data, and built a network of national and international digital partners.

However, the IG also reported that the strategic planning process at the Library was not well integrated with essential planning components and not instituted Library-wide. Specifically, strategic planning for IT was not linked directly to the overall Library strategic plan and did not have a “forward-looking” view; strategic planning was not linked to the IT investment process; the organizational structure of the ITS directorate did not foster strategic planning and good IT governance; areas of overlap existed in support services and systems, including a number of service units that maintained their own technology offices and help desk functions; the Library was missing an enterprise architecture program, which should be coupled with a strategy for implementing future technology; and ITS customer service needed improvement, to include the use of service-level agreements.

The IG stated that these findings were in large part the result of an unclear sense of how IT planning fits into the Library’s mission and the roles and responsibilities of its employees, as well as a lack of linkage between IT strategic planning processes and actual performance. The IG made a number of recommendations to address these weaknesses, and Library management agreed with the majority of the report’s findings and recommendations.

¹⁸Library of Congress, Office of the Inspector General, *Information Technology Strategic Planning: A Well-Developed Framework is Essential to Support the Library’s Current and Future IT Needs*, Report No. 2008-PA-105 (March 2009).

¹⁹Certification and accreditation is a comprehensive assessment and official management authorization of the management, operational, and technical security controls of an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

The Library's IG issued a follow-up report in December 2011, in which it found that the Library had made progress toward implementing the recommendations made in its prior report, but not as much as expected.²⁰ Specifically, it reported that the Library needed to (1) develop an updated OSI strategic plan, (2) improve data for IT investments, (3) separate the IT function from OSI and establish an Office of the Chief Information Officer, (4) develop a structured procedure to continuously identify and prevent duplicative IT costs throughout the Library by consolidating IT services, (5) increase oversight of the Library's enterprise architecture, and (6) strengthen customer service to the service units. Library management concurred with 17 of the 21 recommendations the IG made in its report.

More recently the IG has reported on challenges relating to (1) procurement of IT workstations, (2) oversight of the National Library Catalog Project, and (3) certification and accreditation.

- In September 2012, the IG reported that a lack of inventory controls had resulted in unnecessary purchases and an aging IT inventory.²¹ Specifically, the IG found that the Library's logistics directorate and ITS did not effectively coordinate with service units, which resulted in unnecessary purchases, such as 484 24-inch, flat-panel monitors that had sat undistributed at the Library's warehouse since 2008, and 224 24-inch, flat-panel monitors that were purchased in 2010 but also sat in the warehouse undistributed. The IG recommended, among other things, that ITS improve its communications and transparency with service units. The Library concurred with this recommendation.
- In September 2013, the IG reported that the Library did not provide effective oversight of the National Library Catalog Project.²² Specifically, the IG found that the Library's IT Steering Committee (ITSC)—the committee responsible for reviewing and analyzing IT

²⁰Library of Congress, Office of the Inspector General, *Follow-up Review: Information Technology Strategic Planning*, Report No. 2011-IT-103 (December 2011).

²¹Library of Congress, Office of the Inspector General, *Improvements Needed to Prevent Wasteful Procurement and Inefficient Disposal of IT Workstations*, Report No. 2012-PA-101 (Sept. 28, 2012).

²²Library of Congress, Office of the Inspector General, *The Library is Taking the Right Steps to Ensure that Its Web Search Strategy Is an Enterprise-wide Solution but Needs to Expand Its Oversight of Other Projects*, Report No. 2013-IT-102 (Sept. 30, 2013).

investments—did not review Library Services’ now-terminated \$2.2 million National Library Catalog project despite its meeting the cost criterion requiring oversight by the committee (i.e., 3-year costs exceeding \$1 million). The IG stated that the ITSC did not review this investment because it was in development prior to the formation of the committee. The IG recommended that the ITSC review any other investments in development that met criteria requiring its oversight. The Library agreed with the recommendation.

- In October 2014, the IG reported that governance and management oversight of the Library’s certification and accreditation process needed to be strengthened.²³ Specifically, the IG found that security assessments and remedial action plans were not always completed in a timely manner. The IG recommended, among other things, that the Library ensure that the security assessments and plans be completed in accordance with Library policy and establish an enforcement mechanism to ensure that remedial action plans are addressed. The Library concurred with these recommendations.

Congress has also recognized the Library’s IT management challenges. For example, in its report accompanying the fiscal year 2012 legislative branch appropriations bill, the House Appropriations Committee directed the Librarian of Congress to consider managing within the Office of the Librarian all Library IT planning and resource allocations to ensure that IT requirements are properly prioritized and resources are effectively used.²⁴

Key IT Management Disciplines

GAO has identified a set of essential and complementary management disciplines that provide a sound foundation for IT management. These include the following:

- **Strategic planning:** Strategic planning defines what an organization seeks to accomplish and identifies the strategies it will use to achieve desired results. A defined strategic planning process allows an agency to clearly articulate its strategic direction and to establish linkages among planning elements such as goals, objectives, and strategies. A well-defined IT strategic planning process helps ensure

²³Library of Congress, Office of the Inspector General, *Report on the Library’s Certification and Accreditation Policies, Procedures and Operating Effectiveness*, Report No. 2013-IT-104 (Oct. 28, 2014).

²⁴H.R. Rep. No. 112-148, at 23 (July 15, 2011).

that an agency's IT goals are aligned with its strategic goals.²⁵ Also as part of their strategic planning efforts, organizations should develop an enterprise architecture, which is an important tool to help guide an organization toward achieving the goals and objectives in its IT strategic plan,²⁶ and implement human capital management practices to sustain a workforce with the skills necessary to execute the organization's strategic plan.²⁷ Library policy also recognizes the importance of IT strategic planning, enterprise architecture, and sustaining a workforce that is aligned with the strategic plan.²⁸

- **IT investment management:** IT projects can significantly improve an organization's performance, but they can also become costly, risky, and unproductive. Agencies can maximize the value of IT investments and minimize the risks of IT acquisitions by having an effective and efficient IT investment management and governance process, as described in GAO's guide to effective IT investment management.²⁹ Recognizing the importance of IT investment management, in 1996 Congress passed the Clinger-Cohen Act, which requires executive branch agencies to establish a process for selecting, managing, and evaluating IT investments in order to maximize the value and assess

²⁵GAO, *Social Security Administration: Improved Planning and Performance Measures Are Needed to Help Ensure Successful Technology Modernization*, [GAO-12-495](#) (Washington, D.C.: Apr. 26, 2012).

²⁶GAO, *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0)* (Supersedes [GAO-03-584G](#)), [GAO-10-846G](#) (Washington, D.C.: August 2010).

²⁷Such practices have been identified by both the Office of Personnel Management and GAO. See Office of Personnel Management, *The Human Capital Assessment and Accountability Framework—Systems, Standards, and Metrics* (http://www.opm.gov/hcaaf_resource_center/) and GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, [GAO-04-39](#) (Washington, D.C.: Dec. 11, 2003).

²⁸Library of Congress Regulation (LCR) 220-1, *Functions and Organization of the Office of Strategic Initiatives*; LCR 1600, *Information Resource Management Policy and Responsibilities*; and LCR 212-1, *Functions and Organization of Human Resources Services*.

²⁹GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (Supersedes AIMD-10.1.23), [GAO-04-394G](#) (Washington, D.C.: March 2004).

and manage the risks of IT acquisitions.³⁰ Although not required to do so, the Library has embraced this requirement.³¹

- **System acquisition and development:** Agencies should follow disciplined processes for developing or acquiring IT systems. These include requirements development, risk management, and cost estimating and scheduling, among others. Best practices in these areas have been identified by organizations such as Carnegie Mellon University's Software Engineering Institute (SEI) and GAO.³²
- **Information security and privacy:** Federal agencies rely extensively on IT systems and electronic data to carry out their missions. Effective security for these systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information, including personal information entrusted to the government by members of the American public. Recognizing the importance of information security and privacy, Congress enacted the Federal Information Security Management Act of 2002 (FISMA), which requires executive branch agencies to develop, document, and implement an agency-wide information security program.³³ Additionally, in order to help agencies develop such a program, the National Institute of Standards and Technology (NIST) has developed guidance for information security and privacy. Although it is not subject to FISMA, the Library has embraced the

³⁰40 U.S.C. § 11312.

³¹LCR 1600.

³²SEI, *Capability Maturity Model® Integration for Acquisition (CMMI-ACQ)*, Version 1.3 (November 2010); GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, [GAO-09-3SP](#) (Washington, D.C.: March 2009); and GAO *Schedule Assessment Guide: Best Practices for Project Schedules—Exposure Draft*, [GAO-12-120G](#) (Washington, D.C.: May 2012).

³³FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). Near the conclusion of our review, the Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014) was enacted. While the new law largely supersedes the 2002 FISMA, it incorporates the requirements from the prior law that are relevant to this report.

law's requirements as well as NIST guidance for information security and privacy.³⁴

- **Service management:** Agencies should develop and implement a process for ensuring that IT services are aligned with the business needs of an organization and actively support them. The Information Technology Infrastructure Library practices are a widely accepted approach to IT service management.³⁵ According to the Director of ITS, the Library has adopted these practices for managing ITS's services.
- **IT leadership:** Effective leadership, such as that of a CIO, can drive change, provide oversight, and ensure accountability for results. Congress has also recognized the importance of having a strong agency CIO. For example, as part of the Clinger-Cohen Act, Congress required executive branch agencies to establish the position of agency CIO.³⁶ The act also gave these officials responsibility and accountability for IT investments, including IT acquisitions, monitoring the performance of IT programs, and advising the agency head whether to continue, modify, or terminate such programs. More recently, in December 2014, Congress passed federal information technology acquisition reform legislation (commonly referred to as FITARA), which strengthened the role that agency CIOs are to play in managing IT.³⁷ For instance, the law required executive branch agencies to ensure that the CIO had a significant role in the decision process for IT budgeting, as well as the management, governance, and oversight processes related to IT. As previously mentioned, although not required to do so, the Library has established a CIO position, and has made this official responsible for, among other

³⁴LCR 1620, *Information Technology Security Policy of the Library of Congress*; LCR 1921, *Protection and Disclosure of Personally Identifiable Information*; and *Information Technology Security Directive 01: General Information Technology Security* (Nov. 17, 2014).

³⁵Lou Hunnebeck and Colin Rudd, *ITIL: Service Design* © (London: The Stationary Office, 2011).

³⁶Pub. L. No. 104-106 (Feb. 10, 1996), sec. 5125; 40 U.S.C. § 11315 and 44 U.S.C. § 3506(a).

³⁷Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Div. A, Title VIII, Subtitle D—Federal Information Technology Acquisition Reform, Pub. L. No. 113-291 § 831; 40 U.S.C. § 11319.

things, overseeing the Library's enterprise architecture and IT investment management processes.³⁸

Library's Approach to IT Lacks Key Planning Practices to Effectively Guide Efforts

Comprehensive strategic planning is essential for an organization to define what it seeks to accomplish, identify strategies to efficiently achieve the desired results, and effectively guide its efforts. Key elements of IT strategic planning include an IT strategic plan and an enterprise architecture that together outline the agency's IT goals, measures, and timelines. In addition, effective human capital management is critical to sustaining an IT workforce with the necessary skills to execute a range of management functions that support the agency's mission and goals.

However, the Library has not completed an IT strategic plan. An IT strategic plan has been drafted, but it does not identify strategies for achieving defined goals and interdependencies among projects. Regarding enterprise architecture, the Library has developed an architecture intended to reflect the current state of its IT systems and operations, but, according to the official who served as acting CIO from April 2014 to January 2015, the architecture is not reliable. Further, the Library has not developed a target architecture that defines its desired state or a plan for achieving this state. Senior Library officials noted that the agency had not made IT strategic planning or enterprise architecture a priority. At the conclusion of our review in January 2015, the Library's Chief of Staff stated that the agency plans to draft a new IT strategic plan within 90 days.

Further, the Library has not performed an organization-wide assessment of IT skills or future needs. Instead, each service unit is responsible for undertaking this assessment on its own. Until it fully implements key elements of IT strategic planning, the Library cannot be assured that its IT investments will match its strategic direction and effectively position the agency to cope with future challenges.

³⁸LCR1600, LCR 220-1, and LCR 212-2, *Functions and Organization of Information Technology Services, Office of the Librarian*.

Library Lacks a Strategic Plan to Guide Its IT Investments

As we have previously reported, an IT strategic plan serves as an agency's vision or road map and helps align its information resources with its business strategies and investment decisions.³⁹ Key elements of an IT strategic plan include, among other things, (1) alignment with the agency's overall strategic plan, (2) results-oriented goals and performance measures that permit it to determine whether it is succeeding, (3) strategies it will use to achieve desired results, and (4) descriptions of interdependencies within and across projects so that these can be understood and managed.⁴⁰ Further, Library policy states that OSI has primary responsibility for setting the Library's IT strategic direction.⁴¹

In 2010, the Library developed its most recent overall strategic plan for fiscal years 2011 through 2016.⁴² The plan included five strategic goals and strategies to achieve those goals, including strategies involving IT. For example, strategies for achieving the goal of *managing proactively for demonstrable results* included implementing an enterprise architecture program and improving IT governance and investment management processes. As another example, one strategy for achieving the goal of *sustaining an effective national copyright system* was to improve processes and IT infrastructure to ensure timeliness of copyright registration.

However, the Library has not completed an IT strategic plan. The official who served as Deputy Librarian from June 2012 to December 2014 explained that, during his tenure he provided the Librarian with draft versions of agency-wide and IT-specific strategic plans that he had developed. The draft IT plan covered fiscal years 2015 to 2020 and addressed some, but not all, key IT strategic planning elements. Specifically, the plan included five goals: (1) use a shared services approach, (2) establish the most effective IT organization and governance, (3) apply outside consultation and guidance where applicable to meet library needs, (4) align Library staff skills with its IT needs, and (5) ensure high levels of information security and preservation.

³⁹GAO-12-495.

⁴⁰GAO-12-495.

⁴¹LCR 220-1.

⁴²Library of Congress, *Strategic Plan: Fiscal Years 2011-2016*.

However, the draft IT plan did not identify what strategies the Library would use to achieve these goals and related performance measures. Additionally, the plan did not describe interdependencies between projects, which would help further define the relationships between projects and shared services. The former Deputy Librarian explained that the IT strategic plan would be followed by an IT support plan, which would include initiatives, projects, milestones, and timelines for implementing the IT strategic plan.

Further, the date for completing the Library's IT strategic plan slipped twice. Specifically, during a hearing on the Library's fiscal year 2015 budget in March 2014, the former Deputy Librarian first committed to delivering the IT strategic plan by the end of August 2014.⁴³ Subsequently, that date slipped to January 2015, and then was delayed again to September 2015. Moreover, we were told by the Librarian in December 2014 that the draft IT plan was merely a starting point for the Library's IT strategic planning efforts and is not the agency's official draft. In January 2015, at the conclusion of our review, the Chief of Staff stated that the Library plans to draft a new IT strategic plan within 90 days. The Librarian stated that the Library intends to finalize the plan by September 2015.

If the Library finalizes an IT strategic plan that sets forth a long-term vision and the intermediate steps that are needed to guide the agency, it will be better positioned to effectively prioritize investments and use the best mix of limited resources to move toward its longer-term, agency-wide goals.

Enterprise Architecture Has Not Been Fully Developed

Like an IT strategic plan, an enterprise architecture is an important tool to help guide an organization's IT investments by ensuring that the planning and implementation of those investments take full account of the business and technology environment in which the systems are to operate. According to our research, a well-defined enterprise architecture thoroughly describes the current and target states of an organization's IT systems and business operations and identifies the gaps and specific intermediate steps it plans to take to achieve the target state.⁴⁴

⁴³*Budget Hearing - Library of Congress, Before the Legislative Branch Sub. Comm., H. Comm. on Appropriations, 113th Cong. (Mar. 5, 2014) (statement of Robert Dizard, Deputy Librarian of Congress).*

⁴⁴[GAO-10-846G](#).

Additionally, in order to enable institutional commitment to an enterprise architecture, agencies should, among other things, develop an organizational policy for enterprise architecture and establish an executive committee representing the enterprise that is responsible and accountable for enterprise architecture.

To its credit, the Library has established a policy and executive committee for enterprise architecture.⁴⁵ This policy describes roles and responsibilities for developing, maintaining, and using the enterprise architecture. For example, the agency's chief architect is to report to the CIO and is responsible for, among other things, coordinating and overseeing business and IT planning and advising key stakeholders in business and IT planning. Additionally, the policy makes the Library's Executive Committee responsible for ensuring that the architect assumes responsibility for the Library's enterprise architecture.

However, the Library of Congress has not fully developed its enterprise architecture. The agency has an enterprise architect who developed an architecture that describes the current state of the Library's IT systems and operations, to include performance, business, data, services, and technology. However, management has raised concerns about the architecture's reliability. For example, according to the former acting CIO, data for the architecture were not gathered from management and validated stakeholders (i.e., individuals identified by their respective service unit as being knowledgeable about the current and target states of the unit's IT systems and business operations). Instead, the enterprise architect gathered information for the architecture by interviewing over 500 employees across the Library. Additionally, the architecture does not reflect the target state of the Library's IT systems and business operations, or the gaps and specific steps that the Library should take to achieve the target state.

The lack of progress in developing the enterprise architecture was enabled, in large part, by limited oversight from the Library's CIO. According to the former acting CIO, developing the Library's enterprise architecture was not a priority for the previous CIOs. She also told us that the previous CIOs did not effectively oversee the enterprise architect. In the absence of appropriate oversight, according to the acting CIO, the

⁴⁵LCR 1600.

enterprise architect has taken an isolated, self-directed approach to developing the architecture, which has not met the organization's needs.

The Library has taken initial steps toward improving its architecture. According to the former acting CIO, the three individuals who have recently served as acting CIO on a rotating basis collectively decided to improve the management of the enterprise architect. That official also stated that, in order to improve the reliability of the data collected by the enterprise architect, that individual is now required to collect data from stakeholders in each service unit who have been identified by the ITSC. Additionally, at the conclusion of our review, the former acting CIO stated that the enterprise architect has been detailed to work under the direction of the Deputy Director of ITS until April 2015 so that his work can be integrated with other architecture work in ITS. Further, she stated that an independent, expert reviewer will assess the enterprise architect's work and determine how the Library can move its architecture to the next level of maturity. That official also stated that strategic direction for the enterprise architecture program will be integrated with the Library's IT strategic plan.

Until the Library establishes and implements an approach to developing a well-defined enterprise architecture—to include providing adequate oversight of the work performed by the enterprise architect—there is increased risk that organizational operations and supporting technology infrastructures and systems will be duplicative, poorly integrated, unnecessarily costly to maintain, and unable to respond quickly to shifting environmental factors.

Library Has Largely Not Assessed Current and Future IT Skills

Key to an agency's success in managing its IT systems is sustaining a workforce with the necessary knowledge, skills, and abilities to execute a range of management functions that support the agency's mission and goals.⁴⁶ Achieving such a workforce depends on having effective human capital management, which includes assessing current and future agency skill needs by, for example, analyzing the gaps between current skills and future needs, and developing strategies for filling the gaps. Taking such

⁴⁶GAO, *A Model of Strategic Human Capital Management*, [GAO-02-373SP](#) (Washington, D.C.: March 2002); *Human Capital: Key Principles for Effective Strategic Workforce Planning*, [GAO-04-39](#) (Washington, D.C.: Dec. 11, 2003); and *Information Technology: FDA Needs to Establish Key Plans and Processes for Guiding Systems Modernization Efforts*, [GAO-09-523](#) (Washington, D.C.: June 2, 2009).

steps is consistent with activities outlined in human capital management models that we and the Office of Personnel Management have developed.⁴⁷

Although its human capital plan calls for the organization to assess gaps in current and anticipated skills across all employees within the Library,⁴⁸ such an assessment has not been performed for IT skills. Additionally, although identifying skills and competencies that are clearly linked to an agency's mission and longer-term IT goals is essential—especially in an organization like the Library, which has IT staff in every service unit—the Library's IT human capital plan does not provide information about future IT human resource needs.

The former acting CIO acknowledged that the Library has not performed an organization-wide assessment of skills or future needs. Instead, according to the acting CIO, each service unit is responsible for managing its own human capital skills. For example, that official told us that, with respect to OSI, skills and competencies are identified when an individual leaves the organization, or when OSI plans to hire additional staff. However, this approach does not provide the CIO with visibility into the service units' IT human capital efforts. We have previously reported that CIOs at executive branch agencies without sufficient influence over the hiring of IT staff were limited in their ability to ensure appropriate IT staff were being hired to meet mission needs.⁴⁹

The Library has taken initial steps to assess the needs of its IT workforce. According to the Director of Human Resources Services, the Library's Human Capital Planning Board conducted a pilot initiative in the Acquisitions and Bibliographic Access Directorate within Library Services to identify competencies and skills, including those relating to IT. According to the Director of Human Resources Services, the Library plans to identify skills and competencies, including those relating to IT, to be used initially in order to assess the skills for three succession planning

⁴⁷Office of Personnel Management, *Human Capital Assessment and Accountability Framework—Systems, Standards, and Metrics* (http://www.opm.gov/hcaaf_resource_center/).

⁴⁸Library of Congress, *Human Capital Management Plan* (December 2010).

⁴⁹GAO, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management*, [GAO-11-634](#) (Washington, D.C.: Sept. 15, 2011).

groups: senior-level executives, managers/supervisors, and succession target occupations. This official stated that this effort is expected to extend into fiscal year 2016, and that the Library plans to institutionalize this approach in other Library offices. However, the Library has yet to establish a date for completing the effort.

Until the Library ensures that its human capital planning and analysis address the specific competencies and skills critical to meeting its future IT needs, the agency jeopardizes its ability to deliver IT support. Additionally, without an organization-wide approach to assessing needed IT skills, the Library is at risk of developing a workforce in each service unit with overlapping competencies.

Library Is Not Effectively Managing the Selection and Oversight of IT Investments

Ensuring that investments in IT meet the needs of the organization and are being effectively managed is important for any federal agency. Congress has recognized the importance of effective IT investment management by requiring agencies in the executive branch to establish an investment management process.⁵⁰ Although not required by law to do so, the Library has also begun to establish such a process. Specifically, the Library's *Information Resource Management Policy and Responsibilities* calls for the Library to align IT investments with its strategic goals and to connect strategic planning, enterprise architecture, and IT investment management in order to design and leverage Library resources to meet the needs of Congress and the public.⁵¹

Since 2010, the Library has taken steps to build a foundation for managing its IT investments, including instituting an investment board and establishing elements of a process for selecting investments. However, the Library has not implemented an IT investment management process that fully addresses key practices. In particular, its investment board has not always operated as intended. Further, the Library's process for selecting IT investments is not aligned with decisions to fund investments, and no process has been established for reselecting ongoing investments. Moreover, the Library, including its service units, did not always follow its own policy for including major investments in its agency-wide investment review process. Regarding investment oversight, the Library established a process for overseeing the performance of

⁵⁰40 U.S.C. § 11312.

⁵¹LCR 1600.

selected investments, but the data informing this process were not always complete. Moreover, the Library does not have a comprehensive process for tracking its IT spending and does not have an accurate inventory of its IT assets. Consequently, the Library does not know how much it spends annually on IT or what kinds of equipment it is currently using. Finally, the Library is not managing its IT as a portfolio to determine that capabilities, once implemented, are delivering intended value and that the agency is identifying the appropriate mix of IT projects that best meet its mission needs.

These weaknesses can be attributed, in part, to unclear or incomplete policies as well as inconsistent implementation of the policies that have been developed. Until the Library addresses these weaknesses, it will not have the investment structure and processes needed to effectively manage its IT projects, systems, and assets.

Key Practices for Managing Individual IT Investments Have Not Been Fully Established or Implemented

GAO's IT investment management framework is composed of five progressive stages of maturity that mark an agency's level of sophistication with regard to its IT investment management capabilities.⁵² Such capabilities are essential to the governance of an organization's IT investments. At the Stage 2 level of maturity, an organization lays the foundation for sound IT investment processes that help it attain successful, predictable, and repeatable investment control processes at the project level. These processes focus on the agency's ability to select, oversee, and review IT projects.

According to the framework, Stage 2 critical processes include the following:

- **Instituting the investment board:** As part of this process, an agency is to establish an enterprise-wide investment review board to be responsible for defining and implementing the IT investment management governance process.
- **Selecting investments that meet business needs:** As part of this process, an agency is to establish and implement policies and

⁵²GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (Supersedes AIMD-10.1.23), [GAO-04-394G](#) (Washington, D.C.: March 2004).

procedures for selecting and reselecting IT investments that meet the agency's needs.

- **Providing investment oversight:** This process includes establishing and implementing policies and procedures for overseeing IT projects and ensuring that they align with the agency's business needs.
- **Capturing investment information:** This process includes establishing and implementing policies and procedures for developing and maintaining a comprehensive repository of information on IT investments and assets.

Library Has Established an Investment Board, but Its Policies and Procedures Are Not Always Clear

The establishment of decision-making bodies or boards is a foundational component of effective IT investment management. According to the IT investment management framework developed by GAO, an organization should, among other things, establish an enterprise-wide investment review board to be responsible for defining and implementing IT investment governance policies and procedures. In order for the IT investment management process to function effectively, an investment board must operate within its assigned authority and responsibility so that investments are properly aligned with the organization's objectives and are reviewed by those with the authority to make IT management decisions. Additionally, the organization's IT investment management process should describe how these processes are coordinated with other organizational plans, processes, and documents, including, at a minimum, the IT strategic plan and enterprise architecture.

The Library established an investment board that is responsible for defining and implementing IT investment governance policies and procedures. Specifically, the Library's policy on information resource management established the ITSC, an investment board made up of senior officials from across the Library's various service units. The policy requires the board to review major investments in IT that meet at least one of several agency-defined criteria. These include those investments that are high risk, have high visibility (internally or externally), or have estimated 3-year costs exceeding \$1 million. The Library's information resource management policy also gives the ITSC responsibility for formalizing the policies and procedures for selecting and managing IT investments. Library policy also describes IT management responsibilities of the Executive Committee—the Library's most senior governance board. For example, this committee is to provide strategic mission and priority guidance to the ITSC.

However, the Library has not clearly defined the division of responsibilities between the two bodies. Specifically, although Library policy gives IT investment selection decision-making authority to both the ITSC and the Executive Committee, it does not clearly specify when the ITSC should make a decision and when circumstances require an Executive Committee decision. Since the establishment of the ITSC in 2010, the Executive Committee has not made any decisions regarding the selection of IT investments; instead, the ITSC has made all such decisions.

In March 2014, the ITSC developed a process for determining when investments are to be reviewed by the Executive Committee; however, this process has not yet resulted in any decisions being escalated to the Executive Committee. Moreover, the Director of ITS, who also chaired the ITSC from July 2013 to January 2015, stated that this process had not been approved by the Librarian or the Executive Committee. According to this individual, he plans to submit this revision to the Office of the Librarian as part of a Library-wide effort to streamline and centralize Library policies.

Additionally, the Library's investment management process is not fully coordinated with its IT strategic plan and enterprise architecture. Specifically, as previously mentioned, the Library does not have an IT strategic plan or a complete enterprise architecture to guide its IT investment decisions and ensure that those decisions meet the organization's business needs. Coordination between the Library's investment management process and its efforts to improve its strategic plan and enterprise architecture could help ensure that investments support the Library's strategic goals and do not duplicate existing investments. Until Library policy is updated to clearly define the roles and responsibilities of the ITSC and Executive Committee and these bodies operate according to their designated authority and responsibilities, the Library cannot ensure that investments are properly aligned with the business needs of the entire organization. In addition, without a strategic plan, enterprise architecture, and a process for linking these areas to the investment management process, the ITSC and Executive Committee will not have a roadmap needed to make investment decisions that best meet the needs of the Library.

Library Has Not Fully
Developed and Implemented a
Selection Process

According to our IT investment management framework, to support well-informed decisions, organizations should establish and implement policies and procedures for selecting and reselecting IT investments that meet the agency's needs, and these policies should integrate funding and

selection decisions. Documenting and implementing these processes are basic steps toward realizing increased maturity in how the organization selects its IT projects.

To its credit, the Library developed policies and procedures that outline how IT investments are to move through the selection process, from initial proposal to final approval, with steps for evaluating and prioritizing the investments based on their alignment with business needs. As previously mentioned, Library policy requires the ITSC to review investments that are high risk, have high visibility, or have estimated 3-year costs exceeding \$1 million. Before an investment is selected, the ITSC is to assign it a score based on quantifying its risk factors (e.g., high cost, length of development cycle, lack of clear and measurable objectives) and then evaluating those factors along with the significance of its program benefits (e.g., how it will contribute to organizational performance or how it will respond to user needs). The ITSC is then to use the score to determine whether it will select the investment for project development.

However, the Library has not developed policies or procedures for reselecting investments that are already operational for continued funding. This is important because, according to the former acting ITSC chair, operational investments account for the majority of the Library's IT spending. That same official also stated that the Library decided not to review, as part of its investment management process, investments that were either in development or already operational prior to the establishment of the ITSC in February 2010. For instance, in September 2013, the Library's IG reported that the ITSC did not review Library Services' now-terminated \$2.2 million National Library Catalog project because it was in development prior to the ITSC's formation.⁵³ In October 2013, the former acting ITSC chair directed the members to bring before the committee any projects that (1) met the Library's definition of major investments in IT that are to be reviewed by the ITSC, (2) were still in development, and (3) were in development prior to the establishment of the ITSC in February 2010. While this was a positive step, this decision did not address investments that were operational. Additionally, because the decision was made 3 years after the creation of the ITSC, there were

⁵³Library of Congress, Office of the Inspector General, *The Library is Taking the Right Steps to Ensure that Its Web Search Strategy Is an Enterprise-wide Solution but Needs to Expand Its Oversight of Other Projects*, Report No. 2013-IT-102 (Sept. 30, 2013).

likely some IT investments that were developed and completed during this time that did not receive ITSC review. According to the former acting ITSC chair, the Library will consider whether to review additional investments in the future.

In addition, the Library does not have policies and procedures for integrating funding and selection decisions. In fact, according to the former acting ITSC chair, ITSC selection does not affect decisions to allocate funding for investments, because, in some instances, the service units secure funding for their investments before the selection process begins. The former acting ITSC chair added that, as a compensating control, the ITSC could request that ITS not devote its own resources to an investment until the committee's concerns are resolved. However, this process would not affect the investment if the service unit proposing it decides not to use ITS resources. Until the Library fully integrates IT investment selection with funding decisions, selection decisions may not reflect an organization-wide perspective on what IT investments may best meet the Library's needs.

Further, the Library, including its service units, did not always follow its process for selecting new investments. Specifically, the ITSC does not review all major IT investments that, according to its policy, should be reviewed. For example, as discussed in more detail in our report on the Copyright Office, the office did not present four of its recent IT initiatives to the ITSC, despite each having estimated 1-year costs exceeding \$1 million.⁵⁴ In addition, the ITSC did not review the Twitter Research Access investment while it was in the planning stages because it was approved by the Executive Committee without going through the Library's selection process. However, by not going through the Library's selection process, investments are not subject to the selection reviews, which evaluate, among other things, cost, schedule, scope, strategic impact, and customer needs on an enterprise-wide level. For example, as discussed in more detail later in the report, the Twitter Research Access investment did not create a reliable cost estimate nor did it develop a schedule. Going through the selection process would help ensure that investments are better planned and better aligned with agency needs from the outset,

⁵⁴GAO, *Information Technology: Copyright Office Needs to Develop Plans that Address Technical and Organizational Challenges*, GAO-15-338 (Washington, D.C.: Mar. 31, 2015).

Library Has Established a Process for Overseeing Investments, but Data Used Were Not Always Complete

which could eliminate or reduce the severity of future problems during system development.

Until it establishes and implements a complete selection process for all major IT investments that links its IT investment selection decisions with agency funding decisions, the Library is at greater risk of not selecting the appropriate mix of IT investments that would best meet its organizational and technological needs as well as support its priorities for improvement.

As with investment selection, organizations should have a documented, well-defined process for overseeing investments once they have been selected to ensure that they continue to align with the agency's business needs. Effective investment oversight and evaluation involves, among other things, developing policies and procedures for reviewing the progress ongoing projects have made in meeting cost, schedule, and risk expectations.

The ITSC established procedures to assess the progress of investments in development. These reviews center on quarterly reports submitted to the ITSC by the investment teams, which update the board on, among other things, cost and schedule variances, as well as how the teams are managing key risks.

However, for the three selected investments that we reviewed,⁵⁵ the cost, schedule, and risk data in the quarterly performance reports were not always complete or reliable.

- Regarding cost information, one investment—Momentum Upgrade and Migration—included initial and current cost estimates and the variances between the two figures in its July 2014 quarterly report. However, the other two investments—FAME and Twitter Research Access—did not provide all cost information in their July 2014 submissions. For the FAME investment, although OSO provided cost information for the investment as a whole, it listed the costs needed to achieve its next key milestone in September 2014 as \$0. Finally, the Twitter Research Access investment did not provide any cost information in its quarterly report submitted in July 2014. In a written response to our findings, the Library acknowledged that this

⁵⁵The three selected investments are FAME, Momentum Upgrade and Migration, and Twitter Research Access.

information was omitted for the Twitter Research Access investment, and stated that this information was included in the subsequent report. Moreover, the cost information provided in these reports is not fully reliable. Specifically, as discussed in more detail later in the report, the initial cost estimates for all three investments were not comprehensive.

- With respect to schedule information, two of the three investments—Momentum Upgrade and Migration and Twitter Research Access—submitted all schedule information as part of their quarterly performance reports submitted in July 2014. Regarding FAME, although the Library identified the planned start and completion dates for the investment, the investment did not provide any meaningful information regarding its next quarter. Rather, the relevant section of the quarterly performance report simply stated “9/30/2014,” which was the last day of the relevant quarter. Moreover, the schedule information provided in the reports was not fully reliable. Specifically, as explained in more detail later in this report, one investment—Twitter Research Access—did not develop a project schedule, and the other investments’ schedules were not well-constructed.
- Regarding risk, as discussed in more detail later in this report, the three investments did not always document the context and consequences of occurrence for all risks, and one of the investments—FAME—did not describe mitigation plans for all risks.

Library officials recognized the need to make improvements to these data and recently revised the quarterly performance report template in order to help facilitate improvements. Until its oversight processes are informed by complete and accurate investment information, the Library cannot ensure that its investments are meeting expectations related to cost, schedule, and risk. Without this information, the Library may not be able to see the early warning signs that indicate the need for corrective action, resulting in failed investments or investments that do not adequately support business processes, meet user needs, or provide a successful return on investment.

Library Does Not Have an Accurate Inventory of Its IT Spending and Assets

To make informed decisions regarding IT investments, an organization must be able to acquire, store, and retrieve pertinent information about each investment to be used in future investment management decisions.

As we have reported, for this critical area, the organization should establish and implement a process for maintaining a full and accurate accounting of IT-related expenditures.⁵⁶ In addition, the organization should track information on the organization's IT assets, including, for instance, the physical location and owner of each resource. According to the GAO IT investment management framework, effectively capturing investment information requires using a standard, documented procedure for developing and maintaining IT data that are not only useful for decision-making, but are also timely, sufficient, complete, and comparable.

The Library has not fully established and implemented a process for maintaining a full accounting of IT-related expenditures. Instead, it only collects information on the investments reviewed by the ITSC, which includes investment charters, cost-benefit analyses, and performance reports.⁵⁷ Consequently, the Library does not know how much it spends on IT.

In the absence of this information, we estimated that the Library obligated at least \$119 million on IT for fiscal year 2014. We based this estimate on data from the Library's accounting and human resources systems. This allowed us to identify spending on IT equipment and services as well as salary information for staff performing IT-related functions. However, as discussed in more detail in appendix I, this \$119 million does not reflect all of the Library's IT spending.

At the conclusion of our review in December 2014, the Library's Chief Financial Officer told us that the Library has required that service units indicate, for planned fiscal year 2015 expenditures, whether the expenditures relate to IT. A senior advisor to the Chief Financial Officer estimated that the Library would be able to provide a reliable IT spending figure by March 2015. However, the Library has not established guidance to assist service units in classifying planned IT expenditures.

⁵⁶GAO, *Information Technology Management: Governmentwide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved*, [GAO-04-49](#) (Washington, D.C.: Jan. 12, 2004).

⁵⁷The cost estimates for the investments reviewed by the ITSC in fiscal year 2014 collectively totaled approximately \$12.5 million, which is a small percentage of the Library's overall IT spending.

With regard to capturing IT asset information, the Library's primary asset inventory system is highly inaccurate.⁵⁸ Integrated Support Services, a division of OSO, has developed a system to track and manage the Library's assets, including those assets related to IT. However, many of these IT assets are no longer in use. For example, the system lists over 18,000 "active" personal computers, even though, according to Library officials, it actually has fewer than 6,500 personal computers in use. The list of "active" personal computers includes over 12,000 computers from the manufacturer from which the Library primarily purchases computers and more than 5,000 computers from four other manufacturers. Without an accurate inventory, there is increased risk of undetected theft and loss.

In a written response, the Library acknowledged that its primary inventory system does not have reliable information on IT hardware. The Library cited multiple reasons for this weakness, including that its primary inventory system contains legacy data from an obsolete, decommissioned system. Additionally, the Library stated that a comprehensive inventory of non-capitalized assets has not been conducted in several years. Further, the Library said that its current policy on inventory management does not require non-capitalized assets to be identified in its primary inventory system.

The Library also noted that ITS and CRS maintain other systems with accurate and reliable information about the majority of hardware connected to the Library's network. It added that the items in the ITS and CRS systems make up the vast majority of the IT inventory in the Library.⁵⁹ However, while these systems may have reliable information on most Library IT hardware currently in use, they do not have information on the hardware in the primary inventory system that is no longer in use. Without this information, the Library cannot provide the disposition of the hardware that is no longer being used. Additionally, maintaining this information in separate systems can increase the risk of unnecessary purchases of items already on hand, which, as discussed later in this

⁵⁸ Additionally, as discussed later in this report, the Library did not have, as part of its information security program, a complete and accurate inventory of its information systems.

⁵⁹ According to a senior OSEP electronic security engineer, OSEP also maintains a separate database of its IT hardware.

report, has occurred at the Library. Further, the ITS and CRS systems do not include information on IT not connected to the Library's network.

At the conclusion of our review, the Library outlined steps it plans to take to address the reliability of its primary inventory. These include revising its policy in early 2015 to require key non-capitalized IT hardware assets to be identified in the Library's primary inventory system and populating the Library's primary inventory system with data from the ITS and CRS systems. The Library added that, because it has not yet developed a process for this, it will not have an accurate inventory in its primary system until March 2016.

Without fully developing and implementing a process for maintaining a full accounting of IT-related expenditures, the Library will not have the information needed to make informed decisions. Further, until it ensures that its primary inventory system has accurate information on IT hardware, there is increased risk of unnecessary purchases of items already on hand.

Library Has Not Begun to Manage Its Investments as a Portfolio

Once an agency attains Stage 2 maturity, it needs to implement critical processes for managing its investments as a portfolio to move on to Stage 3. An IT investment portfolio is the combination of an organization's IT assets, resources, and investments (including those in production). Taking an agency-wide perspective enables an organization to consider new proposals along with previously funded investments, identifying the appropriate mix of IT projects that best meet mission needs, organizational needs, technology needs, and priorities for improvement. According to GAO's IT investment management framework, Stage 3 critical processes include, among others, (1) conducting post-implementation reviews to compare actual investment results with decision makers' expectations for cost, schedule, performance, and mission improvement outcomes; (2) defining the portfolio criteria; (3) creating the portfolio; and (4) evaluating the portfolio.

Although the Library has established procedures for conducting post-implementation reviews, it has yet to apply these procedures to all operational investments. Specifically, in August 2014 and September 2014, the ITSC developed templates and instructions for conducting the reviews. At the conclusion of our review in March 2015, the interim CIO stated that the ITSC performed the first four post-implementation reviews. Although this is a positive step, the Library has yet to perform these reviews on all of its operational investments. Until such reviews are

consistently performed on all operational investments, the Library will not be able to learn from all past investments and evaluate the effectiveness of its investment management process.

With respect to defining portfolio criteria and creating and evaluating the portfolio, according to the former acting ITSC chair, the agency has not concentrated on implementing these Stage 3 key practices because it has focused its resources on establishing the Stage 2 practices associated with building the IT investment management foundation at the level of the individual investment. Full implementation of the Stage 3 critical processes associated with portfolio management will provide the Library with the capability to determine whether it is selecting the mix of products that best meet the agency's business needs.

Library of Congress Has Not Fully Established and Implemented Key IT Acquisition Practices

The Software Engineering Institute (SEI) at Carnegie Mellon University, GAO, and others have developed and identified best practices to help guide organizations to effectively plan and manage their acquisitions of major IT systems.⁶⁰ Our prior reviews have shown that proper implementation of such practices can significantly increase the likelihood of delivering promised system capabilities on time and within budget.⁶¹ These practices include, among others, risk management, requirements development, cost estimating, and scheduling.

However, the Library has not developed policies in these areas that address key practices. Partly because the Library does not have organization-wide policies in these areas, the selected investments that we examined⁶² did not fully implement key practices for risk management, requirements development, cost estimating, and scheduling. Until the Library establishes and implements these practices, there is increased risk that its investments will incur cost overruns and schedule slippages and fail to deliver capabilities needed to meet the mission of the Library.

⁶⁰SEI, *CMMI-ACQ*, Version 1.3; [GAO-09-3SP](#); and [GAO-12-120G](#).

⁶¹See, e.g., GAO, *Information Technology: Critical Factors Underlying Successful Major Acquisitions*, [GAO-12-7](#) (Washington, D.C.: Oct. 21, 2011).

⁶²The three selected investments are FAME, Momentum Upgrade and Migration, and Twitter Research Access.

Risk Management Practices Were Not Fully Established and Implemented

Risk management is a process for anticipating problems and taking appropriate steps to mitigate risks and minimize their impact on program commitments. According to leading industry guidance,⁶³ it includes the following elements:

- developing a risk management strategy;⁶⁴
- identifying and documenting risks;
- evaluating, categorizing, and prioritizing risks;
- developing risk mitigation plans; and
- monitoring the status of each risk periodically and implementing the risk mitigation plans as appropriate.

Organizations should establish a risk management policy that calls for these elements to be addressed by individual investments.

The Library of Congress has not established an organization-wide policy for IT risk management. Instead, only one directorate within a service unit—OSI's ITS—has developed guidance in this area. This guidance includes templates for a risk management strategy and a risk register. The risk register provides a mechanism for investments to identify, document, evaluate, categorize, and prioritize risks; develop risk mitigation plans; and monitor the status of risks and implement risk mitigation plans as needed. However, this guidance is not mandatory for any projects in the Library—including those that are managed by ITS.

Additionally, the three selected investments—FAME, Momentum Upgrade and Migration, and Twitter Research Access—did not fully implement the following key risk management practices.

- **Establish a risk management strategy:** None of the three selected investments established a risk management strategy for all investment risks. With respect to the Momentum Upgrade and Migration investment, although the contractor developed a project management plan that addresses risk management, it did not address the government's efforts for managing risk. Additionally, the Library

⁶³SEI, *CMMI-ACQ*, Version 1.3.

⁶⁴The risk management strategy addresses the specific actions and management approach used to apply and control the risk management program. It also includes identifying and involving relevant stakeholders in the risk management process.

did not establish a strategy for the FAME and Twitter Research Access investments.

- **Identify and document risks to include the context, conditions, and consequences of risk occurrence:** Although each of the three selected investments identified risks, they did not always document the context and consequences of risk occurrence. For example, the FAME investment charter identified four risks—business requirements and process, technical support resources, project funding, and contract.⁶⁵ However, the charter did not include any descriptions of these risks that would provide additional context and consequences of risk decisions. As another example, the Twitter Research Access investment charter included a risk regarding limited institutional support and prioritization, but did not provide the context needed for management to fully understand this risk. As a final example, the Momentum Upgrade and Migration acquisition plan included a risk that was described as “resources.” Although the description of the risk mitigation plan provides some context for this risk, the acquisition plan does not describe the consequences of this risk’s occurrence.
- **Evaluate, categorize, and prioritize risks using defined risk categories and parameters:** The three selected investments did not always evaluate, categorize, and prioritize risks using defined risk categories and parameters. Specifically, for the Twitter Research Access and FAME investments, the Library evaluated, categorized, and prioritized all of the identified risks; however, it did not do so using defined risk categories. With respect to the Momentum Upgrade and Migration investment, the Library evaluated, categorized, and prioritized risks identified in the risk register, but did not do so for additional risks identified in its acquisition plan.
- **Develop risk mitigation plans in accordance with the risk management strategy:** The Library of Congress did not develop risk mitigation plans for all risks identified for the selected investments, and plans that were developed were not done so in accordance with risk management strategies. Specifically, for the Twitter Research Access and Momentum Upgrade and Migration investments, although the Library developed risk mitigation plans for all identified risks, it did

⁶⁵In a written response at the conclusion of our review, the Director of Integrated Support Services stated that the Library later defined risks and mitigation plans for FAME during the course of its work.

not develop them in accordance with risk management strategies for those investments. With regard to the FAME investment, the Library did not develop risk mitigation plans for any of the identified risks.

- **Monitor the status of each risk periodically and implement the risk mitigation plans as appropriate:** Although the Library's IT investment management process requires quarterly reports on, among other things, risks identified in the investments' charters, the reports for the three investments did not fully address this information. Specifically, for the Twitter Research Access investment, although the July 2014 quarterly report included the identified risks and their associated mitigation plans, it did not fully document the context of risk occurrence. With respect to the Momentum Upgrade and Migration and FAME investments, the risk sections of the July 2014 quarterly reports did not identify any risks or risk mitigations plans.⁶⁶

The incomplete implementation of risk management can be attributed to the lack of an organization-wide policy, as noted previously. At the conclusion of our review, the Library acknowledged that it has not established an organization-wide policy for risk management and stated that it would establish a policy that requires all IT acquisitions valued at \$100,000 or more to follow a Library-wide risk management policy and process. The Library stated that this new risk management policy and process will be established for fiscal year 2016. Until the Library establishes and implements organization-wide risk management policies and procedures, officials will not have assurance that risks facing IT investments are being adequately addressed.

Requirements Development Practices Were Not Fully Established and Implemented

Requirements establish what the system is to do, how it is to do it, and how it is to interact with other systems. According to leading practices, effective requirements development includes eliciting stakeholder needs, developing customer requirements, and prioritizing customer requirements.⁶⁷ In order to enable consistent implementation, processes for requirements development should be established in organizational policy.

⁶⁶In written comments on a draft of this report, the Library stated that participants in the Momentum Upgrade and Migration investment hold monthly risk meetings at which risks are discussed, reviewed, and updated.

⁶⁷SEI, *CMMI-ACQ*, Version 1.3.

The Library of Congress has not established an organization-wide policy for requirements development. Although ITS has developed requirements management guidance that ITS investments are required to follow, this guidance does not apply to other service units' investments. This guidance includes a template for documenting requirements, including those developed by customers.

Additionally, while the Library implemented key requirements development practices for two of the three selected investments, it did not consistently do so for the third. For two of the investments—Twitter Research Access and Momentum Upgrade and Migration—the Library elicited stakeholder needs and developed prioritized customer requirements. For example, for the Twitter Research Access investment, Library Services convened a group of stakeholders, referred to as the Twitter Access Group, to develop functional requirements to support research access to the Twitter archive. Based on these efforts, that group developed customer functional requirements and prioritized them by placing them into three priority categories.

However, the FAME investment did not fully implement key requirements development practices. Specifically, the Library elicited customer needs and developed customer requirements for only one of the three components of the FAME investment and did not prioritize them. In a written response, Integrated Support Services acknowledged that it had not elicited customer needs for all three components of the FAME investment, stating that it would do so as the components are implemented. It explained that this is appropriate because FAME uses commercial, off-the-shelf software with “out-of-the-box” functionality. However, according to leading practices, while requirements will evolve as more is learned about the selected product, some stakeholder needs should be elicited and developed prior to the selection of a commercial, off-the-shelf solution to ensure that the solution meets those needs.⁶⁸

The incomplete implementation of requirements development practices can also be attributed to the lack of an organization-wide policy, as discussed previously. At the conclusion of our review, the Library acknowledged that it has not established an organization-wide policy for requirements development and stated that it would do so, consistent with

⁶⁸SEI, *CMMI-ACQ*, Version 1.3, and *Capability Maturity Model® Integration (CMMI®) for COTS-Based Systems* (September 2003).

the industry guidance cited in this report. The former acting CIO stated that the Library intends to finalize this policy by September 2015. Until the Library establishes and implements a consistent requirements development process across the organization, it will not have assurance that its IT investments will meet stakeholder and customer needs.

Cost Estimating Practices Were Not Fully Established and Implemented

Reliable cost estimates are critical for successfully delivering IT investments. Such estimates provide the basis for informed investment decision making, realistic budget formulation, meaningful progress measurement, and accountability for results. GAO's *Cost Estimating and Assessment Guide* defines 12 leading practices related to four characteristics—*comprehensive*, *well-documented*, *accurate*, and *credible*—that are important to developing high-quality, reliable estimates.⁶⁹ To institutionalize cost estimating best practices, organizations should establish policies that require cost estimates to demonstrate these four characteristics.

The Library of Congress has not established an organization-wide policy for cost estimating. Instead, only one directorate within a service unit—ITS—has developed guidance in this area that ITS projects are largely required to follow. Moreover, ITS's cost estimating guidance does not substantially address the leading practices relating to developing high-quality, reliable estimates. Specifically, the guidance partially addresses the *well-documented* characteristic and minimally addresses the *comprehensive*, *accurate*, and *credible* characteristics.

Table 3 shows the extent to which the guidance addressed the four characteristics.

⁶⁹ [GAO-09-3SP](#).

Table 3: GAO Summary Assessment of ITS's Cost Estimating Guidance

Characteristic	GAO assessment	Key examples of rationale for assessment
<i>Comprehensive.</i> The estimate accounts for all possible costs associated with a program, is structured in sufficient detail to ensure that costs are neither omitted nor double counted, and documents all cost-influencing assumptions.	●	ITS has developed a checklist to assist investments in developing their estimates. However, ITS's guidance does not provide a standard estimating structure to ensure that all costs are captured and that costs are not omitted or double counted. Additionally, the guidance does not require management to approve assumptions. This is important because the rejection of even a single assumption by management could invalidate a cost estimate.
<i>Well-documented.</i> Supporting documentation explains the process, sources, and methods used to create the estimate; contains the underlying data used to develop the estimate; and is adequately reviewed and approved by management.	●	ITS's guidance includes cost estimating templates with sections for documenting the process used to develop the estimates. However, ITS's guidance does not identify the underlying sources and methods that can be used to develop an estimate, such as subject matter expert opinion and historical data. Additionally, although the guidance requires management approval, it does not require the estimator to provide a briefing for management to show how it is accurate, complete, and of high quality.
<i>Accurate.</i> The estimate is not overly conservative or optimistic, is based on an assessment of the costs most likely to be incurred, and is regularly updated so that it always reflects the program's current status.	●	ITS's guidance includes some requirements aimed at ensuring that estimates are not overly conservative or optimistic. However, the guidance does not call for estimates to rely on historical data to the extent possible. Additionally, ITS's guidance does not require estimates to be updated.
<i>Credible.</i> Any limitations of the analysis because of uncertainty or sensitivity surrounding data or assumptions are discussed, the estimate's results are cross-checked, and an independent cost estimate is conducted by a group outside the acquiring organization to determine whether other estimating methods produce similar results.	●	ITS's guidance includes a questionnaire for identifying risks associated with the investment. Additionally, ITS provides guidance for discussing the sensitivity analysis of the estimates. However, its guidance on sensitivity does not address identifying the key assumptions and cost drivers. Additionally, ITS does not require independent estimates to be performed.

Key:

- =Fully met—The Library provided complete evidence that satisfies the associated tasks of the leading practices.
- =Substantially met—The Library provided evidence that satisfies a large portion of the associated tasks of the leading practices.
- =Partially met—The Library provided evidence that satisfies about half of the associated tasks of the leading practices.
- =Minimally met—The Library provided evidence that satisfies a small portion of the associated tasks of the leading practices.
- =Not met—The Library did not provide evidence that satisfies any of the associated tasks of the leading practices.

Source: GAO analysis of agency documentation. | GAO-15-315

The weaknesses in the Library's cost estimating policies and guidance are reflected in the estimates for the selected investments. To its credit, the Library developed cost estimates for all three selected investments. However, none of the estimates fully met the *comprehensive* characteristic, which is necessary for the estimate to fully address the

other three characteristics. Specifically, one of the three selected investments' estimates—the estimate for the Momentum Upgrade and Migration investment—partially met the *comprehensive* characteristic, and the other two estimates minimally met the *comprehensive* characteristic. Regarding Momentum Upgrade and Migration, to its credit, the Library developed documentation that defined several components of the investment, including its assumptions about the investment, key risks, and a schedule. However, the cost documentation does not include enough detail to ensure that all costs are included. For example, costs for government staff are not clearly described in the documentation. Additionally, the estimating documentation was not always structured in sufficient detail to ensure that costs are neither omitted nor double counted.

Regarding the estimates for the Twitter Research Access and FAME investments, although the estimates included some costs, they did not include enough detail to confirm that all costs were included. For example, neither estimate included a work breakdown structure—which is the cornerstone of every project because it defines in detail the work necessary to accomplish a project's objectives. Additionally, the estimates did not include all cost-influencing assumptions.

At the conclusion of our review, the Library acknowledged that it had not established an organization-wide policy for cost estimating and stated that it would establish, by December 2015, cost estimating guidance for all IT projects with an initial investment over \$1 million. Until the Library establishes and implements an effective cost estimating process, there is increased risk that cost estimates may not be reliable—thereby impairing its ability to make well-informed funding decisions and affecting how it allocates resources across competing investments.

Scheduling Practices Were Not Fully Established and Implemented

The success of an IT investment depends in part on having an integrated and reliable master schedule that defines when the investment's set of work activities and milestone events are to occur, how long they will take, and how they are related to one another. Among other things, a reliable schedule provides a road map for systemic execution of an IT investment and the means by which to gauge progress, identify and address potential problems, and promote accountability. GAO's *Schedule Assessment Guide* defines 10 leading practices related to four characteristics—

comprehensive, well-constructed, credible, and controlled—that are vital to having an integrated and reliable master schedules.⁷⁰ To institutionalize sound scheduling practices, organizations should establish policies that require schedules to demonstrate these four characteristics.

The Library of Congress has not established an organization-wide policy for scheduling. As with cost estimating, ITS has developed some guidance in this area that ITS projects are largely required to follow. Additionally, the guidance does not substantially address the leading practices related to developing integrated and reliable master schedules. Specifically, ITS's guidance minimally addresses the *credible* and *controlled* characteristics and does not address the *comprehensive* and *well-constructed* characteristics. Table 4 shows the extent to which ITS's scheduling guidance addresses the four characteristics.

⁷⁰[GAO-12-120G](#).

Table 4: GAO Summary Assessment of ITS's Scheduling Guidance

Characteristic	GAO assessment	Key examples of rationale for assessment
<i>Comprehensive.</i> A comprehensive schedule includes all activities for both the government and its contractors necessary to accomplish a project's objectives as defined in the project's work breakdown structure. The schedule includes the labor, materials, and overhead needed to do the work and depicts when those resources are needed and when they will be available. It realistically reflects how long each activity will take and allows for discrete progress measurement.	○	Although ITS's guidance calls for a schedule to be completed, it does not describe the detail that should be included in the schedule, such as activities needed for the government and contractor to complete their respective objectives, and the resources needed to complete the work. Additionally, ITS does not provide guidance on the duration of activities.
<i>Well-constructed.</i> A schedule is well-constructed if all its activities are logically sequenced with the most straightforward logic possible. Unusual or complicated logic techniques are used judiciously and justified in the schedule documentation. The schedule's critical path represents a true model of the activities that drive the project's earliest completion date and total float accurately depicts schedule flexibility.	○	ITS's guidance does not include information on sequencing tasks, confirming a critical path, and ensuring that total float accurately depicts schedule flexibility.
<i>Credible.</i> A schedule that is credible is horizontally traceable—that is, it reflects the order of events necessary to achieve aggregated products or outcomes. It is also vertically traceable: activities in varying levels of the schedule map to one another and key dates presented to management in periodic briefings are in sync with the schedule. Data about risks and opportunities are used to predict a level of confidence in meeting the project's completion date. The level of necessary schedule contingency and high-priority risks and opportunities are identified by conducting a robust schedule risk analysis.	◐	Although ITS's guidance includes a risk questionnaire that contains a section regarding schedule risks, the guidance does not discuss conducting a schedule risk analysis. Additionally, ITS does not have guidance for ensuring that schedules are horizontally and vertically traceable.
<i>Controlled.</i> A schedule is controlled if it is updated periodically by trained schedulers using actual progress and logic to realistically forecast dates for program activities. It is compared against a designated baseline schedule to measure, monitor, and report the project's progress. The baseline schedule is accompanied by a baseline document that explains the overall approach to the project, defines ground rules and assumptions, and describes the unique features of the schedule. The baseline schedule and current schedule are subject to a configuration management control process.	◐	Although ITS's guidance calls for schedules to be updated regularly, it does not identify who is responsible for doing so. Additionally, the guidance does not address establishing and maintaining a baseline schedule.

Key:

- =Fully met—The Library provided complete evidence that satisfies the associated tasks of the leading practices.
- ◐=Substantially met—The Library provided evidence that satisfies a large portion of the associated tasks of the leading practices.
- ◑=Partially met—The Library provided evidence that satisfies about half of the associated tasks of the leading practices.
- ◒=Minimally met—The Library provided evidence that satisfies a small portion of the associated tasks of the leading practices.
- =Not met—The Library did not provide evidence that satisfies any of the associated tasks of the leading practices.

Source: GAO analysis of agency documentation. | GAO-15-315

The weaknesses in the Library's scheduling policies and guidance are reflected in the schedules for the three selected investments. One investment—Twitter Research Access—did not develop a schedule,⁷¹ and the other investments' schedules did not substantially address the *well-constructed* characteristic, which relates to the foundational practices for a high-quality, reliable schedule. The FAME investment developed two schedules—each of which relates to one of the investment's projects—that, considered together, partially addressed the *well-constructed* characteristic. Specifically, the activities in each schedule were largely sequenced with straightforward logic. However, the schedules did not include valid critical paths,⁷² and their float values⁷³ do not always accurately represent schedule flexibility.

At the conclusion of our review in January 2015, the Director of Integrated Support Services stated that the schedules we reviewed were immature because they were created when project management activities were just beginning. He also provided two updated schedules, stating that they were more robust and addressed the weaknesses we identified. We reviewed one of the two schedules⁷⁴ and found that the schedule partially addressed the *well-constructed* characteristic. Similar to the previous schedules, it did not include a valid critical path and the float values did not always accurately represent schedule flexibility. In contrast to the other schedules, however, the updated schedule was not sequenced with straightforward logic. For example, 25 (20.2 percent) of the remaining 119 activities did not have successor activities. Not linking related activities can cause problems because changes to the durations of these activities will not accurately change the dates for related activities. Additionally, 40 (32.3 percent) of the remaining activities were constrained by "finish no earlier than" dates, which is significant because it means that these

⁷¹Although the Library outlined time frames for key capabilities to be deployed as part of its investment charter, it did not establish a schedule—that is, it did not develop documentation that connects all scheduled work in a collection of linked sequences of activities.

⁷²The critical path represents the chain of dependent activities with the longest total duration in the schedule. If any activity on the critical path slips, the entire project will be delayed.

⁷³Float is the time that a predecessor activity can slip before the delay affects successor activities.

⁷⁴We did not review the other schedule because, according to the Director of Integrated Support Services, the project relating to that schedule was completed in January 2015.

activities would not be allowed to finish earlier, even if their respective predecessor activities have been completed.

The Momentum Upgrade and Migration investment developed a schedule that minimally addressed the *well-constructed* characteristic. For example, 400 (33.9 percent) of the remaining 1,129 activities did not have successor activities. Additionally, the schedule did not have a valid critical path, and its float values did not always accurately represent schedule flexibility.

At the conclusion of our review, the Library acknowledged that it had not established an organization-wide policy for scheduling and stated that it will develop a schedule management process based on GAO's and other best practices and will establish a Library-wide policy that requires all investments to follow the new schedule management process. The Library stated that the new policy and process will be established for fiscal year 2016. However, the Library has yet to establish a date for completing the effort.

Until the Library establishes and implements a process for effectively managing its schedules, there is increased risk of schedule slippages and cost overruns. Additionally, it will be difficult for the Library to obtain meaningful measurement and oversight of investment status and progress, as well as accountability for results.

Security and Privacy Weaknesses Threaten Information and Systems That Support the Library's Mission

Protecting its data and information systems is a key objective for any federal agency. This is essential not only to defend an agency's operations against disruption by cyber attacks, but also to protect sensitive information entrusted to it by members of the public. To protect their systems and information, agencies should establish information security and privacy programs and effectively implement management and technical security and privacy controls. Toward this end, NIST has developed guidance to assist federal agencies in developing and implementing information security and privacy programs.

Consistent with NIST guidance, the Library established security and privacy programs by delineating roles and responsibilities and developing

policies and procedures.⁷⁵ However, it has not fully implemented management controls to ensure the protection of its systems and information. Specifically, while the Library did establish and implement a process for handling security incidents, it did not (1) have a complete inventory of its systems for purposes of monitoring security controls, (2) fully outline security controls in system security plans, (3) conduct complete security testing of its systems, (4) develop and complete in a timely fashion plans for remediating identified security weaknesses, (5) establish contingency plans for its systems, (6) fully document security training policies or ensure that all users had taken required training, (7) include security-related requirements in all applicable contracts for IT services, or (8) fully assess risks to the privacy of personal information in its systems. Further, we identified numerous weaknesses in technical security controls at the Library related to preventing unauthorized access to and securely configuring systems. Until it addresses these weaknesses, the Library's systems and the information they contain will be at increased risk of compromise.

Library Established Security and Privacy Programs for Information Systems

NIST guidance calls for agencies to develop, document, and implement programs for securing information systems, and protecting the privacy of personal information in those systems.⁷⁶ With respect to information security, such a program should include risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout an information system's life cycle. Additionally, information security programs should include a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices.

⁷⁵Federal executive branch agencies are required by law and the Office of Management and Budget to follow NIST information security and privacy standards and guidance. The Library, while not an executive branch agency, has established requirements that follow that guidance.

⁷⁶See, for example, NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication (SP) 800-53, Revision 4 (Gaithersburg, Md.: April 2013); *Computer Security Incident Handling Guide*, SP 800-61, Revision 2 (Gaithersburg, Md.: August 2012); *Guide for Developing Security Plans for Federal Information Systems*, SP 800-18, Revision 1 (Gaithersburg, Md.: February 2006); and *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (Gaithersburg, Md.: February 2010).

Library Developed Security-Related Policies and Procedures

Regarding privacy, according to NIST guidance, organizations should implement a broad set of controls to ensure the appropriate use and protection of personal information maintained by the organization.⁷⁷ This includes establishing an organization-wide program overseen by a chief privacy officer, conducting privacy impact assessments to assess the privacy risks associated with collecting and using personal information, and providing an organized and effective response to privacy incidents.

The Library took steps to establish protections for its systems as part of its information security program. It assigned overall responsibility for securing the agency's information and systems to appropriate officials, including, among others, the

- Librarian, who is responsible for ensuring that the Library's security program is being implemented;
- Deputy Librarian, who is responsible for enforcing the Library's security program;
- CIO, who is responsible for overseeing the Library's program; and
- Chief Information Security Officer (CISO), who is to act as the single point of contact for all information security activities.

Additionally, Library business owners are responsible for ensuring that systems they are responsible for are developed in accordance with, and comply with, Library information security policies.

The Library also documented information security policies and procedures to safeguard its information and systems and to reduce the risk and minimize the effects of security incidents. For example, the *Information Technology Security Policy of the Library of Congress* established the agency's overall information security program and sets ground rules under which it is to operate and safeguard its information and information systems to reduce the risk and minimize the effect of security incidents.⁷⁸ In addition, the Library's *General Information Technology Security* identifies specific IT control requirements for all information systems, including measures and controls designed to respond to any incidents that occur and recovery of information resources

⁷⁷NIST, SP 800-53, Revision 4, Appendix J.

⁷⁸LCR 1620.

Library Developed Policies
Aimed at Protecting the
Privacy of Information

in the event of a disaster.⁷⁹ The Library recently updated this directive to align with the latest revision to NIST's guidelines for building effective security plans, which according to NIST outlines expanded security and privacy controls and provides a more holistic approach to information security.⁸⁰

The Library has also taken steps to protect the privacy of data processed by its systems. It designated the Library's General Counsel as the agency's Chief Privacy Officer, which includes overall responsibility for managing the protection of personally identifiable information (PII)⁸¹ maintained by the Library's systems.⁸²

The agency also documented a policy for protecting PII and responding to reports of unauthorized access or improper disclosure of PII. Specifically, the Library regulation *Protection and Disclosure of Personally Identifiable Information* establishes, among other things, the following requirements for the Chief Privacy Officer and service units:

- **Incident handling:** Any known or suspected unauthorized access to or improper disclosure of PII must be reported by the impacted service unit immediately to both the Chief Privacy Officer and the IG, who are to coordinate a response to minimize any harm. The Library has also developed guidance for responding to privacy incidents relating to information systems.
- **PII training:** The Chief Privacy Officer and service units are responsible for the provision of PII training to Library employees.
- **Assessment of privacy risks:** Service units are required to identify PII and the purposes for which it is used, assess the sensitivity of the information, and determine appropriate levels of protection.

⁷⁹Library of Congress, *Information Technology Security Directive 01: General Information Technology Security* (Washington, D.C.: Nov. 17, 2014).

⁸⁰NIST, SP 800-53, Rev. 4.

⁸¹PII is any information that can be used to distinguish or trace an individual's identity—such as name, date, and place of birth, and Social Security number—or other types of personal information that can be linked to an individual—such as medical, educational, financial, and employment information.

⁸²LCR 1921.

Separately, the Library's *General Information Technology Security Directive* requires system owners to conduct privacy impact assessments⁸³ for all systems in order to mitigate privacy risks.

- **Oversight of privacy activities:** The Chief Privacy Officer has overall responsibility for all of the Library's privacy information activities, including the assurance of privacy policy compliance.

Library Has Not Fully Implemented Security and Privacy Management Controls

Although the Library established security and privacy programs for information systems, it did not fully implement management controls associated with these processes.

Library Established and Implemented an Incident Handling Process for Selected Incidents

Even strong controls may not block all intrusions and misuse, but organizations can reduce the risks associated with such events if they take steps to promptly report and respond to them before significant damage is done. In addition, analyzing security incidents allows organizations to gain a better understanding of the threats to their information and the costs of their security-related problems. Such analyses can pinpoint vulnerabilities that need to be eliminated so that they will not be exploited again. Incident reports can be used to provide valuable input for risk assessments, help in prioritizing security improvement efforts, and illustrate risks and related trends for senior management. NIST guidance recommends that agency information security programs include, among other things, procedures for reporting and responding to security incidents.⁸⁴

The Library has established and implemented an incident handling process. Specifically, it developed procedures for reporting and responding to security incidents. Additionally, for the 22 selected incidents we reviewed, the Library followed these procedures, to include documenting, analyzing, halting the spread of or limiting the damage caused by, and recovering from the incidents, as appropriate.

⁸³A privacy impact assessment is an analysis of how personal information is collected, stored, shared, and managed in an information system. These assessments are conducted to identify privacy risks and methods to mitigate those risks.

⁸⁴NIST, SP 800-61, Rev. 2.

Inventory of Systems Was Not Complete or Accurate

As a result, the Library has increased assurance that it will be able to promptly report and respond to intrusions and misuse before significant damage is done.

According to NIST guidelines, agencies should develop and maintain an inventory of their information systems.⁸⁵ A complete and accurate inventory of major information systems is a key element of managing the agency's IT resources, including the security of those resources. The inventory can be used to track agency systems for purposes, such as periodic security testing and evaluation, patch management, contingency planning, and identifying system interconnections. Further, ITS policy⁸⁶ requires the CISO to develop an inventory that includes all general support systems and major applications.⁸⁷

However, the Library's inventory of its information systems was not complete and accurate. In particular, an inventory maintained by the CISO did not include systems identified in inventories maintained by Library Services. For example, the list maintained by the CISO had 30 Library Services systems, but the list provided to us by Library Services in May 2014 identified 46 systems. After we raised the discrepancy with Library Services, officials from that service unit provided us with a revised list of 70 systems. Moreover, none of the lists maintained by the CISO or Library Services included the networks used by the overseas offices, and the Chief of the Library Services Automation and Planning Office acknowledged that these systems have not been certified and accredited.

According to the CISO, he did not know about some of the missing systems until they were brought to his attention by GAO. The CISO noted that there were a few systems that needed to be included in the system list. He added that in fiscal year 2015 the Library plans to implement a new system for managing its security program, which will include scanning the Library's network to identify its systems. In addition, the CISO stated that many of the systems not included in the various inventories are legacy systems that have been exempted from performing

⁸⁵NIST, SP 800-53, Rev. 4.

⁸⁶Library of Congress, *Information Technology Security Directive 01*.

⁸⁷Major applications are those that require special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Library Did Not Fully Establish and Implement a Process for Documenting Key Controls in System Security Plans

key information security management processes. Specifically, according to Library policy, all low-impact operational IT systems implemented prior to August 20, 2004, that have not undergone a major change (e.g., software or hardware upgrade) are not required to undergo a triennial certification and accreditation. However, without a complete inventory that includes all legacy systems, there is increased risk that the Library will not be able to track legacy systems that undergo a major change and ensure that appropriate controls are put in place to protect them.

Further, the CISO stated that the Library is taking steps to mitigate risks at its overseas offices. For example, according to the CISO, the Library is performing vulnerability scans of the offices, upgrading the operating system of their workstations, and routing their e-mails through the Library's firewalls. Although these steps should improve the security of these offices, the Library will not be able to identify all risks associated with the overseas offices—and thus ensure that controls have been implemented to appropriately mitigate those risks—without certifying and accrediting the networks for those sites.

Until the Library has a complete and accurate inventory of its systems, it cannot ensure that the appropriate security controls have been implemented to protect these systems.

The objective of system security planning is to improve the protection of IT resources. A system security plan is to provide a complete and up-to-date overview of the system's security requirements and describe the controls that are in place—or planned—to meet those requirements. According to NIST guidelines, system security plans should include descriptions of how security controls are implemented and, for controls recommended by NIST but not implemented, a justification for why the controls were deemed not necessary for the system.⁸⁸ Further, to the extent that a system relies on controls established for another system, known as inherited or common controls, NIST guidelines call for describing those controls, noting that organizations should assess how effective they are for the new system being planned and identify compensating or supplementary controls as needed.

⁸⁸NIST, SP 800-18, Rev. 1.

Library policy does not fully address NIST guidelines. Specifically, although Library policy calls for system security plans to describe or reference security controls that fulfill the security requirements of the system, it does not explicitly require plans to describe common controls.⁸⁹

This weakness in Library policy was reflected in the system security plans for most of the nine selected systems that we reviewed.⁹⁰ Specifically, only two of the nine plans—the plans for the Application Hosting Environment and the OSEP Physical Security Network—described all of the common controls on which those systems relied. By contrast, the security plan for the Enterprise Infrastructure General Support System did not always describe controls that were inherited; instead, the plan said that the controls were inherited from the information security program without identifying what system was responsible for implementing them. Additionally, the security plan for eCO did not always describe controls inherited from the Library of Congress Data Network and the Application Hosting Environment.

In addition, the plan for one system did not always include descriptions of how security controls were implemented. Specifically, for PICS/NIOSS the system security plan identified controls that were implemented, but did not include associated descriptions.⁹¹

Further, the plan for one system did not include a justification for why certain controls were deemed not necessary for the system. Specifically, the system security plan for Momentum deemed all physical and environmental protection controls as not applicable; however, the plan did not provide a justification for why the 17 controls were not necessary for the system. According to the CISO, these controls were likely deemed not applicable because they are inherited from another system. Nevertheless,

⁸⁹Library of Congress, *Information Technology Security Directive 01*.

⁹⁰As previously mentioned, the nine systems we reviewed were the ITS Library of Congress Data Network, OSEP Physical Security Network, CRS Enterprise Infrastructure General Support System, ITS Application Hosting Environment, ITS Library of Congress Office Automation System, Copyright Electronic Copyright Office (eCO), Library Services System Management Information Network II (SYMIN II), NLS Production Information Control System/NLS Integrated Operations Support System (PICS/NIOSS), and Office of the Chief Financial Officer Momentum.

⁹¹The Library did not describe how two controls relating to access controls were implemented.

Library Did Not Conduct Complete Security Testing

he acknowledged that the description of these controls in the plan was not acceptable.

The CISO acknowledged the weaknesses with the plans and stated that, until recently, he did not have the resources needed to audit these plans. This official added that the Library recently hired an IT specialist with previous experience reviewing certification and accreditation packages, including security plans, and that this specialist has started to audit these packages.

Without complete system security plans, it will be difficult for agency officials to make fully informed judgments regarding the risks involved in operating those systems, increasing the risk that the confidentiality, integrity, or availability of the systems could be compromised.

A key element of an information security program is regular testing and evaluation to ensure that systems are in compliance with policies and that the policies and controls are both appropriate and effective. Such testing demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies areas of noncompliance and ineffectiveness requiring remediation. NIST guidance emphasizes that agencies should regularly test the implementation of security controls to determine the extent to which they are implemented correctly, are operating as intended, and meet security requirements.⁹² NIST also notes that security testing should assess both the controls implemented by a system and those inherited from other systems.

The Library has taken steps to establish a policy on security testing that is consistent with NIST guidance, but has not finalized guidance on how the policy is to be implemented. Until recently, Library policy required that security testing of all controls for a particular system be conducted as part of the system's triennial certification and accreditation process. However, in November 2014, the Library revised its policy to require near-real-time testing—an approach commonly referred to as continuous monitoring.⁹³ Specifically, the Library now requires service units to assess the risk associated with each security control through a continuous monitoring

⁹²NIST, SP 800-37, Rev. 1.

⁹³Library of Congress, *Information Technology Security Directive 01*.

program and perform testing as frequently as needed in order to appropriately mitigate the risks. According to the CISO, this policy is to be implemented by service units when the certification and accreditation of their systems are due to be renewed. Although the Library has established policy for continuous monitoring, its guidance on how service units are to carry out this policy has not been finalized.

Additionally, the Library did not always follow its policy. In particular, each of the nine selected systems inherited security controls relating to the Library's information security program, but, according to the CISO, the Library has not assessed these inherited controls to ensure that they have been appropriately implemented. The CISO acknowledged that these controls should be tested periodically and stated that the Library plans to do so as part of the implementation of a new system for managing its information security program, which is to occur in fiscal year 2015.

Additionally, the Library's security testing did not always identify control weaknesses. For example:

- Although all nine selected systems' most recent security testing documentation reported that appropriate background investigations had been performed, we identified seven individuals with elevated privileges to three systems—Library of Congress Data Network, PICS/NIOSS, and OSEP Physical Security Network—for which the Library did not have a record of a background investigation.
- Although seven systems' most recent security evaluations reported that privacy impact assessments had been developed as appropriate,⁹⁴ we found that four of these systems—Library of Congress Office Automation System, eCO, SYMIN II, and Momentum—had never completed such an assessment.

Further, the Library did not complete security assessments in a timely manner for three systems. As of January 2015, three systems—SYMIN II, Library of Congress Office Automation System, and Library of Congress Data Network—had not completed security assessments consistent with

⁹⁴Security testing for the OSEP Physical Security Network and the Application Hosting Environment stated that these systems did not have privacy impact assessments.

Library policy, which requires such assessments to be performed at least every 3 years.

- With respect to SYMIN II, the CISO stated that ITS opened a remedial action plan that tasks Library Services with completing this assessment.
- Regarding the Library of Congress Office Automation System and Library of Congress Data Network, the ITS Assistant Director for Operations signed waivers for the systems that extended the deadline for completing the security assessments to October 2015 and July 2015, respectively. This was because the contractor to be used to perform the testing was not available as it was performing testing on the Library's financial hosting environment.

Although, to its credit, the Library analyzed and accepted the risk of not performing testing as scheduled, such lapses between testing can significantly increase the risk that exploitable weaknesses will not be identified and addressed in a timely manner. Without comprehensive and effective testing, the Library does not have reasonable assurance that its security controls for the selected systems are working as intended, increasing the risk that attackers could compromise the confidentiality, integrity, or availability of the systems.

Library Did Not Always
Develop Remedial Action
Plans and Did Not Always
Close Those That Had Been
Developed in a Timely Fashion

When a security weakness is identified as part of security testing, agencies should develop a remedial action plan, also known as a plan of action and milestones (POA&M) to address the issue. Such a plan assists agencies in identifying, assessing, prioritizing, and monitoring progress in correcting security weaknesses that are found in information systems. NIST guidance emphasizes the use of such plans in order to document the organization's planned actions to correct identified weaknesses.⁹⁵

The Library has established a policy for developing and monitoring remedial action plans. According to Library policy, when weaknesses are discovered during a security assessment, a POA&M must be produced, to include a schedule for implementing any mitigation.⁹⁶

⁹⁵NIST, SP 800-37, Rev. 1.

⁹⁶Library of Congress, *Information Technology Security Directive 01*.

However, the Library did not always follow its policy. Specifically, eight of the nine systems that we reviewed had POA&Ms that were delayed and, in many cases, POA&M items were over a year past their expected completion date. For one system—the OSEP Physical Security Network—although OSEP’s 14 open POA&M items from its security testing in September 2013 were to be completed by September 2014, according to the CISO, OSEP has not reported any updates for these items since they were opened in September 2013. Additionally, as of December 2014, of the 229 items included in the POA&Ms for the other eight selected systems, 49 had a status of “delayed.” Of particular concern are the 28 POA&M items for PICS/NIOSS that were identified in 2011 and have yet to be completed. Table 5 shows the number of delayed POA&M items for the other eight selected systems.

Table 5: Plan of Action and Milestone (POA&M) Status for Selected Systems, as of December 2014

System	Number of delayed POA&M items
Application Hosting Environment	6
Library of Congress Data Network	0
Library of Congress Office Automation System	3
Enterprise Infrastructure General Support System	2
eCO	2
SYMIN II	6
PICS/NIOSS	28
Momentum	2

Source: GAO analysis of agency documentation. | GAO-15-315
Note: We did not include the OSEP Physical Security Network in this table because OSEP had not reported updates to its POA&M items since September 2013.

The CISO acknowledged that POA&M closure has been a known issue for some time, noting that some items have been open for multiple years. As previously mentioned, Library business owners are responsible for ensuring that their systems are in compliance with Library information security policies. At the conclusion of our review in March 2015, the interim CIO stated that she received briefings on the status of POA&Ms in February and March 2015 and will meet with the heads of service units to review older POA&M items and discuss their resolution.

Until weaknesses with the Library’s remediation of vulnerabilities have been resolved, they will compromise the ability of the agency to track,

Library Systems Did Not Always Have Authorization to Operate

assess, and accurately report the status of the agency's information security program.

Under NIST guidance, after testing is completed, organizations are to compile an authorization package—composed of the security plan, testing report, and POA&M items—for the system's authorizing official to review.⁹⁷ The authorizing official is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk. According to NIST guidance, if the authorizing official, after reviewing the authorization package, deems that the risks (e.g., unaddressed vulnerabilities) are acceptable, an authorization to operate is issued for the information system. The information system is authorized to operate for a specified time period in accordance with the terms and conditions established by the authorizing official. Additionally, NIST guidance states that authorizing officials can also deny authorization to operate for an information system or, if the system is already operational, halt operations if unacceptable risks exist.

To its credit, the Library's policy is consistent with NIST guidance; specifically, it requires authorization packages to be created prior to receiving authorization to operate.⁹⁸ Additionally, Library policy states that, until the system has authorization to operate, it cannot be deployed as an operational system. Until recently, Library policy required that systems be reauthorized every 3 years as part of the certification and accreditation process. In November 2014, as part of the Library's adoption of continuous monitoring, the Library revised its policy to require that, after the initial authorization to operate is in place, systems only be reauthorized in the event of a major change (e.g., software or hardware upgrade). According to draft Library guidance on implementing continuous monitoring, in place of the 3-year reauthorization cycle, authorizing officials will review the reported security status on an ongoing basis to form a continuous authorization decision.

However, the Library did not always consistently implement its policy. As of January 2015, four systems—SYMIN II, eCO, Library of Congress Office Automation System, and Library of Congress Data Network—were operating without a current authorization.

⁹⁷NIST, SP 800-37, Rev. 1.

⁹⁸Library of Congress, *Information Technology Security Directive 01*.

-
- With respect to SYMIN II, it did not have this authorization because, as previously mentioned, it had not completed its security testing.
 - Regarding eCO, the Deputy Director of the Copyright Office's Technology Office signed a waiver moving the date for the authorization package to be completed from May 2014 to May 2015. The waiver cited multiple upgrades that were to occur between May 2014 and May 2015.
 - Regarding the Library of Congress Office Automation System and the Library of Congress Data Network, the ITS Assistant Director for Operations signed waivers for the systems that allowed them to postpone their authorization to operate to October 2015 and July 2015, respectively. The waivers cited the need to complete testing, which was delayed because the contractor used to perform that testing was engaged in security testing for another system.

Additionally, for two systems—the OSEP Physical Security Network and the Application Hosting Environment—the Library did not ensure that authorizations to operate were signed in a timely manner.

- With respect to the OSEP Physical Security Network, although the system has been operational since 2003, the Library did not authorize the system to operate until February 2015. This is particularly concerning because the Library has classified this system as high impact—that is, it has determined that the loss of the system's confidentiality, integrity, or availability could be expected to have a catastrophic effect on organizational operations, organizational assets, or individuals. In a written response, the Library stated that, although OSEP completed an authorization package for this system in September 2013, the authorization was not completed until February 2015 because of a lack of program oversight.
- Regarding the Application Hosting Environment, although ITS signed the authorization to operate for the system in October 2014, this was 4 months later than allowed by Library policy. During this time, the Application Hosting Environment continued to operate. Similar to eCO, the Director of ITS signed a 4-month waiver that extended the authorization to operate, citing the need for additional time to finalize the authorization package.

The CISO acknowledged that these systems did not have authority to operate, but noted that, instead of just extending the authorization, the Library requires service units to sign a waiver reflecting a risk-based

decision to continue operating the systems without authorization. Although extending the time required to obtain authorization to operate may occasionally be valid, the Library's persistent use of these waivers increases the probability that risks, such as unaddressed vulnerabilities, are not being communicated to management. This concern is heightened by the sometimes extended length of time associated with these delays.

The CISO also added that these weaknesses should not recur once the Library implements its continuous monitoring program, because service units will not need to reauthorize systems at the end of each certification and accreditation cycle. Instead, the Library's continuous monitoring program will allow authorizing officials to review the reported security status on an ongoing basis to make continuous authorization decisions. If the Library fully establishes and implements its continuous monitoring program, it will be better positioned to ensure that continuous authorization decisions are fully informed. However, as previously mentioned, although the Library has established policy for continuous monitoring, its guidance on how service units are to carry out this policy has not been finalized. Until its approach to continuous monitoring is fully implemented, the Library will not have assurance that appropriate officials have been informed of system risks and that these officials have either accepted these risks and assumed responsibility for them, or halted system operations until the risks are acceptable.

Library Systems Did Not Always Have Contingency Plans

Contingency planning controls are intended to provide assurance that, when unexpected events occur, essential operations can continue without interruption or can be promptly resumed and that sensitive data are protected. Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an entity's ability to accomplish its mission. If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. According to NIST guidelines, agencies should develop contingency plans for their information systems that, among other things, provide established procedures for assessment and recovery of systems following a system disruption.⁹⁹

⁹⁹NIST, SP 800-53, Rev. 4.

Security Awareness and
Privacy Training Policies Were
Not Fully Documented, and
Training Was Not Tracked or
Completed by All Users

The Library has developed a policy on contingency planning that requires system owners to ensure, for each IT system under their purview, the development and maintenance of a contingency plan. These plans should include, among other things, procedures for ensuring that the systems are successfully recovered.¹⁰⁰

However, only three of the nine selected systems—Enterprise Infrastructure General Support System, eCO, and Momentum—had a contingency plan that addressed NIST guidance and Library policy. For three of the systems—the Application Hosting Environment, Library of Congress Data Network, and the Library of Congress Office Automation System—their security plans indicated that contingency planning was to be addressed in the Library’s Information Technology Continuity of Operations Plan; however, this plan does not include specific procedures for recovering these systems. Additionally, three systems—OSEP Physical Security Network, SYMIN II, and PICS/NIOSS—have not established contingency plans.

The CISO acknowledged that these systems did not have contingency plans and stated that he will open POA&Ms for them to be created. Until it develops contingency plans for its key information systems, the Library may have delays in recovering systems or may be unable to recover systems entirely in the event of a large disaster.

According to NIST guidelines, agencies should provide basic security awareness training to all information system users as part of initial training for new users, and regular refresher training to all users on an agency-defined basis. This training should inform personnel, including contractors and other users of information systems supporting the operations and assets of an agency, of information security risks associated with their activities and their roles and responsibilities to effectively implement the practices that are designed to reduce these risks. In addition, NIST guidelines call for organizations to administer basic privacy training on a regular basis.¹⁰¹

The Library has established policies and procedures that generally address NIST guidelines on security awareness training. Specifically,

¹⁰⁰Library of Congress, *Information Technology Security Directive 01*.

¹⁰¹NIST, SP 800-53, Rev. 4.

Library policy requires all personnel, including staff, contractors, and volunteers with access to Library of Congress IT systems, to complete the IT security awareness training on an annual basis.¹⁰² The Chief Privacy Officer and CISO told us that privacy is also covered in the Library's annual security awareness training, and the CISO provided a copy of the fiscal year 2014 training, which addresses employee responsibilities for handling PII.

However, the Library did not ensure that all required users completed security awareness and privacy training. Of the personnel tracked in its database of record, the Library estimated that 4,131 of 4,145 users (99.7 percent) completed the required awareness training in fiscal year 2014. However, we identified 1,345 user accounts—204 from OSEP, 42 from CRS, and 1,099 from the rest of the Library—with access to Library IT systems that were not tracked in the database. Library officials were unable to provide comprehensive information on how many of the additional personnel had completed the required awareness training.

- Regarding the 204 accounts in OSEP, the Library reviewed 47 accounts that we identified. Of those, the Library found 8¹⁰³ in its database of record, and only 3 of those individuals reportedly took the training in fiscal year 2014. According to the Director of Workforce Performance and Development, many of these accounts are Capitol Police personnel who have access to OSEP's Physical Security Network, but who are not tracked in the Library's database of record. The CISO stated that the Library does not provide security awareness training to these users. Instead, they rely on the Capitol Police to provide adequate training. Additionally, OSEP stated that, although the Capitol Police provide training to their staff, the Library does not ensure that all Capitol Police users of Library systems have completed the training.

¹⁰²Library of Congress, *Information Technology Security Directive 01*.

¹⁰³The Director of the Office of Workforce Performance and Development noted that, because the e-mail addresses—which the Library uses as a unique identifier—were different in the OSEP list and its database of record, the nine matches were performed using names. Given the common occurrence of individuals with the same name, it is possible that one or more of the matches were not associated with the same person.

-
- Of the 42 accounts from CRS, the Library found 28 names in its database of record—only 12 of which reportedly took the training in 2014.
 - With respect to the 1,099 accounts for the rest of the Library, the Library reviewed 103 accounts. Of those, the Library found 55 in the database of record, and only 14 of those individuals reportedly took the training in 2014.

The Library cited multiple reasons for the differences between the accounts we identified and the training database of record. According to the Director of the Office of Workforce Performance and Development, some of the accounts that we identified appeared to be associated with personnel who no longer work for the Library. Additionally, that official stated that, in some cases, the user name for an individual was different in the training database of record and the database used to authorize access to Library systems.

At the conclusion of our review, the Assistant Director for Human Resource Operations stated that the Human Resources Services, ITS, and other appropriate offices will assemble a complete and accurate list of staff, contractors, and others with access to Library networks in fiscal year 2014. That official added that Human Resources Services will also implement a process for obtaining a complete and accurate listing of staff for the next cycle of training.

Until the Library ensures that all personnel with access to its network take security awareness training, it will have less assurance that they have a basic awareness of information security issues and agency security and privacy policies and procedures.

Contracts Did Not Always Address Security and Privacy Requirements

The Library relies on the services of contractors to operate and secure its computer systems on its behalf. While contractor personnel who operate systems and provide services to federal agencies can provide significant benefits, they, as with government employees, can also introduce risks to agency information and systems, such as the unauthorized access, use, disclosure, and modification of federal data.

In order to ensure that contractors meet information security and privacy requirements, NIST recommends that organizations include information

security and privacy requirements in their contracts for IT systems and services.¹⁰⁴ Toward this end, Library policy calls for all IT contracts to require contractors to comply with Library security and privacy requirements.¹⁰⁵ Additionally, the Library has developed standard sections addressing NIST guidelines that are required in all IT solicitations.¹⁰⁶

However, contracts for eight of the nine selected systems we reviewed did not fully address Library security and privacy requirements for IT system and services contracts. Specifically, only one contract—for PICS/NIOSS—included the standard sections that Library policy requires.

In a written response, the Library agreed that contracts for eight systems did not address Library requirements and explained that this occurred because internal reviewers did not consistently identify the missing information. The Library also has made draft revisions to its contractual security requirements because officials determined that the prior requirements were overly broad. These revisions are consistent with NIST guidelines. For example, the standard sections require the contractor's work to be conducted in accordance with the latest version of NIST's information security and privacy controls.¹⁰⁷ The Library told us that the Office of General Counsel is to review these requirements for promulgation in fiscal year 2015. However, the Library has yet to establish a date for finalizing these requirements.

In the interim, the Library stated that service units are to review all current contracts for IT systems and services to ensure that the current requirements have been incorporated. The Library added that the Office of Contracts and Grants Management, with support from the Office of General Counsel, will continue to review statements of work for IT systems and services and identify any potential gaps in IT security requirements prior to contract award.

¹⁰⁴NIST, SP 800-53, Rev. 4.

¹⁰⁵Library of Congress, *Information Technology Security Directive 01*.

¹⁰⁶Library of Congress, *Inclusions for All IT Solicitations* (June 8, 2009).

¹⁰⁷NIST, SP 800-53, Rev. 4.

Library Did Not Fully Assess
Privacy Risks in Privacy Impact
Assessments

Until the Library finalizes its standard contract sections for information security and privacy and ensures that contracts for IT systems and services include these provisions, it increases the risk that meeting enterprise-wide security requirements could require costly contract modifications or that these requirements will not be implemented according to Library policy.

According to NIST guidelines, agencies should assess privacy risks of an information system when developing a privacy impact assessment.¹⁰⁸ These risk assessments are intended to help program managers and system owners identify privacy risks and techniques to reduce those risks.

Library policy is consistent with NIST guidance. Specifically, it calls for privacy impact assessments to be performed for all Library systems.¹⁰⁹

However, the Library only conducted privacy impact assessments for two of the nine selected systems we reviewed—Enterprise General Support System and PICS/NIOSS.

- As previously mentioned, the security tests for four systems—Library of Congress Office Automation System, eCO, SYMIN II, and Momentum—reported that privacy impact assessments had been developed as appropriate; however, when asked for copies of these assessments, Library officials responsible for these systems stated that privacy impact assessments had not been performed. According to the CISO, POA&M items have been opened for privacy impact assessments to be performed on these systems.
- Security testing for the OSEP Physical Security Network stated that the system did not have a privacy impact assessment and this has been an open POA&M item since September 2013.
- Security testing for the Application Hosting Environment determined that the system did not have a privacy impact assessment. In describing the risk associated with this weakness, the test report stated that, although there may be systems hosted on the Application

¹⁰⁸NIST, SP 800-53, Rev. 4.

¹⁰⁹Library of Congress, *Information Technology Security Directive 01*.

Hosting Environment that collect, process, or store PII, these systems have their own privacy impact assessments. However, as previously noted, eCO, which is hosted on the Application Hosting Environment, did not have a privacy impact assessment. The testing report also recommended that the Library conduct a privacy impact assessment to verify that the Application Hosting Environment does not collect, process, or store PII independent of the systems that it hosts.

- Regarding the Library of Congress Data Network, its security plan states that this control is not applicable because the system does not collect, maintain, or disseminate information—it only transfers data from one place to another. However, NIST guidance calls for privacy impact assessments to be performed to assess risks resulting not only from the collection, storing, or use of PII, but also the transmission of such data.¹¹⁰

One reason for the inconsistent performance of privacy impact assessments is the lack of oversight to ensure compliance with Library-wide privacy policy and requirements. According to the Library's General Counsel, who also serves as the Chief Privacy Officer, the Office of General Counsel does not review the Library's privacy program because it is not required to do so. Rather, that official told us that she relies on the service units to carry out their responsibilities. However, according to Library policy, the Chief Privacy Officer has overall responsibility for all of the Library's privacy information activities, including ensuring PII policy compliance.¹¹¹ Additionally, the policy states that the Chief Privacy Officer shall have overall responsibilities for managing the protection of PII maintained in the Library's systems and files.

Until the Chief Privacy Officer establishes and implements a process for reviewing the Library's privacy program, including ensuring that privacy impact assessments have been conducted for all IT systems, PII collected by the Library will be at increased risk of compromise.

¹¹⁰NIST, SP 800-53, Rev. 4.

¹¹¹LCR 1921.

Control Weaknesses Threaten Library Information and Systems

A basic management objective for any agency is to protect the resources that support its critical operations and assets from unauthorized access. An agency can accomplish this by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computer resources (e.g., data, programs, equipment, and facilities), and securely configure information systems, thereby protecting them from unauthorized disclosure, modification, and loss. Controls relating to these areas include policies, procedures, and protections regarding authorization, identification and authentication, cryptography, background investigations, and environmental safety. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of sensitive information and information systems supporting the Library's mission.

The Library did not effectively implement or securely configure key security tools and devices on the nine selected systems to sufficiently protect users and information from threats to confidentiality, integrity, and availability. Specifically, weaknesses existed in the following control categories:

- **Authorization:** The Library did not always establish and implement a process for documenting approvals for elevated permissions to selected systems. NIST guidance and Library policy call for such a process in order to ensure that only authorized users can access a system.¹¹² Specifically, only one of the nine selected systems—Momentum—provided records documenting who approved accounts with elevated privileges and why those accounts were created. At the conclusion of our review, the Library acknowledged in a written response that it had not fully established and implemented such a process. The Library stated that the IT Security Group has requested account creation procedures from all information system security officers and will create a POA&M for all systems without these procedures. Until the Library establishes and implements a process for documenting elevated permissions, in the event of an incident the Library may not be able to determine if an account was appropriately created or had been accidentally or maliciously assigned inappropriate permissions.

¹¹²NIST, SP 800-53, Rev. 4.

-
- **Identification and authentication:** The Library did not always require two-factor authentication for access to sensitive Library resources. NIST recommends using multifactor authentication¹¹³ for users to access network resources.¹¹⁴ Until the Library consistently uses two-factor authentication, there is increased risk that its systems will not limit access appropriately.
 - **Cryptography:** The Library did not always ensure that sensitive information transmitted across its network was being adequately encrypted.¹¹⁵ NIST recommends that organizations employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.¹¹⁶ In a written response at the conclusion of our review, the Library acknowledged this weakness and opened a POA&M to address it, with a scheduled completion date of July 2015. Until the Library addresses this weakness, there is increased risk that an individual could capture information, such as user credentials or other sensitive data, and use the information to gain unauthorized access to data and system resources.
 - **Background investigations:** As previously mentioned, the Library did not perform background investigations for seven individuals with elevated privileges to three systems—Library of Congress Data Network, PICS/NIOSS, and OSEP Physical Security Network. NIST guidance¹¹⁷ and Library policy¹¹⁸ call for personnel to undergo background screening commensurate with their level of access to Library systems in order to ensure that they are trustworthy and meet established security criteria. At the conclusion of our review, the

¹¹³NIST defines multifactor authentication as authentication using two or more factors to achieve authentication. Factors include (1) something you know (e.g., password or personal identification number); (2) something you have (e.g., cryptographic identification device or token); or (3) something you are (e.g., biometric).

¹¹⁴NIST, SP 800-53, Rev. 4.

¹¹⁵Cryptography involves the use of mathematical functions called algorithms and strings of seemingly random bits called keys to, among other things, encrypt a message or file so that it is unintelligible to those who do not have the secret key needed to decrypt it, thus keeping the contents of the message or file confidential.

¹¹⁶NIST, SP 800-53, Rev. 4.

¹¹⁷NIST, SP 800-53, Rev. 4.

¹¹⁸Library of Congress, *Information Technology Security Directive 01*.

Library said in a written response that it would take action to address this by performing background investigations for six of the individuals. The Deputy Chief of OSO stated that the office removed elevated privileges to the OSEP Physical Security Network for the remaining individual.

- **Environmental safety:** The Library did not ensure that an annual inspection of the fire suppression system for the primary data center was performed in a timely manner. NIST recommends that organizations employ and maintain fire suppression and detection systems for the information systems and regularly inspect those systems for deficiencies.¹¹⁹ After we informed the Library of this issue, an inspection of the system was performed.

In addition to the above weaknesses, we identified other security weaknesses in controls related to authorization, configuration management, boundary protection, patch management, and physical security that limit the effectiveness of the security controls on the selected systems and unnecessarily place sensitive information at risk of unauthorized disclosure, modification, or exfiltration. We intend to issue a separate report with limited distribution to describe in greater detail the control weaknesses we identified during this review.

¹¹⁹NIST, SP 800-53, Rev. 4.

Library Has Not Ensured That IT Services Are Supporting Organizational Needs, Resulting in Inconsistent Satisfaction with Services and Duplicative or Overlapping Efforts

Recognized industry best practices call for ensuring that an organization's IT services are aligned with and actively support its business needs. As the central IT organization within the Library, the Office of Strategic Initiative's Information Technology Services (ITS) directorate is responsible for providing an array of IT services to other units within the Library.

However, ITS has not ensured that its services support the business needs of the Library. While it has developed a catalog that identifies the services it provides to other units within the agency, it has not established service-level agreements for all these services that include agreed-upon performance targets. The Library has drafted a new policy for such service-level agreements, but it has yet to be finalized. Further, our survey of service units within the Library revealed that they were often not satisfied with the services provided by ITS. Although ITS has begun to conduct customer satisfaction surveys, it has not developed a plan for improving satisfaction with its services Library-wide. Moreover, inconsistent satisfaction with the services provided by the Library's central IT office has likely contributed to duplicative or overlapping efforts across the Library. Specifically, units across the Library performed many of the same functions as ITS, including maintaining their own networks and servers, purchasing duplicate copies of desktop software, and maintaining duplicative security solutions.

Key Service Management Practices Have Not Been Implemented

The development and implementation of Information Technology Infrastructure Library practices are widely recognized as hallmarks of successful public and private IT organizations.¹²⁰ This guidance includes key practices to ensure that IT services are aligned with the business needs of an organization and actively support them. For example:

- **A service catalog** identifies all current IT services delivered by the service provider to its customers.
- **A service-level agreement (SLA)** establishes agreement between an IT service provider and a customer to describe the IT services, specify the responsibilities of both parties, and document the expected

¹²⁰Lou Hunnebeck and Colin Rudd, *ITIL: Service Design* © (London: The Stationary Office, 2011). The guide is available at: <http://www.axelos.com/Publications-Library/IT-Service-Management-ITIL/>.

service-level targets.¹²¹ Organizations should define how these agreements are to be structured such that IT services and customers are covered in a manner best suited to the organization's needs (e.g., one agreement for each service or one for each customer).

As the central IT organization within the Library, ITS provides services to the various service units. According to Library policy, ITS management and staff are to work to satisfy customer requirements, provide outstanding customer service, and represent customer interests. The Director of ITS stated that ITS has adopted Information Technology Infrastructure Library practices in order to meet customer needs.

Although ITS has developed a service catalog, it has not fully established SLAs.

- **Service Catalog:** To its credit, ITS developed a service catalog that captures its current IT services. Specifically, the catalog identified 31 administrative, management, and technical IT services that are available to ITS customers. For example, ITS provides services that cover service desks (e.g., problem management), backup and recovery, and network services (e.g., design, construction, security and maintenance).
- **SLAs:** The Library has not defined a structure for ensuring that IT services and customers are covered by SLAs in a manner that meets the service units' needs. In the absence of such a structure, ITS has established 19 SLAs with individual service units, each of which describes the services that ITS will provide and the roles and responsibilities of each party. For example, ITS established an SLA with the Copyright Office for the management, operation, maintenance, and security of eCO. The SLA identifies six services—including services relating to disaster recovery and database management—and describes the roles and responsibilities for both ITS and Copyright. However, the 19 SLAs do not fully address all IT services and customers, or always establish expected service-level targets. Specifically:

¹²¹Examples of service-level targets include the hours that customers can expect the service to be available (e.g., 8:00 a.m. to 6:00 p.m., Monday through Friday), availability of a service during the agreed service hours (e.g., 99.5 percent), and maximum number of failures or incidents that can be tolerated within an agreed time period.

-
- The SLAs do not address all of the services in ITS's service catalog. Specifically, the agreements collectively only address 14 of the 31 services ITS provides to the Library of Congress. For example, ITS does not have a SLA that addresses the services it provides CRS for its Enterprise Infrastructure General Support System.
 - The SLAs do not include service-level targets for all services. Specifically, only 9 of the 19 SLAs contained such targets, covering 3 of the 31 services. For example, according to the SLA governing the management of eCO, in the event of a disaster that affects IT operations in the main data center, ITS is to recover the eCO system at its alternate computing facility within 24 hours of the disaster. However, ITS did not establish targets for any of the other 28 services in its service catalog, such as the amount of time systems are available as part of its hosting service.

According to the ITS Assistant Director for Operations, ITS recently established service-level targets for one additional service: the service desk. These targets pertained to how quickly problems should be resolved, depending on their severity. He added that these targets reflect ITS's intent to provide the same level of service to all of its customers. However, the service units have not agreed to these targets. According to the ITS Assistant Director for Operations, he briefed the services units on these targets and received feedback, but acknowledged that ITS did not establish formal agreements with the service units. Without agreement from the service units, it is unclear whether these service-level targets will meet the unique business needs of the Library's service units.

The ITS Assistant Director for Operations further stated that ITS has drafted a policy documenting its approach to developing SLAs. If approved, the policy will call for ITS to continue to develop two types of SLAs—(1) those with individual service units to define a unique service, and (2) SLAs with the Library of Congress as a whole. Although the draft policy calls for the use of service-level targets for Library-wide SLAs, it does not do so for SLAs with individual service units. Moreover, given that the policy is to govern ITS, it is unclear whether the policy will reflect an SLA structure that covers the IT services and customers in a manner best suited to meet the needs of both ITS and its customers. For example, the policy would no longer allow ITS to enter into agreements with individual service groups within a service unit—such as NLS. At the conclusion of our review, the ITS Assistant Director for Operations told us that ITS submitted the policy to the Library's interim CIO in January 2015. He also

stated that the ITSC and Executive Committee will complete their reviews by May 2015 and that SLAs under the new policy will be completed by September 2015.

Until the Library establishes and implements an SLA structure—to include the use of service-level targets—that meets the needs of the organization, there is increased risk that ITS will not provide services that meet the needs of its customers. In the case of the Copyright Office, this risk has been realized. For example, according to the Copyright CIO, the Library controls when eCO is shut down for maintenance and these have, at times, been scheduled during periods of heavy traffic from the office's external users.

Service Units Were Often Not Satisfied with Library IT Services, but ITS Has Not Established a Plan for Improvement

The weaknesses in ITS's implementation of service-level management practices were reflected by inconsistent satisfaction with the services that it provides. To be successful, IT organizations should measure the satisfaction of their users and take steps to improve it. In this regard, effectively managing activities to improve user satisfaction requires planning and executing such activities in a disciplined fashion. The Software Engineering Institute's IDEALSM model is a recognized approach for managing efforts to make system improvements.¹²² According to this model, user satisfaction improvement efforts should include a written plan that serves as the foundation and basis for guiding improvement activities, including obtaining management commitment to and funding for the activities, establishing a baseline of commitments and expectations against which to measure progress, prioritizing and executing activities and initiatives, determining success, and identifying and applying lessons learned. Through such a structured and disciplined approach, improvement resources can be invested in a manner that produces optimal results.

However, ITS has not demonstrated that user satisfaction improvement efforts are being guided by a documented plan that defines prioritized improvement projects and associated resource requirements, schedules, and measurable goals and outcomes. Instead, efforts that the office undertook to improve user satisfaction were ad hoc and did not meet with

¹²²IDEALSM is a service mark of Carnegie Mellon University and stands for initiating, diagnosing, establishing, acting, and leveraging. For more information on this model, see *IDEALSM: A User's Guide for Software Process Improvement* (CMU/SEI-96-HB-001).

success. Specifically, ITS only measures user satisfaction for 1 of the 31 services it provides to other service units (help desk services).

In the absence of comprehensive data on ITS customer satisfaction, we surveyed the heads of the Library's seven service units, as well as the head of NLS, about the extent to which they were satisfied with the IT services provided by ITS. The results showed that ITS's customers—the Library's service units—vary in the extent to which they are satisfied with the services provided by ITS, but collectively these customers are generally not satisfied.

Specifically, the average score for all IT services provided by ITS was 3.17 (on a 5-point satisfaction scale, where 1 is very dissatisfied and 5 is very satisfied),¹²³ and the scores for each service ranged from a low of 2.33 to a high of 4.40. More specifically, only 2 of the 29 services had an average score above 4, indicating that service units were generally very satisfied or somewhat satisfied with these services. The majority of the services—19 of the 29 services—ranged from 3.75 to 3.0, indicating that service units were generally neither satisfied nor dissatisfied or somewhat satisfied with these services. Lastly, a little more than a quarter of the services (8 of 29) had an average score below 3, which indicates that service units were generally neither satisfied nor dissatisfied or somewhat dissatisfied. Table 6 shows the average customer satisfaction score for each of the 29 IT services that ITS provides.¹²⁴

¹²³Specifically, we asked survey respondents to rate their organization's satisfaction using the following scale: 5 is "very satisfied," 4 is "moderately satisfied," 3 is "neither satisfied nor dissatisfied," 2 is "moderately dissatisfied," and 1 is "very dissatisfied."

¹²⁴As previously mentioned, ITS's service catalog identifies 31 services. However, we removed 4 of the services from our survey, because, according to the Director of ITS, ITS does not provide them to customers outside of ITS. We also added 2 services based on the comments and suggestions we received during our pretests, namely Internet services and multimedia group production team assistance services.

Table 6: Information Technology Services (ITS) Customer Satisfaction Survey Results

IT service	Average score
ITS Scanning Services	4.40
Multimedia Group Production Team Assistance	4.29
Special Events IT Support Services	3.75
Customer Relationship Services	3.63
Audio/Visual Services	3.63
Voice Telecommunications Services	3.50
Account & Access Management Services	3.43
Hosted Application Services	3.43
Facility Services	3.29
Help Desk Services	3.25
Mobile Device Services	3.25
Network Services	3.25
Internet Services	3.25
Communications Support Services	3.14
Server Hosting Services	3.14
Workstation Services	3.14
Messaging & Collaboration Services	3.13
Change Management Services	3.00
Asset Management Services	3.00
Technology Assessment Services	3.00
IT Test Environment Services	3.00
Continuity of Operations & Disaster Recovery	2.88
Enterprise Storage Backup & Recovery Services	2.86
Software Development Services	2.71
Project/Program Management Services	2.63
IT Planning Support	2.57
Technical Architecture Services	2.50
Information Security Management Services	2.50
Consultation & Support Services	2.33

Source: GAO survey of heads of Library of Congress service units and NLS. | GAO-15-315

In addition to providing scores, the survey respondents also provided written comments. Five factors were cited by two or more respondents as contributing to their dissatisfaction with the services provided by ITS:

-
- **Lack of transparency:** Six of the eight respondents cited a lack of transparency from ITS as a source of dissatisfaction with its services. For example, two respondents discussed transparency issues with the Library's IT Continuity of Operations Planning: one cited issues with testing, while the other discussed a need for more transparency with respect to the decision making on the priority of systems to be recovered in the event of a disaster.¹²⁵ Further, one respondent stated that OSI/ITS develops the IT strategic direction for the organization without consulting with the senior leadership of the respondent's service unit.
 - **Poor quality of service:** Five respondents cited the poor quality of service provided by ITS as a key source of dissatisfaction. For example, three respondents described problems with the Library's telework infrastructure, noting that the service is frequently unavailable. Additionally, two respondents stated that the configuration of the software used to prevent access to certain websites results in overbroad restrictions. One respondent also noted that the implementation of the process used to gain access to restricted sites is uneven—some requests are resolved in a timely manner, while others are not. In addition, one respondent stated that during recent data center emergencies, data were lost by ITS. Similarly, according to that respondent, during a power outage in 2009, ITS could not maintain power to the data center because of known problems with one of its emergency power devices, resulting in unplanned outages and disruptions to day-to-day operations.¹²⁶
 - **Inconsistent implementation of IT management processes:** Five respondents cited inconsistent implementation of IT management processes as one of the reasons for their dissatisfaction with some of the services provided by ITS. For example, two respondents described weaknesses in ITS's implementation of project

¹²⁵According to the ITS Assistant Director for Operations, ITS does not independently determine the priority levels of systems to be recovered in the event of a disaster. He stated that providing more transparency on the priority setting process is the responsibility of the ITSC.

¹²⁶According to the ITS Assistant Director for Operations, ITS is not responsible for power emergencies. He explained that the Architect of the Capitol is responsible for providing power and uninterruptable power supply services to the data center. He also added that there have not been any data lost in any of the power emergencies or planned power outages.

management practices, noting that ITS needs more experienced project managers and improvements in cost estimating. Additionally, four respondents cited problems with ITS's change management practices: two respondents stated that ITS frequently does not follow its established process, one said that the process takes months to review applications, and the other said that more consistent configurations and settings are needed. Furthermore, two respondents stated that the Library has not conducted testing needed for its continuity of operations and disaster recovery process. Additionally, three respondents described challenges relating to the certification and accreditation process, citing problems with cost, timeliness, and inconsistent implementation.

- **Inconsistent communication:** Four respondents cited inconsistent communication as a reason for dissatisfaction with some of the services provided by ITS. For example, three respondents stated that ITS did not always effectively communicate when outages in IT systems were to occur. One respondent described instances where they were informed of outages affecting public-facing systems from external customers before they were notified by ITS. In addition, one respondent described instances where they received conflicting information and direction from ITS.
- **Use of outdated technology:** Four respondents cited outdated technology used by ITS as a reason for dissatisfaction with its services. For example, two respondents stated that ITS needs to invest in a modern infrastructure; one respondent explained that, without such an infrastructure, the Library will not be able to meet the technical requirements for acquiring and stewarding digital collections.

According to ITS, it has recently taken steps to measure and improve user satisfaction. For example, in September 2014, ITS began conducting surveys of customers that used its service desk, and reported that it received very positive feedback on this service.

However, ITS has not demonstrated that user satisfaction improvement efforts are being guided by a documented plan that defines prioritized improvement projects and associated resource requirements, schedules, and measurable goals and outcomes. Given the Library's reliance on IT services provided by ITS, as well as the results of our survey, it is critical that ITS identify and implement improvements in a disciplined and structured fashion. For example, as discussed later in this report, continued dissatisfaction with ITS services may have led customers to perform the services themselves in order to improve their IT performance

and decrease their reliance on ITS. Without a documented improvement plan, efforts to improve user satisfaction may be reduced to trial and error, and ITS will not be able to adequately ensure that it is effectively investing resources on improvement efforts that will satisfy users.

Duplicative or Overlapping IT Activities Are Being Performed by Service Units across the Library

The lack of an enterprise-wide approach to managing IT, in combination with dissatisfaction with the services provided by ITS, has contributed to other service units independently performing duplicative or overlapping activities in support of their business needs. For example, although ITS is responsible for the Library's primary IT service desk (which provides IT troubleshooting service to all Library personnel), CRS and Library Services maintain separate service desks for their personnel. According to the CRS CIO and the Chief of Library Services Automation Planning & Liaison Office, although the service desks maintained by CRS and Library Services perform some functions that ITS's service desk performs (e.g., resetting passwords), their service desks also perform unique functions. However, because they perform some overlapping functions, the Library may be spending more than it needs to on these service desks.

As another example, as previously mentioned, according to the official who served as acting CIO from April 2014 to January 2015, each service unit is responsible for managing its own human capital skills. For example, that official told us that, for its own staff needs, OSI identifies skills and competencies when an individual leaves the organization or when OSI plans to hire additional staff.

Additionally, although the service units vary in the extent to which they purchase IT, all of them have purchased commodity IT¹²⁷ in the past 3 years. For example, most of the service units have purchased desktops, laptops, and workstation software. Table 7 identifies commodity IT purchased by Library service units and NLS in the past 3 years.

¹²⁷According to the Office of Management and Budget, commodity IT includes services such as IT infrastructure (data centers, networks, desktop computers and mobile devices); enterprise IT systems (e-mail, collaboration tools, identity and access management, security, and web infrastructure); and business systems (finance, human resources, and other administrative functions).

Table 7: Examples of Key Commodity IT Purchased by Library Units in the Past 3 Years

Examples of commodity IT	Library unit							
	CRS	Copyright	Librarian	Library Services	NLS	Law	OSO	OSI
Desktop systems	X		X	X	X		X	X
Laptops	X	X	X	X	X	X	X	X
Mobile devices	X	X		X	X		X	X
Servers	X	X			X		X	X
Network devices	X			X	X		X	X
Workstation software	X	X		X	X	X	X	X
Server software	X	X		X	X		X	X

Source: GAO analysis of statements from Library of Congress officials. | GAO-15-315

As a result, there is increased risk that the service units will make duplicative investments in commodity IT. In the case of monitors and workstation software, this risk has been realized. Because, as previously discussed, the Library did not have an accurate inventory of its non-capitalized IT assets, we visited the Library's warehouse in Landover, Maryland. At that facility, we observed that, as of December 2014, ITS had approximately 100 24-inch monitors that were purchased in 2010.¹²⁸ However, instead of using the monitors purchased by ITS, Library Services purchased 82 additional 24-inch monitors between June 2013 and July 2014. Of particular concern is that Library Services purchased all of these monitors after the Library's IG issued a report noting this surplus of monitors.¹²⁹

According to Library Services, at the time that it purchased the monitors, it was not aware that ITS had 24-inch monitors. It added that ITS previously maintained a "PC Store" from which Library Services acquired computers, monitors, printers, and scanners; however, this service was discontinued about 3 years ago. Since that time, according to Library Services, its attempts to purchase equipment have met with mixed success, and it has often needed to acquire equipment independently.

¹²⁸Although these monitors were several years old, according to ITS officials, they had never been used and were still in their original packaging.

¹²⁹Library of Congress, Office of the Inspector General, *Improvements Needed to Prevent Wasteful Procurement and Inefficient Disposal of IT Workstations*, Report No. 2012-PA-101 (Washington, D.C.: Sept. 28, 2012).

Finally, Library Services stated that it recently became aware of monitors available through ITS and is working with them to obtain as many as possible to meet its needs.

The Library has also made duplicative investments in desktop software, which has led the Library to purchase too many licenses. For example, collectively, the Copyright Office, Library Services, and ITS purchased 459 licenses to Microsoft's Visio 2010 Professional, but as of November 2014 were only using 227. According to the ITS Assistant Director for Operations, service units are responsible for tracking the usage of licenses that they procure. He noted, however, that ITS is implementing a new system to be used to track and analyze data on the usage of software licenses. Additionally, according to the ITS Assistant Director for Operations, in some cases the Library has decided to purchase more licenses than are currently required in anticipation of additional Library employees, existing employees who will be reassigned to roles requiring the licenses, and new contractors who will need the licenses. However, this does not explain why the Library is not using almost half of the licenses it purchased for this application.

According to the Copyright Office Chief of Operations, the Copyright Office needs software that can allow access to the many and varied digital formats submitted by registration customers. He added that, in recent years, ITS has increasingly required the Copyright Office to purchase its own licenses for applications that were previously centrally funded and that the Copyright Office does not consistently receive information from ITS regarding what licenses the Library has or how many users are on each license.

In addition to purchasing commodity IT, each of the service units and NLS perform many of the same types of IT activities. For example, CRS, NLS, OSO, and OSI manage and support servers. Table 8 identifies key IT activities independently performed by the service units.

Table 8: IT Activities Performed by Library Units

IT activities	Library unit							
	CRS	Copyright	Librarian	Library Services	NLS	Law	OSO	OSI
Server management and support	X				X		X	X
Network management	X				X		X	X
Storage and archive	X				X		X	X
Database administration	X			X	X	X	X	X
Directory services management	X			X		X	X	X
Desktop support	X	X		X	X	X	X	X
Internet and web management	X	X	X	X	X	X	X	X
Facilities and data center management					X		X	X

Source: GAO analysis of statements from Library of Congress officials. | GAO-15-315

In performing these activities, the Library has made potentially duplicative investments in IT for four of the eight IT activities identified above. Specifically:

- **Server management and support:** ITS and CRS each operate and maintain separate environments for the same server virtualization¹³⁰ solution: VMware. As another example, OSEP and CRS maintain, separate from ITS's Application Hosting Environment, their own technical infrastructures for hosting their organizations.
- **Network management:** OSEP's Physical Security Network is completely separate from the rest of the Library's network. Consequently, OSEP acquires and maintains network devices, many of which would not be needed if its systems were hosted on the Library of Congress Data Network. Additionally, although more integrated with the Library of Congress data network than OSEP's network, CRS's Enterprise Infrastructure General Support System also includes a number of network devices that CRS purchases and manages largely independent of ITS.
- **Directory services management:** ITS, CRS, and OSEP maintain separate environments for authenticating and authorizing users and computers. These three organizations also maintain separate e-mail

¹³⁰Server virtualization enables the use of multiple operating systems and applications on a single physical server.

environments. Additionally, ITS and OSEP both operate and maintain different solutions for performing two-factor authentication.

- **Internet and web management:** Although OSI has a Web Services division, which is responsible for developing strategies, plans, standards, and policies to guide the Library's web initiatives, the Copyright Office updated its website in July 2014 independently of OSI's Web Services division. The Special Assistant to the Register of Copyrights stated that this was because OSI did not understand the office's requirements and needs. However, the Chief of the Web Services division stated that he had met with Copyright staff and attempted to reach agreement on updating the website collaboratively.

In addition, although the Copyright Office only performs two of the above-mentioned IT activities, officials have recently expressed their intent to make additional investments in IT that could be duplicative of activities performed by ITS. In particular, the Copyright Office has requested funding for its own software application development environment, as well as a "digital repository" for deposits of works (e.g., films, books, music, photographs, and software) for which copyright owners are asserting ownership and seeking protection. However, ITS has a software application development environment, and currently works with the Copyright Office to maintain digital deposits.

Another consequence of potentially duplicative IT activities is that the Library may be spending more than it needs to on IT-related staff. As previously mentioned, the IT activities performed outside of OSI and ITS are performed and led by the 134 IT staff that work for other service units. In fiscal year 2014, the Library spent about \$15 million on the salaries for these staff. Table 9 identifies the amount that each service unit spent on salaries for IT staff in fiscal year 2014.

Table 9: IT Staff Salaries by Service Unit, Fiscal Year 2014

Service unit	IT staff salaries
CRS	\$5,166,946
Copyright Office	\$1,954,565
Law Library	\$687,690
Library Services	\$5,322,607
OSI	\$30,433,675
OSO	\$930,082
Office of the Librarian	\$1,449,777

Source: GAO analysis of agency data. | GAO-15-315

As described in more detail below, officials from CRS and OSEP offered various reasons for why they needed to manage much of their IT independent of ITS, and the Copyright Office described reasons why the structure used to manage its IT systems is not adequate.

- According to the Director of CRS, CRS tries to leverage ITS resources whenever possible, and the Director described the division between ITS and CRS as a “division of labor.” However, the Director also stated that CRS needs to maintain independence when managing its IT because of its unique mission in support of Congress. In particular, the Director stated that CRS must be able to (1) provide information to Congress quickly and (2) keep its information confidential. Regarding the timeliness of CRS’s responses to Congress, a senior advisor to the CRS Director noted that CRS is directed by law to provide efficient and effective service to Congress.¹³¹ With respect to confidentiality, the Deputy Director of CRS told us that CRS considers its information gathering to be covered under the “Speech or Debate Clause” of the U.S. Constitution.¹³² Accordingly, that individual stressed the importance of keeping CRS’s information confidential, and expressed concern about storing CRS data with the rest of the Library’s data. To this end, the Director of CRS stated that it must have separate IT

¹³¹2 U.S.C. § 166(b)(1).

¹³²The Constitution protects the speech of members of Congress, stating that members of both Houses of Congress “shall in all Cases, except Treason, Felony and Breach of the Peace, be privileged from Arrest during their attendance at the Session of their Respective Houses, and in going to and from the same; and for any Speech or Debate in either House, they shall not be questioned in any other Place.” U.S. Const. art. I, § 6, cl. 1.

because its IT group has a better understanding of what CRS and Congress need than ITS. A senior advisor to the CRS Director added that CRS is directed by law to have “the maximum practicable administrative independence” in performing its duties to Congress.¹³³ According to this individual, the division between ITS and CRS has evolved over the years as a result of this administrative independence.

- Regarding OSEP, a senior electronic security engineer explained that it maintains its systems independent of ITS because it has always done so. In particular, that official stated that previous iterations of its camera and physical intrusion detection systems were not integrated with IT and, therefore, OSEP did not need the assistance of ITS. He noted, however, that these systems are now integrated with IT. The OSEP Director said the office is open to a solution that involves ITS but that ITS had expressed a lack of knowledge of security systems. The Director added that OSEP coordinated with ITS on a statement of work for an assessment of staffing, technology improvements, and best practices for its IT.
- With respect to the Copyright Office, its General Counsel stated in a memo prepared for GAO that the “current IT regime impedes the Copyright Office’s ability to carry out its legal responsibilities.” Among other things, the General Counsel stated that the existing Library IT infrastructure cannot ensure the security or integrity of digital deposits. For example, she explained that the Library has decided to host Copyright IT systems in the same environment as other Library systems, with the result that ITS staff—not Copyright Office staff—are responsible for administering many of the security controls. Additionally, the General Counsel stated that, despite the requirement to be able to retain published works for 75 years and unpublished works for the full term of the copyright, the Copyright Office’s eCO system does not have the capability to validate the integrity of these works. Further, the Library does not have any systems that are capable of storing digital deposits for 75 years or more.

These concerns are understandable, given that service units were often not satisfied with the services provided by ITS. Accordingly, service units may believe that pursuing IT solutions and commodity IT independent of

¹³³2 U.S.C. § 166(b)(2).

ITS is their only viable alternative. Nevertheless, allowing service units to do so likely increases costs and inefficiencies.

Our research on reducing duplicative IT investments in the executive branch has found that through the Office of Management and Budget's PortfolioStat initiative—a process where agencies gather information on their IT investments and develop plans for consolidation and increased use of shared-service delivery models—agencies can avoid duplicative, wasteful, and low-value investments. Congress also recently recognized the value of these reviews when it required executive branch agencies to complete them annually.¹³⁴ However, the Library has not performed such a review. Service units' independent pursuit of IT activities presents an opportunity for the Library to both explore the costs and benefits of the existing duplicative or overlapping IT activities and identify areas for consolidating or eliminating services where appropriate.

The individual who served as the Deputy Librarian from June 2012 until December 2014 acknowledged that service units perform IT activities that are duplicative of ITS. The former Deputy Librarian also noted that one of the goals of the draft IT strategic plan that he led the development of was to use shared services to collaboratively establish IT systems that meet common requirements across organizations. The former Deputy Librarian also described actions that he took to consolidate IT management during his tenure:

- **Web Governance Board:** According to the former Deputy Librarian, in 2010, he established the Web Governance Board in order to ensure that the Library's web presence is coordinated across the service units. The Deputy Librarian chaired this board from January 2010 until December 2014. He added that, prior to the development of the board, many of the service units developed their websites independently. Additionally, the former Deputy Librarian stated that he led the development of the Library's web strategy, which identified three core areas for transforming the Library's web presence: (1) Congress, (2) National Library, and (3) Copyright. However, as previously mentioned, the Copyright Office updated its website in July 2014 independent of OSI's Web Services division.

¹³⁴Pub. L. No. 113-291, § 831; 40 U.S.C. § 11319(b).

-
- **Geospatial information systems:** The former Deputy Librarian told us that the Law Library, CRS, and Library Services previously pursued geospatial information system solutions independently.¹³⁵ However, he tasked these service units with collaboratively implementing a geospatial hosting environment that will enable Library of Congress staff and patrons, as well as Congress, to perform research and analysis using geospatial datasets acquired by the Library.
 - **Mobile devices:** According to the former Deputy Librarian, in the past, service units independently acquired cell phones for managers. He told us that in 2014, as part of a program to upgrade the Library's aging cell phones, he required the service units to acquire cell phones using one contract.

Although these activities could improve coordination and thus reduce overlap in IT activities throughout the Library, in the absence of a PortfolioStat-type assessment of the costs and benefits of consolidating IT activities, the service units will continue to spend money on IT that may not constitute an efficient use of Library resources. Until such an assessment is completed, the Library will not be able to justify whether its IT spending provides the appropriate balance of meeting business needs and saving taxpayer dollars.

Library Lacks Strong Leadership Needed to Address Its IT Management Weaknesses

Our research and experience at federal agencies indicates that agencies should have a CIO with responsibility for managing their IT—including commodity IT—and clearly define responsibilities between the CIO and officials responsible for IT management at component organizations. Congress has also recognized the need for strong CIOs, and recent legislation has reaffirmed this by strengthening the CIO position in executive branch agencies.

However, the Library does not have the leadership needed to address the IT management weaknesses identified in this report. Specifically, the Library's CIO does not have adequate responsibility for the agency's IT—in particular, authority over commodity IT and oversight of investments in

¹³⁵A geographic information system is a system of computer software, hardware, and data used to capture, store, manipulate, analyze, and graphically present a potentially wide array of geospatial information (i.e., information that describes entities or phenomena that can be referenced to specific locations relative to the earth's surface).

mission-specific systems made by other service units. Further, responsibilities and authorities of the CIO and personnel responsible for IT management at the service unit level have not been clearly defined. These challenges have been exacerbated by the fact that the Library has had five temporary CIOs since 2012 and by the recent reassignment of the Deputy Librarian, who, in the absence of a CIO, had led a number of IT efforts.

After we shared our preliminary results with the Library, the Librarian announced plans to hire a permanent CIO and Deputy CIO. According to the Chief of Staff, the Library plans to appoint these officials by September 2015. While appointing a permanent CIO could potentially address the Library's gap in IT leadership, the details of this position have yet to be fully defined. Until it establishes strong IT leadership, the Library will continue to face difficulties in addressing its numerous IT management weaknesses.

Library CIO Does Not Have Adequate Responsibility for Managing IT

According to our research and experience at federal agencies,¹³⁶ leading organizations adopt and use an enterprise-wide approach to managing IT under the leadership of a CIO that includes the following:

- **Responsibility for commodity IT:** The CIO should have the responsibility and authority, including budgetary and spending control, for commodity IT across the entity. Consolidating commodity IT under a CIO can help to reduce duplicative services and make it easier for an organization to effectively negotiate with vendors for volume discounts and improved service levels. We have previously reported that, according to CIOs, more control over component-level IT funding, including commodity IT, could help ensure greater visibility into and influence on the effective acquisition and use of IT.¹³⁷
- **Oversight of mission-specific systems:** The CIO should have the ability to adequately oversee mission-specific systems to ensure that funds being spent on component agency investments will fulfill

¹³⁶ [GAO-11-634](#).

¹³⁷ [GAO-11-634](#); see also, *Reducing Duplication and Improving Outcomes in Federal Information Technology, Before the S. Comm. on Homeland Security and Governmental Affairs*, 113th Cong. 32 (2013) (statement of David Powner, Director of IT Management Issues, U.S. Government Accountability Office).

mission needs. We previously reported on the importance of agency CIOs having adequate oversight to ensure that funds being spent on IT component agency investments, including mission-specific systems, are aligned with the needs of the organization.¹³⁸

- **Clear relationships between CIO and components:** The responsibilities and authorities governing the relationships between the CIO and component organizations should be defined. We have previously reported that the effectiveness of agency CIOs depends in large measure on having clear roles and authorities.¹³⁹

Congress has also recognized the importance of having a strong agency CIO. In 1996, Congress passed the Clinger-Cohen Act, which established the position of agency CIO for executive branch agencies and gave these officials responsibility and accountability for IT investments, including IT acquisitions, monitoring the performance of IT programs, and advising the agency head whether to continue, modify, or terminate such programs.¹⁴⁰ More recently, in December 2014, Congress enacted federal information technology acquisition reforms, which required most executive branch agencies to ensure that the CIO had a significant role in the decision process for IT budgeting, as well as the management, governance, and oversight processes related to IT.¹⁴¹ This legislation also required that CIOs review and approve (1) all contracts for IT or IT services prior to executing them and (2) the appointment of any other employee with the title of CIO, or who functions in the capacity of a CIO, for any component organization within the agency. Although these laws are not applicable to the Library, they demonstrate that Congress recognizes the importance of strong CIOs in federal agencies.

Although the Library has established a CIO position (the head of OSI), it has not provided that position with Library-wide authority and has not clearly defined the responsibilities between the CIO and the service units. Specifically:

¹³⁸[GAO-11-634](#).

¹³⁹[GAO-11-634](#).

¹⁴⁰Clinger-Cohen Act of 1996, Pub. L. No. 104-106 (Feb. 10, 1996), §§ 5122 & 5125; 40 U.S.C. § 11315 and 44 U.S.C. § 3506(a).

¹⁴¹Pub. L. No. 113-291, § 831; 40 U.S.C. § 11319(b).

-
- **Commodity IT:** The Library's CIO does not have responsibility for the Library's entire commodity IT even though a significant portion of the Library's IT funding is allocated and spent at the service unit level on commodity IT systems. As previously mentioned, each service unit has independently purchased commodity IT in the past 3 years, and, in some cases, this has led to wasteful spending.
 - **Mission-specific systems:** The Library's CIO does not have the ability to adequately oversee mission-specific systems to ensure that funds being spent on component agency investments will fulfill mission needs. As previously mentioned, although the Library has established elements of an investment management process, the ITSC, which is to be chaired by the CIO, does not review all major IT investments. Additionally, as noted previously, the former acting ITSC chair told us that ITSC approvals do not affect decisions to allocate funding for investments, as service units have already secured funding for the investments before the selection process begins. Until the Library gives its CIO adequate visibility into mission-specific systems, there is increased risk that these investments will experience significant cost and schedule overruns, with questionable mission-related achievements.
 - **Relationships between CIO and component IT leadership:** The Library has not clearly defined the responsibilities and authorities governing the relationships of the CIO and component organizations. In particular, although each service unit performs IT management activities to varying extents, the Library has not defined the relationships between the CIO and those in the service units responsible for those functions. Of particular concern is the lack of defined relationships between the Library's CIO and the other two CIO positions that exist in the Library—one at the Copyright Office and the other at CRS. Until the responsibilities and authorities governing the relationships between the Library CIO and service unit IT leadership are clearly defined, the Library CIO may not be able to effectively manage and oversee component IT spending.

Library Has Had Five Temporary CIOs in the Past 2 Years, and Deputy Librarian Who Led IT Efforts Was Recently Reassigned

Compounding the lack of CIO authority, the Library has lacked consistent leadership in this position. We have previously noted that one element that influences the likely success of an agency CIO is the length of time the individual in the position has to implement change. For example, in our prior work on agency CIOs, we reported that CIOs and former agency IT executives believed it was necessary for a CIO to stay in office for 3 to

5 years to be effective and 5 to 7 years to fully implement major change initiatives in large public sector organizations.¹⁴²

However, since the departure of the most recent permanent CIO in 2012, four individuals have served as acting CIO, and another was recently appointed to serve in an interim capacity until a permanent CIO is found. Upon the last permanent CIO's departure in June 2012, the Deputy CIO served as acting CIO until August 2013. Subsequently, three senior officials within OSI took turns serving as CIO, with the first two serving in that role for 4 months each, and the third from April 2014 to January 2015. The most recent former acting CIO noted that she was originally only assigned to serve in the position for 4 months. However, her tenure as acting CIO was extended twice: once in August 2014, when it was extended until December 2014, and again in December 2014, when it was extended until March 2015. Finally, in January 2015, a new interim CIO was appointed when the Librarian detailed the Director of the Office of Public Records and Repositories at the Copyright Office to that position until a permanent CIO is appointed.

According to the official who served as Deputy Librarian from June 2012 until December 2014, he did not advocate for hiring a CIO during his tenure for two reasons. First, he stated that the Library needed to develop an IT strategic plan before appointing a permanent CIO in order to provide that individual with priorities. Second, the former Deputy Librarian explained that he did not want to hire a CIO to oversee, among other things, the IT activities performed by CRS and the Copyright Office, when he had not been empowered by the Librarian with the authority to manage these offices' IT activities.

In the absence of a CIO, the former Deputy Librarian managed many of the Library's recent IT efforts. For example, as previously mentioned, the former Deputy Librarian (1) drafted an IT strategic plan, (2) chaired the Web Governance Board, and (3) led the Library's efforts to consolidate mobile phone contracts and geospatial information systems.

However, in December 2014, the Librarian reassigned the individual serving as Deputy Librarian to be a senior advisor to the Librarian.

¹⁴²GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, [GAO-04-823](#) (Washington, D.C.: July 21, 2004).

Subsequently, in January 2015, the Librarian appointed the Law Librarian to be the new Deputy Librarian.

After we shared the preliminary results of our review with the Library in January 2015, the Librarian announced plans to hire a permanent CIO and deputy CIO; according to the Chief of Staff, the Library plans to do so by September 2015. While this search is conducted, the interim CIO will be responsible for drafting the Library's IT strategic plan, chairing the Web Governance Board, and leading the Library's efforts to consolidate mobile phone contracts and geospatial information systems. Although appointing a permanent CIO could potentially address the Library's gap in IT leadership, the details of this position have yet to be fully defined. If the Library hires a permanent CIO with responsibility for IT, sufficient authority, and clearly defined responsibilities, it will be better positioned to effectively acquire, operate, and maintain its IT in support of its mission.

Conclusions

As information is increasingly created, shared, and preserved digitally, effectively managing its IT resources will be even more critical for the Library to carry out its mission of preserving and making available the knowledge and creative output of the American people. To its credit, although not required to do so, the Library has embraced standards and practices set forth in laws that require executive branch agencies to develop processes for investment management, information security, and privacy. However, widespread weaknesses in implementing these processes and several other IT management disciplines call into question whether the Library is well positioned to meet the challenges of making the most efficient and productive use of its technology resources. Just as important, the Library's lack of strong, consistent leadership in these areas has hampered its ability to make needed improvements in the face of long-standing challenges.

Specifically, without an up-to-date IT strategic plan that is linked to the overall agency strategic plan and includes goals, performance measures, strategies, and interdependencies among projects, the Library will lack a clear definition of what it wants to accomplish with IT and strategies for achieving those results. This challenge is compounded by the lack of a complete and reliable enterprise architecture that accurately captures the Library's current IT environment, describes its target environment, and outlines a strategy for transitioning from one to the other. Additionally, the Library will be hindered in carrying out an IT strategy without an organization-wide assessment of its human capital needs, and plans for addressing any gaps.

Further impeding the Library's ability to make strategic decisions is an incompletely implemented process for managing the selection and oversight of its IT investments. Specifically, the lack of clearly defined roles and responsibilities and other gaps in policies have resulted in an inconsistent approach to reviewing and selecting investments for the Library's portfolio. As a result, there is less assurance that proposed investments are receiving adequate scrutiny and that the Library is expending its resources on the appropriate mix of systems that will effectively and efficiently meet its needs. Moreover, by not applying adequate oversight to investments that have already been selected, the Library is not in a position to ensure that they are meeting cost, schedule, and performance goals and delivering the capabilities the agency needs to carry out its mission. More basically, because the Library does not have accurate data on what it spends on IT each year or an accurate inventory of IT assets, it is limited in its ability to make informed investment decisions or ensure that it does not waste money on IT.

Concerns about the Library's ability to acquire IT systems that meet its needs are further raised by the absence of organization-wide policies to ensure that its systems acquisition process follows disciplined practices in the areas of risk management, requirements development, cost estimating, and schedule development. The lack of such policies has led to the incomplete implementation of these practices among the investments we reviewed. Without following such key practices, the Library will be challenged in ensuring that systems are delivered on time and within budget and that they deliver the capabilities needed by its users.

Another significant area of concern is the Library's inconsistent implementation of agency-wide information security and privacy programs. While, to its credit, the Library has established roles and responsibilities and policies and procedures for information security and privacy, significant weaknesses in implementing key security management controls call into serious question whether the information and systems at the Library are being adequately protected. These weaknesses, in areas such as documenting security controls, conducting security testing, developing remedial action plans, establishing contingency plans, carrying out security training, ensuring that contracts address security requirements, and assessing risks to privacy, could provide opportunities for either intentional or inadvertent compromise of the Library's systems, resulting in unauthorized access, modification, or loss of sensitive information, or disruption to the Library's operations. These issues are further highlighted by a number of weaknesses we

found in technical security controls that are intended to limit unauthorized access to the Library's systems and ensure their integrity.

While ITS—as the central IT organization within the Library—is responsible for providing IT-related services to the Library's other units, the lack of satisfaction with these services has contributed to the other units pursuing their own IT activities, potentially resulting in duplicative investments and wasted resources. Although the reasons units provided for managing much of their IT independently are understandable given inconsistent satisfaction with the services provided by ITS, allowing service units to do so likely increases costs and inefficiencies. Without a plan for improving the units' satisfaction with ITS services and an organization-wide evaluation of the costs and benefits of the Library's fragmented approach to carrying out IT activities, the agency may be missing opportunities to eliminate duplication, improve the efficiency of its delivery of IT services, and save taxpayer dollars.

Key to all these shortcomings, the Library has lacked consistent, effective leadership for its IT efforts. Because the Library's CIO position lacks adequate authority and oversight, the agency has diminished assurance that investments in IT are being coordinated organization-wide and that they provide an appropriate mix of capabilities that support the Library's mission while avoiding unnecessary duplication.

The Library's intention to appoint a permanent CIO is a positive development, but it will be important to clearly define this position and ensure that this official has sufficient authority to address the many challenges facing the Library's IT management. If it follows through on plans to appoint such an official and invests the position with the appropriate authority, the Library will be in a stronger position to address the IT management challenges we have identified and make a more effective and efficient use of technology to support its mission.

Recommendations

To provide stable, consistent, and effective leadership for addressing the weaknesses identified in this report, as well as for improving the organization's management of IT, we recommend that the Librarian expeditiously hire a permanent chief information officer responsible for managing the Library's IT and ensure that this official has clearly defined responsibilities and adequate authority, consistent with the role of a chief information officer as defined by best practices. This should include, among other things, (1) responsibility for commodity IT; (2) oversight of mission-specific systems, through the ITSC or another oversight

mechanism; and (3) clarification of responsibilities and authorities between the Library CIO and service unit IT leadership.

To provide strategic direction for the Library's use of its IT resources, we recommend that the Librarian of Congress take the following 3 actions:

- Complete an IT strategic plan within the time frame the Library has established for doing so. The plan, at a minimum, should (1) align with the agency's overall strategic plan, (2) provide results-oriented goals and performance measures, (3) identify the strategies for achieving the desired results, and (4) describe interdependencies among projects.
- Establish a time frame for developing a complete and reliable enterprise architecture that accurately captures the Library's current IT environment, describes its target environment, and outlines a strategy for transitioning from one to the other, and develop the architecture within the established time frame.
- Establish a time frame for implementing a Library-wide assessment of IT human capital needs and complete the assessment within the established time frame. This assessment should, at a minimum, analyze any gaps between current skills and future needs, and include a strategy for closing any identified gaps.

To provide a framework for effective IT investment management and ensure that the Library has accurate information to support its decisions, we recommend that the Librarian take the following 10 actions:

- Clarify investment management policy to identify which governance bodies are responsible for making investment decisions, and under what conditions.
- Establish and implement a process for linking IT strategic planning, enterprise architecture, and IT investment management.
- Establish and implement policies and procedures for reselecting investments that are already operational.
- Establish and implement policies and procedures for ensuring that investment selection decisions have an impact on decisions to fund investments.

-
- Ensure that appropriate governance bodies review all investments that meet defined criteria.
 - Require investments in development to submit complete investment data (i.e., cost and schedule variances and risk management data) in quarterly reports submitted to the ITSC.
 - Fully establish and implement policies, to include guidance for service units on classifying expenditures as IT, for maintaining a full accounting of the Library's IT-related expenditures.
 - Fully establish and implement policies for developing a comprehensive inventory of IT assets.
 - Implement policies and procedures for conducting post-implementation reviews of investments.
 - Fully establish and implement policies and procedures consistent with the key practices on portfolio management, including (1) defining the portfolio criteria, (2) creating the portfolio, and (3) evaluating the portfolio.

To effectively plan and manage its acquisitions of IT systems and increase the likelihood of delivering promised system capabilities on time and within budget, we recommend that the Librarian take the following 4 actions:

- Complete and implement an organization-wide policy for risk management that includes key practices as discussed in this report, and within the time frame the Library established for doing so.
- Establish and implement an organization-wide policy for requirements development that includes key practices as discussed in this report.
- Establish and implement an organization-wide policy for developing cost estimates that includes key practices as discussed in this report.
- Establish a time frame for finalizing and implementing an organization-wide policy for developing and maintaining project schedules that includes key practices as discussed in this report, and finalize and implement the policy within the established time frame.

To better protect IT systems and reduce the risk that the information they contain will be compromised, we recommend that the Librarian take the following 10 actions:

- Develop a complete and accurate inventory of the agency's information systems.
- Revise information security policy to require system security plans to describe common controls, and implement the policy.
- Ensure that all system security plans are complete, including descriptions of how security controls are implemented and justifications for why controls are not applied.
- Conduct comprehensive and effective security testing for all systems within the time frames called for by Library policy, to include assessing security controls that are inherited from the Library's information security program.
- Ensure that remedial action plans for identified security weaknesses are consistently documented, tracked, and completed in a timely manner.
- Finalize and implement guidance on continuous monitoring to ensure that officials are informed when making authorization decisions about the risks associated with the operations of the Library's systems.
- Develop contingency plans for all systems that address key elements.
- Establish and implement a process for comprehensively identifying and tracking whether all personnel with access to Library systems have taken required security and privacy training.
- Establish a time frame for finalizing and implementing the Library's standard contract sections for information security and privacy requirements, and finalize and implement the requirements within that time frame.
- Require the chief privacy officer to establish and implement a process for reviewing the Library's privacy program, to include ensuring that privacy impact assessments are conducted for all information systems.

To help ensure that services provided by ITS meet the needs of the Library's service units, we recommend that the Librarian take the following 2 actions:

- Finalize and implement a Library-wide policy for developing service-level agreements that (1) includes service-level targets for agreements with individual service units and (2) covers services in a way that best meets the need of both ITS and its customers, including individual service units.
- Document and execute a plan for improving customer satisfaction with ITS services that includes prioritized improvement projects and associated resource requirements, schedules, and measurable goals and outcomes.

In addition, to help ensure an efficient and effective allocation of the agency's IT resources, we recommend that the Librarian take the following action:

- Conduct a review of the Library's IT portfolio to identify duplicative or overlapping activities and investments, including those identified in our report, and assess the costs and benefits of consolidating identified IT activities and investments.

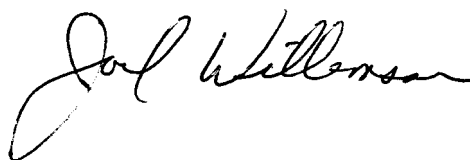
In a subsequent report with limited distribution, we will also be making a number of recommendations to address weaknesses we identified in technical security controls at the Library.

Agency Comments and Our Evaluation

We provided a draft of this product to the Library of Congress for comment. In his written comments, reproduced in appendix II, the Librarian stated that he generally concurred with our recommendations. In this regard, he described ongoing and planned actions to address them, and provided milestones for completing these actions. If effectively implemented, these actions should help address the weaknesses we identified. The Library also provided technical comments that were incorporated, as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Librarian of Congress, and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-6253 or willemsenj@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.

A handwritten signature in black ink, reading "Joel Willemssen". The signature is fluid and cursive, with the first name "Joel" being more prominent and the last name "Willemssen" following in a similar style.

Joel C. Willemssen
Managing Director, Information Technology

Appendix I: Objectives, Scope, and Methodology

The House Appropriations Committee report accompanying the fiscal year 2015 legislative branch appropriations bill required GAO to review the Library of Congress's management of information technology (IT). Our specific objectives for this review were to assess the extent to which the Library of Congress (1) addressed in its strategic planning the IT and related resources required to meet its goals and objectives; (2) established an IT governance structure to manage the selection, control, and evaluation of IT investments; (3) used IT acquisition and development best practices; (4) established programs for ensuring the information security and privacy protection of its information and information systems; (5) used best practices for managing IT services; and (6) has a chief information officer (CIO) with authority to exercise control and oversight of IT management functions.

To address our first objective, we reviewed the agency's overall strategic plan, and evaluated its draft IT-specific strategic plan against key practices for IT strategic planning that we have previously identified.¹ Those best practices include developing an IT strategic plan that

- aligns with the agency's overall strategic plan,
- provides results-oriented goals and performance measures that permit it to determine whether it is succeeding,
- identifies the strategies it will use to achieve desired results, and
- describes interdependencies within and across projects so that these can be understood and managed.

Additionally, because an enterprise architecture can help an organization determine how it can most effectively execute its IT strategic plan, we evaluated the agency's enterprise architecture documentation against key practices identified in our enterprise architecture framework² to determine the extent to which the Library had established a well-defined enterprise architecture, as well as demonstrated institutional commitment to its architecture. Those practices include

¹GAO, *Social Security Administration: Improved Planning and Performance Measures Are Needed to Help Ensure Successful Technology Modernization*, [GAO-12-495](#) (Washington, D.C.: Apr. 26, 2012).

²GAO, *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0)* (Supersedes [GAO-03-584G](#)), [GAO-10-846G](#) (Washington, D.C.: August 2010).

- developing an architecture that thoroughly describes the current and target states of an organization's IT systems and business operations and identifies the gaps and specific intermediary steps that the organization plans to take to achieve its target state;
- developing an organizational policy for enterprise architecture; and
- establishing an executive committee representing the enterprise that is responsible and accountable for enterprise architecture.

Further, because of the importance of sustaining an IT workforce with the necessary skills to execute an agency's strategic plan, we obtained and reviewed the Library's human capital plan.³ We compared this plan to best practices we have identified in human capital management.⁴ Those practices include

- analyzing the gaps between current skills and future needs and
- developing strategies for filling the gaps.

We also interviewed the enterprise architect, architecture review board chair, Director of the Information Technology Services (ITS) directorate, former acting Chief Information Officer (CIO), former Deputy Librarian, and Librarian of Congress to obtain information about the Library's IT strategic planning activities.

In addressing our second objective, we compared agency documentation against critical processes associated with Stages 2 and 3 of GAO's information technology investment management framework.⁵ Stage 2 of the framework includes the following key processes:

- instituting the investment board,

³Library of Congress, *Human Capital Management Plan* (December 2010).

⁴GAO, *A Model of Strategic Human Capital Management*, [GAO-02-373SP](#) (Washington, D.C.: Mar. 15, 2002); *Human Capital: Key Principles for Effective Strategic Workforce Planning*, [GAO-04-39](#) (Washington, D.C.: Dec. 11, 2003); and *Information Technology: FDA Needs to Establish Key Plans and Processes for Guiding Systems Modernization Efforts*, [GAO-09-523](#) (Washington, D.C.: June 2, 2009).

⁵GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity (Supersedes AIMD-10.1.23)*, [GAO-04-394G](#) (Washington, D.C.: March 2004).

- selecting investments that meet business needs,⁶
- providing investment oversight, and
- capturing investment information.

Stage 3 includes the following critical processes:

- defining the portfolio criteria,
- creating the portfolio,
- evaluating the portfolio, and
- conducting post-implementation reviews.

Specifically, we reviewed written policies, procedures, guidance, and other documentation that provided evidence of establishing commitment to critical processes, such as *Library of Congress Regulation 1600: Information Resource Management Policy and Responsibilities*; the *Library of Congress Information Resource Management Plan*; the IT Steering Committee charter; and guidance and templates for the selection process, development stage oversight, and the post-implementation review process. We also reviewed IT Steering Committee meeting minutes to determine whether the committee was successfully implementing its documented policies and procedures, as well as for evidence of its decision-making processes. In addition, we reviewed data from the system used by Integrated Support Services to track and manage the Library's assets, including those relating to IT.

Additionally, we selected three investments as case studies to determine the extent to which key activities associated with the critical processes were being carried out. To choose these investments, we identified the 16 investments that the IT Steering Committee was overseeing or considering for review as of July 2014. To narrow this list, we excluded investments that (1) were in the planning stages, (2) had been completed, or (3) would be fully deployed prior to the completion of our review. We then selected the one investment that was managed by more than one service unit: Library Services and the Office of Strategic Initiatives' (OSI) Twitter Research Access investment. We then selected two investments

⁶Stage 2 also includes a critical process referred to as "meeting business needs." This process includes developing a business case that identifies the key executive sponsor and business customers (or end users) and the business needs that the IT project will support. We addressed the key practices associated with this process as part of our review of the critical processes "selecting an investment that meets business needs" and "providing investment oversight."

sponsored by service units other than Library Services and OSI to ensure coverage of other service units. These additional two investments were the Office of Support Operations' (OSO) Facility Asset Management Enterprise (FAME) investment and the Office of the Librarian's Momentum Upgrade and Migration investment.

For these three investments, we reviewed evidence of the implementation of project-level IT investment management processes, including investment concept proposals, investment charters, development stage quarterly reports, budget plans, and an IT Steering Committee scoring worksheet that evaluated risk factors along with the significance of potential benefits. Further, we conducted interviews with officials responsible for managing the selected investments, including the Library's investment management portfolio officer, former acting IT Steering Committee chair, and former acting CIO.

We did not assess progress in establishing the capabilities found in Stages 4 and 5 because the Library has not yet implemented Stage 3 processes.

In addition, because the Library had not established and implemented a process for tracking IT spending, we developed an estimate of how much it spent on IT during fiscal year 2014 using data from the Library's accounting and human resources systems. With respect to IT equipment and services captured in the Library's accounting system, we identified budget object class codes (i.e., codes used by the Library to classify spending) associated with IT. To do so, we performed the following three steps:

- First, we asked the Office of the Chief Financial Officer to identify budget object classification codes that, based on the executive branch definition of IT,⁷ were associated with IT. The Library identified 16 codes associated with IT.
- Second, we identified budget object classification codes that are consistent with the Technical Reference Model in OMB's Federal Enterprise Architecture Reference Model.⁸ We identified an additional 26 codes.
- Third, we shared the additional 26 budget object classification codes with the Library Office of the Chief Financial Officer, the National Library Service for the Blind and Physically Handicapped (NLS), and ITS to review, comment, and provide additional information. Based on their comments, we removed 16 codes from our review and added 1 code.

As a result, we identified 27 budget object classification codes that were associated with IT, 4 of which were associated with both IT and non-IT spending. We then asked the Library to provide us with detailed information for all obligations it made in fiscal year 2014 that were associated with these codes. For the 4 codes that were used to classify both IT and non-IT spending, we identified the obligations classified under these codes that were greater than \$2,500.⁹ For these selected obligations, we asked the service units to identify, based on the executive branch definition of IT, obligations associated with IT. We then added

⁷The Clinger-Cohen Act of 1996, as amended, defines IT as follows: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency, if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires the use of that equipment. It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. 40 U.S.C. § 11101(6).

⁸Executive Office of the President, OMB, *FEA Consolidated Reference Model Document*, Version 2.3 (October 2007).

⁹Regarding services, Library policy states that the maximum amount that can be purchased using a government purchase card is \$2,500.

these obligations to those associated with the other 23 codes to complete our estimate of the Library's IT equipment and services.

Regarding the data in the Library's human resource system, we obtained from the Library's Human Resources division (1) the number of Library staff employed under IT-related job series during fiscal year 2014 and (2) the salary information, in aggregate form, for those employees during that fiscal year. We then added this information to our estimate of the Library's IT equipment and services. We used this combined figure as our estimate of the Library's IT spending for fiscal year 2014. We then shared our estimate with each service unit to review, comment, and provide additional information.

To determine the reliability of the IT spending data, we reviewed Office of the Chief Financial Officer documentation and previous Office of the Inspector General Reports on the Library's financial statements, and interviewed Office of the Chief Financial Officer officials familiar with the financial system to understand the controls used on to create and classify obligations. We determined that the data were sufficiently reliable for our purpose, which was to provide an estimate of the Library's IT spending; however, the estimate does not reflect all of the Library's IT spending. For example, the Library has not defined IT and has not fully established guidance on how to classify IT expenses in its financial accounting system, Momentum. Although Library guidance identifies 5 budget object classification codes as being associated with IT, as noted, we identified additional codes that are used for IT transactions. Additionally, the Library did not ensure that all IT-related transactions were properly associated with IT-related codes. For example, OSI associated about \$2.5 million of its IT budget with a code that, according to Library guidance, excludes IT spending.

Further, as discussed previously, our estimate does not reflect obligations of \$2,500 or less that are associated with 4 budget object classification codes for which the Library made both IT and non-IT obligations. In addition, our estimate does not include salary information for all staff that perform key IT activities. In response to our request for the salary information for all staff whose primary job responsibility is IT, the Assistant Director of Human Resources Services provided information on employees whose job title related to the information technology management series (2210). However, a Copyright budget analyst and the Library's Chief Financial Officer stated that the Library has employees that perform key IT activities, but whose job titles fall outside of the information technology management series.

To determine the reliability of the cost estimates for the investments reviewed by the Library's IT Steering Committee, we (1) performed testing for obvious errors in accuracy and completeness, and (2) interviewed officials knowledgeable about the template used to produce the estimates. Additionally, as discussed in more detail below, we also assessed the extent to which the estimates were created using leading practices consistent with a comprehensive estimate, as identified in GAO's *Cost Estimating and Assessment Guide*.¹⁰ However, none of the investments' estimates fully met the comprehensive characteristic. Despite this limitation, we believe that the cost data are sufficiently reliable for our purpose—that is, as an indicator of the general range of the portion of the Library's IT spending that is reviewed by the ITSC.

To address the third objective, we compared Library policies and procedures in key IT acquisition management areas—risk management, requirements development, cost estimating, and scheduling—to leading practices identified by industry and GAO. We also determined the extent to which the three selected investments identified above were implementing these key IT acquisition practices. Specifically, with respect to risk management and requirements development, we reviewed policies and procedures developed by ITS, as well as acquisition documentation from the three selected investments, and compared them to risk management and requirements development best practices identified by the Software Engineering Institute's (SEI) Capability Maturity Model® Integration for Acquisition (CMMI-ACQ).¹¹

The key risk management practices were

- developing a risk management strategy;
- identifying and documenting risks;
- evaluating, categorizing, and prioritizing risks;
- developing risk mitigation plans; and
- monitoring the status of each risk periodically, and implementing the risk mitigation plans as appropriate.

¹⁰GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, [GAO-09-3SP](#) (Washington, D.C.: March 2009); SEI, *Capability Maturity Model® Integration for Acquisition (CMMI-ACQ)*, Version 1.3 (November 2010);

¹¹SEI, *Capability Maturity Model® Integration for Acquisition (CMMI-ACQ)*, Version 1.3 (November 2010).

The key requirements development practices were

- eliciting stakeholder needs,
- developing customer requirements, and
- prioritizing customer requirements.

We analyzed investment risk documentation, including risks identified in investment charters, acquisition plans, and risk registers; risk mitigation plans; and quarterly performance reports submitted to the IT Steering Committee. Additionally, we assessed investment requirements development documentation, such as requirements obtained from customers and other stakeholders, and a system gap analysis. Further, we interviewed officials responsible for managing the investments to obtain additional information about their risks, requirements, and practices for managing them. We shared our analysis with Library officials to review, comment, and provide additional information, and we adjusted our analysis where appropriate.

With regard to cost estimating, we reviewed policies and procedures developed by ITS, as well as cost estimating documentation from the three selected investments, and compared them to leading practices set forth in GAO's *Cost Estimating and Assessment Guide*.¹² This guide identifies 12 leading practices that represent work across the federal government and are the basis for a high-quality, reliable cost estimate. An estimate created using the leading practices exhibits four broad characteristics: it is *accurate*, *well documented*, *credible*, and *comprehensive*. Each of these characteristics is associated with a specific set of leading practices, which in turn are made up of a number of specific tasks. We assessed ITS's guidance against each of the four characteristics. Each characteristic was assessed as either being fully met—the Library provided complete evidence that satisfies the associated tasks of the leading practices; substantially met—the Library provided evidence that satisfies a large portion of the associated tasks of the leading practices; partially met—the Library provided evidence that satisfies about half of the associated tasks of the leading practices; minimally met—the Library provided evidence that satisfies a small portion of the associated tasks of the leading practices; or not met—the

¹²[GAO-09-3SP](#).

Library did not provide evidence that satisfies any of the associated tasks of the leading practices.

In assessing the reliability of the estimates developed by the three selected investments, we only assessed practices associated with the *comprehensive* characteristic. We did so because none of the investments' estimates fully met the *comprehensive* characteristic, and this characteristic must be completed in order for the estimate to fully address the other three characteristics. We assessed these estimates using the same scoring methodology (i.e., fully met, substantially met, partially met, minimally met, and not met) as described above for the review of ITS's cost estimating policies and procedures. We shared our analysis with Library officials to review, comment, and provide additional information.

Finally, regarding our assessment of the Library's scheduling, we reviewed policies and procedures developed by ITS, as well as scheduling documentation from the selected investments, and compared them to leading practices set forth in the exposure draft of GAO's *Schedule Assessment Guide*.¹³ This guide defines 10 leading practices that are vital to having integrated and reliable master schedules. Similar to a well-developed cost estimate, a schedule created using the leading practices exhibits four broad characteristics: it is *comprehensive*, *well-constructed*, *credible*, and *controlled*. Each characteristic is associated with a specific set of leading practices, which, in turn, are made up of a number of specific tasks. We assessed ITS's guidance against each of the four characteristics.

In assessing the reliability of the schedules developed by the selected investments, we only assessed practices associated with the *well-constructed* characteristic. We did so because none of the schedules substantially addressed the practices associated with this characteristic, and because this characteristic relates to the foundational practices for a high-quality, reliable schedule. We assessed ITS's policies and procedures, as well as the investment schedules using the same methodology (i.e., fully met, substantially met, partially met, minimally met, and not met) as previously described for our assessment of ITS's

¹³GAO, *GAO Schedule Assessment Guide: Best Practices for Project Schedules—Exposure Draft*, [GAO-12-120G](#) (Washington, D.C.: May 2012).

cost estimating policies and procedures. We shared our analysis with Library officials to review, comment, and provide additional information, and we adjusted our analysis where appropriate.

To address our fourth objective, we reviewed relevant information security and privacy laws and guidance, including National Institute of Standards and Technology (NIST) standards and guidance, to identify federal security and privacy control guidelines. We then reviewed the Library's security and privacy policies and procedures to determine their consistency with these guidelines.

Additionally, we selected nine Library systems as case studies to determine the extent to which NIST guidelines and Library policy were being implemented. We chose these systems by following these six steps:

- First, using lists of systems developed by the Chief Information Security Officer (CISO), the Copyright Office, and Library Services as the basis for our selected systems, we separated the systems into eight groups—each of the seven service units, as well as NLS.¹⁴ With two exceptions—Law Library and OSI (both of which are discussed later in this section)—we only selected one system from each group.
- Second, in order to narrow the list of systems, we excluded those with a “low” Federal Information Processing Standards (FIPS) 199¹⁵ impact level.¹⁶ Because the Law Library only had one system, which was labeled as having a “low” FIPS 199 impact level, we did not select any systems from this service unit.

¹⁴Although NLS is not a service unit (it is part of Library Services), we included it as one of the eight groups because—other than the Copyright Office and CRS—it is the only Library unit that receives its own appropriations.

¹⁵NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004).

¹⁶FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security: low, moderate, and high. According to FIPS 199, systems are to be classified as “low” when the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. In contrast, systems are to be classified as “moderate” or “high” if the loss of confidentiality, integrity, or availability could be expected to have a serious (moderate) or severe/catastrophic (high) adverse effect on organizational operations, organizational assets, or individuals.

- Third, we selected the Library's "tier 0 systems"—that is, general support systems use to support critical IT systems that need to be restored before any other systems in the event of a disaster. The three tier 0 systems are the ITS Application Hosting Environment, ITS Library of Congress Data Network, and ITS Library of Congress Office Automation System.
- Fourth, we identified the Library's other general support systems and selected the Congressional Research Service's (CRS) general support system that also processes personally identifiable information—the Enterprise Infrastructure General Support System—as well as the Office of Security and Emergency Preparedness (OSEP) general support system that is classified as having a "high" FIPS 199 impact level—the OSEP Physical Security Network.
- Fifth, for groups without an associated system, we identified the Library's "tier 1" systems (i.e., systems that are to be restored within 24 hours in the event of a disaster). We identified four systems: Copyright's eCO system, the Office of the Librarian's Momentum system, Library Services' Federal Library and Information Network (FEDLINK) Customer Account Management System, and Library Services' System Management Information network (SYMIN) II. From these, we selected Copyright's eCO system and the Office of the Librarian's Momentum system. For Library Services, we randomly selected SYMIN II from the two systems.
- Finally, because NLS did not have any general support systems or tier 1 systems, we identified NLS systems with a moderate FIPS 199 impact level and randomly selected the NLS Production Information Control System/NLS Integrated Operations Support System (PICS/NIOSS).

In summary, this selection process resulted in the following nine systems:

- ITS Application Hosting Environment,
- ITS Library of Congress Data Network,
- ITS Library of Congress Office Automation System,
- CRS Enterprise Infrastructure General Support System,
- OSEP Physical Security Network,
- eCO,
- OFCO Momentum,
- SYMIN II, and
- PICS/NIOSS.

Using NIST guidelines for an effective agency-wide information security program, we evaluated the Library's information security program in the following areas:

- **Incident handling:** We compared the Library's incident handling procedures to NIST guidance on the key steps that agencies should take when responding to incidents.¹⁷ To determine the effectiveness of the Library's response to incidents, we selected 22 incidents to review as case studies. To choose the incidents, we obtained a list of all incidents reported between October 1, 2013, and September 2, 2014. In order to narrow the list of incidents, we removed (1) incidents for which the Library determined that the incident did not require investigation or was a false positive and (2) incidents with a status of open or canceled. We then separated the remaining incidents into eight groups—each of the categories that the Library uses to classify incidents.¹⁸ With the exception of one category—recon activity—we randomly selected 3 incidents from each category. For the recon category, we selected its 1 incident for our review. For these selected incidents, we reviewed documents from the Library's incident tracking system to determine the extent to which the Library had performed analysis, containment, eradication, recovery, reporting, and post-incident procedures in accordance with NIST guidance. To verify the reliability of the data in the agency's incident handling system, we examined it for obvious outliers, omissions, and errors. We determined that these data were sufficient for our purposes, which was to select incidents to use as case studies and determine the extent to which the Library handled those incidents consistent with NIST guidance.

¹⁷NIST, *Computer Security Incident Handling Guide*, Special Publication (SP) 800-61, Revision 2 (Gaithersburg, Md.: August 2012).

¹⁸The eight categories are (1) unauthorized access, (2) denial of service/distributed denial of service, (3) malicious code, (4) multiple components (e.g., possible loss of personally identifiable information or sensitive information or removal of Library links from Internet search engines), (5) recon activity, (6) unsolicited communication, (7) inappropriate usage (e.g., unauthorized software or violation of appropriate Internet usage policy), and (8) other (e.g., request to the Library's Security Operation's Center for information or assistance).

- **Inventory of systems:** We assessed the Library's policy for its system inventory against relevant NIST guidelines.¹⁹ To determine the comprehensiveness and accuracy of the Library's system inventory, we compared the inventory provided to us by the Library's CISO with a separate list provided by Library Services. We also asked the CISO and officials from each service unit to verify the accuracy and completeness of these lists. Although we determined the inventory was not complete and accurate, we believe that the system lists collectively, with lists of tier 0, tier 1, and general support systems, are sufficiently reliable for our purpose—that is, to select systems as case studies for our review.
- **System security plans:** We compared Library policy on system security plans with relevant NIST guidance.²⁰ Additionally, we assessed system security plans for the nine selected systems against the NIST guidelines.
- **Security test and evaluation:** We assessed Library policy on security testing against relevant NIST guidelines.²¹ In addition, we compared testing documentation for the nine selected systems against the NIST guidance and Library policy.
- **Remedial action plans:** We compared Library policy on plans of action and milestones (POA&M) with relevant NIST guidance.²² Additionally, we reviewed POA&Ms for the nine selected systems and, for eight of the systems, identified the number of POA&M items that were delayed, as of December 2014. Regarding the OSEP Physical Security Network, OSEP had not reported any updates to its POA&M items since September 2013; we identified the number of items that were open as of that date, when the items were originally reported. To verify the reliability of the agency's POA&M data, we examined them for obvious outliers and errors. Excluding the data for the OSEP

¹⁹NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

²⁰NIST, *Guide for Developing Security Plans for Federal Information Systems*, SP 800-18, Revision 1 (Gaithersburg, Md.: February, 2006).

²¹NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (Gaithersburg, Md. February 2010).

²²NIST, SP 800-53, Rev. 4.

Physical Security Network, which had not been updated since September 2013, we determined that the POA&M data were sufficient for our purpose, which was to identify the number of items with a status of “delayed.”

- **Authorization to operate:** We assessed Library policy on authorization to operate against relevant NIST guidelines.²³ We also assessed the extent to which the Library completed authorizations to operate for the nine selected systems. In instances where the authorizations had not been completed, we interviewed Library officials responsible for the systems and, where relevant, reviewed documentation in which the Library, for a defined period of time, waived the requirement to authorize the system to operate.
- **Contingency planning:** We compared Library policy on contingency planning with relevant NIST guidance.²⁴ In addition, we determined the extent to which the Library developed contingency plans for the nine selected systems, as called for by NIST guidance and Library policy.
- **Security and privacy awareness training:** We assessed Library policy on security and privacy training against relevant NIST guidance.²⁵ Additionally, we obtained the lists of users identified in three systems: ITS Library of Congress Office Automation System, CRS Enterprise Infrastructure General Support System, and OSEP Physical Security Network. We did so because these were the three systems in our sample for which the Library maintains instances of the Library’s primary service for authenticating and authorizing users. We then compared these lists with the list of users the Library reported as having completed the security and privacy awareness training in fiscal year 2014. We shared our analysis with Library officials to review, comment, and provide additional information.
- **Contract requirements for information security:** We compared Library policy on contract requirements for information security with

²³NIST, SP 800-37, Rev. 1.

²⁴NIST, SP 800-18, Rev. 1.

²⁵NIST, SP 800-53, Rev. 4.

relevant NIST guidance.²⁶ In addition, we determined the extent to which the contracts supporting the nine selected systems included the contract requirements called for by Library policy and NIST guidance.

To evaluate the Library's controls over its information systems, we used our *Federal Information System Controls Audit Manual*,²⁷ which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information. We also used NIST standards and guidelines²⁸ and Library policies, procedures, practices, and standards. Specifically, we reviewed controls in the following areas:

- **Authorization:** For all users with elevated privileges to the selected nine systems, we reviewed the extent to which those users had been authorized to use the system with those elevated permissions, consistent with NIST guidance.²⁹
- **Identification and authentication:** With respect to the selected systems, we assessed controls used to authenticate and authorize users against NIST guidance.³⁰
- **Cryptography:** We observed configurations for providing secure data transmissions across the network to determine whether sensitive data were being encrypted consistent with NIST guidance.³¹

Background investigations: We identified all users with elevated privileges to the selected nine systems and then asked the Library's personnel security officer whether the Library had performed a background investigation for each, consistent with NIST guidance³² and Library policy.

²⁶NIST, SP 800-53, Rev. 4.

²⁷GAO, *Auditing and Financial Management: Federal Information System Controls Audit Manual (FISCAM)*, [GAO-09-232G](#) (Washington, D.C.: February 2009).

²⁸NIST SP 800-53, Rev. 4.

²⁹NIST, SP 800-53, Rev. 4.

³⁰NIST, SP 800-53, Rev. 4.

³¹NIST, SP 800-53, Rev. 4.

³²NIST, SP 800-53, Rev. 4.

- **Physical security and environmental safety:** We identified four Library facilities in the United States that include an IT data center: (1) the James Madison Building on Capitol Hill; (2) the NLS facility in northwest Washington, D.C.; (3) the Packard Campus of the National Audio-Visual Conservation Center in Culpepper, Virginia; and (4) the Library's alternate computing facility in Manassas, Virginia. We visited each of these facilities and assessed the physical security and environmental controls supporting their data centers against relevant NIST guidance.³³ Additionally, because the Library did not have an accurate inventory of its non-capitalized IT assets, we also visited the Library's warehouse in Landover, Maryland, and assessed the physical security and environmental controls supporting this facility.

To address our fifth objective, we evaluated ITS's service management documentation against leading industry practices for managing IT services identified in the Information Technology Infrastructure Library.³⁴ We evaluated the service management practices of ITS, which functions as the Library's central IT organization and is the primary provider to each service unit throughout the Library. The service management practices were

- developing a service catalog;
- defining how service-level agreements (SLA) should be structured so that IT services and customers are covered in a manner best suited to the organization's needs; and
- establishing SLAs consistent with that structure that describe the IT services, specify roles and responsibilities of both parties, and document service level targets.

Specifically, we reviewed ITS's service catalog and SLAs between ITS and its customers. We also we conducted interviews with officials responsible for managing ITS's services, including the Director of ITS, and the ITS Assistant Director for Operations.

Additionally, we assessed ITS's customer satisfaction improvement efforts against a practice identified by the Software Engineering Institute's

³³NIST, SP 800-53, Rev. 4.

³⁴Lou Hunnebeck and Colin Rudd, *ITIL: Service Design* © (London: The Stationary Office, 2011). The guide is available at: <http://www.axelos.com/Publications-Library/IT-Service-Management-ITIL/>.

IDEALSM—namely, establishing a written plan that serves as the basis for guiding its improvement activities. Because the Library did not have comprehensive metrics for the satisfaction with ITS’s services, we conducted a web-based survey of ITS customers. We designed a draft questionnaire in close collaboration with our survey specialist. We also conducted pretests with four officials: one official representing the largest service unit (Library Services), one official representing the smallest service unit (Law Library), the Director of ITS, and the former acting CIO. From these pretests, we made revisions as necessary to reduce the likelihood of overall and item non-response as well as reporting errors on our questions.

We sent the survey via e-mail to the head of each service unit, as well as the head of NLS, on October 15, 2014.³⁵ Log-in information was e-mailed to all contacts. We e-mailed those who had not completed the questionnaire at multiple points during the data collection period, and we closed the survey on November 3, 2014. We received a completed questionnaire from each service unit and NLS.

Because we surveyed all of the unit heads and therefore did not conduct any sampling for our survey, our data are not subject to sampling errors. However, the practical difficulties of conducting any survey may introduce non-sampling errors. For example, differences in how a particular question is interpreted, the sources of information available to respondents, or the types of people who do not respond to a question can introduce errors into the survey results. We included steps in both the data collection and data analysis stages to minimize such non-sampling errors. Our analysts answered respondent questions and resolved difficulties that respondents had in completing our survey. Although the survey responses cannot be used to generalize the opinions and satisfaction of all customers that receive services from ITS, the responses provide data for our defined population.

The final questionnaire asked the heads of the service units and NLS to identify the extent to which they are satisfied or dissatisfied with the

³⁵We included NLS because it is the only Library unit—other than CRS and the Copyright Office—that receives its own appropriations.

services provided by ITS.³⁶ To determine the extent to which ITS is providing satisfactory IT services to its customers, we described the results on a 5-point satisfaction scale, where 5 is “very satisfied” and 1 is “very dissatisfied.”

To obtain additional narrative and supporting context from stakeholders, survey respondents were given multiple opportunities to provide additional open-ended comments throughout our survey. Using these open-ended responses, we conducted a content analysis in order to identify common factors. We then totaled the number of times each factor was mentioned by a respondent, choosing to report on the factors that were identified by two or more respondents.

Further, in order to determine the extent to which service units performed duplicative or overlapping IT activities, we sent a structured questionnaire to each service unit, as well as NLS.³⁷ This questionnaire asked each respondent to identify the extent to which they (1) purchased commodity IT in the past 3 years; (2) performed significant IT activities, as defined by the Information Technology Infrastructure Library; and (3) performed IT service desk functions. We also reviewed network diagrams and system security plans for the nine systems we selected as part of our fourth objective.

In addition, we reviewed portions of the Library’s hardware and software inventories to determine if it had made duplicative IT investments in selected areas:

- **Monitors:** Because the Library did not have an accurate inventory of its non-capitalized IT assets, we visited the Library’s warehouse in Landover, Maryland, and reviewed the facility’s physical and environmental controls. At that facility, we observed that ITS had approximately 400 19-inch monitors purchased in 2008 and about 100 24-inch monitors that were purchased in 2010. Although these monitors were several years old, according to ITS officials, they had never been used and were still in their original packaging. In order to

³⁶Survey respondents were asked to rate their organization’s satisfaction using the following terms: “very satisfied,” “moderately satisfied,” “neither satisfied nor dissatisfied,” “moderately dissatisfied,” “very dissatisfied,” “not applicable,” and “don’t know enough.”

³⁷We included NLS because it is the only Library unit—other than CRS and the Copyright Office—that receives its own appropriations.

determine whether service units purchased duplicative monitors, we asked each service unit, but not including OSI, to provide an inventory of its monitors. We received inventories from NLS, the Law Library, and Library Services.³⁸ We then identified 19-inch and 24-inch monitors in these inventories (1) that were of a different model number than those purchased by ITS and (2) for which their respective manuals were copyrighted later than 2008 for the 19-inch monitors and later than 2010 for the 24-inch monitors.

- **Software licenses:** We identified software applications that were purchased by more than one service unit and determined the extent to which the Library purchased too many or too few licenses. To select the applications, we used the software inventories developed by ITS and CRS with automated tools for deploying software to workstations that they manage.³⁹ First, for the ITS inventory, we identified applications that were deployed to two or more service units. Second, in order to ensure that we only selected software purchased by the Library, we removed any applications that were published by the Library itself. Third, using an open source search, we removed applications that can be legally obtained for free. Fourth, we removed applications that were being used for entities outside of the Library. Fifth, we eliminated purchases made by the Library's Inspector General. Based on these steps, we identified 24 applications. We then compared these 24 applications to CRS's application inventory to determine whether CRS purchased any of these applications. For these 24 applications, we obtained the relevant license agreements, and compared the number of licenses purchased to the number of licenses deployed throughout the Library. We chose to report on applications where the Library purchased at least 100 more licenses than it had deployed. To verify the reliability of the data on the number of deployed licenses, we examined it for obvious outliers, omissions,

³⁸According to Library officials, CRS, the Copyright Office, the Office of the Librarian, and OSO did not have monitor inventories.

³⁹These lists likely do not include workstations that are not connected to the Library's network. For example, we discovered a workstation used by the NLS in its data center that is not connected to the Library's network. Additionally, OSEP also manages, according to OSEP officials, a small number of workstations on its own network (separate from the Library's network). We did not review the OSEP software inventory because the office deploys software to workstations manually. Lastly, these lists do not include the Library's roughly 100 workstations manufactured by Apple, Inc. We do not believe that these three limitations materially impacted our analysis.

and errors, and interviewed officials familiar with the data to gain an understanding of the controls used to create and maintain the data. We determined that these data were sufficient for our purposes, which was to describe the number of Microsoft Visio 2010 Professional licenses the Library deployed.

We discussed the duplicative IT activities and investments with officials responsible for managing IT in CRS, the Copyright Office, Library Services, and OSEP.

To address our sixth objective, we evaluated the Library's IT policies and the position description of the Library's CIO against key practices we identified based on our research on and experience with federal agencies.⁴⁰ These practices related to the following areas:

- **Commodity IT:** The CIO should have the responsibility and authority, including budgetary and spending control, for commodity IT.
- **Mission-specific systems:** The CIO should have the ability to adequately oversee mission-specific systems to ensure that funds being spent on component agency investments will fulfill mission needs.
- **Relationships between CIO and components:** The responsibilities and authorities governing the relationship between the CIO and component organizations should be defined.

We also compared the tenure of the Library's recent CIOs to results from our research which found that CIOs and former agency IT executives believed it was necessary for a CIO to stay in office for 3 to 5 years to be effective and 5 to 7 years to fully implement major change initiatives in large public-sector organizations.⁴¹ Further, we interviewed the Chief of

⁴⁰GAO, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management*, [GAO-11-634](#) (Washington, D.C.: Sept. 15, 2011). See also, *Reducing Duplication and Improving Outcomes in Federal Information Technology*, Before the S. Comm. on Homeland Security and Governmental Affairs, 113th Cong. 32 (2013) (statement of David Pownier, Director of IT Management Issues, U.S. Government Accountability Office).

⁴¹GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, [GAO-04-823](#) (Washington, D.C.: July 21, 2004).

Staff, former Deputy Librarian, and Librarian of Congress to obtain information about the Library's plans for hiring a full-time CIO.

We conducted this performance audit from April 2014 to March 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Library of Congress



THE LIBRARIAN OF CONGRESS

March 16, 2015

Dear Mr. Willemsen:

Thank you for the opportunity to comment on the draft Government Accountability Office (GAO) report, "Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses" (GAO-15-315). I appreciate the Congress' engagement with the Library and its direction to GAO to conduct this study. I also extend my thanks to you and your team for your work on this assignment.

Information technology (IT) is a fundamental resource that is critical to the success of the Library of Congress. I have taken steps to improve the management of the Library's IT so that we may fully realize the possibilities of the digital era. I believe your report gives us a strong basis for further action.

Since December 2014, I have put in place a new and collaborative top management team to bring the Library's traditional analog services and our digital services closer together. We now have an outstanding new Deputy Librarian of Congress, Chief of Staff, and Associate Librarian for Library Services. All three have already successfully exercised multiple responsibilities within the Library of Congress and in the broader library community. In addition, I have assigned an experienced manager with a strong background in IT to serve as Chief Information Officer (CIO) on an interim basis while we conduct a nationwide search for a permanent CIO. I expect a permanent CIO to be on board by September 2015. The interim CIO, supported by an acting Deputy CIO, is focused exclusively on IT matters – managing regular operations and planning for structural and strategic changes. I am confident that their work will establish a solid foundation for the incoming permanent CIO.

To help the Library improve the management of the IT systems that support our programs and operations, the draft report offers 31 recommendations in six key areas. The Library generally concurs with the recommendations and is developing a detailed plan for implementing them. Following are the highlights of our strategy in each of the six areas.

1. Provide strategic direction for use of IT resources through strategic planning, enterprise architecture improvement planning, and human capital planning.

The Library will complete an initial IT strategic plan by April 2015. Prepared by the interim CIO in conjunction with Library service units, this plan will include a year-by-year implementation scheme for addressing each GAO recommendation as well as IT management recommendations made by the Library's Inspector General. This initial plan will provide

101 Independence Avenue, S.E. Washington, DC 20540-1000 Tel.: (202) 707-5205 Fax: (202) 707-1714 E-mail: libofc@loc.gov

2

immediate direction for refocusing our IT efforts. I am currently working with the service unit heads on the regular 5-year update of our agency's strategic plan. When our new Library strategic plan is issued, we will adjust the IT strategic plan as necessary to ensure that it is aligned with the Library's overall future direction.

The Library will finalize and validate the existing draft enterprise architecture (EA) by September 2015, with the assistance of an independent validation and verification team. This work will cover both the technical infrastructure and logical layers of the EA. Beginning in fiscal year (FY) 2016, the Library will implement an EA improvement plan – describing the target state for our EA and identifying steps to transition to the target. A senior IT manager has been assigned to coordinate the EA effort.

Having a diverse and highly skilled workforce is a fundamental strategic goal for the Library across all of our mission areas, including IT. By September 2015, the Library will complete an assessment of skills of IT staff throughout the agency. In early FY 2016, we will identify our future IT skills requirements and prepare a human capital development and hiring plan to address any gaps.

2. Provide a framework for effective IT investment decision-making and investment management.

Effective IT decision-making requires that the CIO and the executives who have legal and programmatic responsibility for the missions of their service units fully understand each other's requirements. To that end, I have made the CIO a permanent member of the Library's Executive Committee.

By September 2015, the Library will update its regulations and directives to clarify the decision-making roles and reporting responsibilities of the Executive Committee, the IT Steering Committee, and the Architecture Review Board with regard to IT investments – proposed new investments, those already in operation, and those in development. At the same time, we will formalize and resource an IT Investment Management Office charged with defining and managing the IT investment portfolio and supporting the IT Steering Committee and other IT governance bodies.

For FY 2016, the Library will implement a uniform method for service units to classify IT expenditures in the central financial system and an approach for maintaining a comprehensive inventory of Library IT assets. Such expenditure and asset data will inform our IT strategic planning and the links between planning, budgeting for FY 2017, and risk management.

3. Plan and manage IT acquisitions to deliver required capabilities on time and within budget through cost estimating, scheduling, and risk management.

During FY 2016, the Library will develop policies and implement the management disciplines of costing, scheduling and risk management for our IT acquisitions. This task will include a review of the Library's current systems development life cycle practices.

4. Protect IT systems and reduce the risk that they may be compromised.

The Library is committed to IT security – protecting our infrastructure, applications, web properties, and the data that is entrusted to us. The Library agrees that aligning our IT security policies and procedures more closely with those in use in executive branch agencies would be helpful. By the end of FY 2015, we will: ensure that our inventory of IT assets is up-to-date; update our information security plans and controls; implement continuous monitoring; fully document remediation efforts; enforce our existing requirement that employees, contractors, and volunteers complete IT security training; and conduct privacy impact assessments of our major IT systems. By the end of FY 2016, we will develop contingency plans following NIST Special Publication 800.53, "Security and Privacy Controls for Federal Information Systems and Organizations," version 4.

5. Ensure that IT services meet the needs of Library component units.

The Library agrees that satisfaction and accountability improve when IT service providers and their customers are working from a clearly documented set of shared expectations. By September 2015, we will update Library regulations to address the responsibilities of the Information Technology Services (ITS) directorate to Library components and require appropriate service level agreements between ITS and program offices. Such agreements, including service targets and satisfaction metrics, will be established by September 2015. The Deputy CIO will meet regularly with each service unit to discuss performance and review open IT issues. During FY 2016, the Library will implement a process to measure customer satisfaction with ITS services and to prioritize, resource, and resolve issues.

6. Allocate IT resources efficiently and effectively, reducing duplication or overlap.

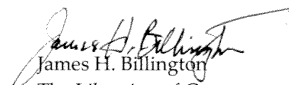
During FY 2016, the Library will identify potentially duplicative IT systems and operations for future review.

The Library intends to deliver timely, effective service to the Congress, the copyright community, researchers, and the American public, and to be an effective steward of the precious collections entrusted to us for generations to come. Thank you for your expert perspective in ensuring that the Library's IT will be up to this important task.

4

If you have any questions, please contact Elizabeth R. Scheffler, Interim Associate Librarian for Strategic Initiatives and Chief Information Officer, (202) 707-6042, esch@loc.gov.

Sincerely,


James H. Billington
The Librarian of Congress

Mr. Joel Willemssen
Managing Director, Information Technology
Government Accountability Office
441 G. St. NW
Washington, DC 20548

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Joel C. Willemssen, (202) 512-6253 or willemssenj@gao.gov

Staff Acknowledgments

In addition to the contact named above, individuals making contributions to this report included Lon Chin, Nick Marinos, and Christopher Warweg (assistant directors), Kaelin Kuhn (analyst-in-charge), Sher'rie Bacon, Chris Businsky, Sa'ar Dagani, Neil Doherty, Torrey Hardee, Thomas Johnson, Abishek Krupanand, Jennifer Leotta, Lee McCracken, David Plocher, Antonio Ramirez, Meredith Raymond, Karen Richey, Kelly Rubin, Kate Sharkey, Andrew Stavisky, Tina Torabi, Kevin Walsh, Shawn Ward, and Charles Youman.

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 website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

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

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548

