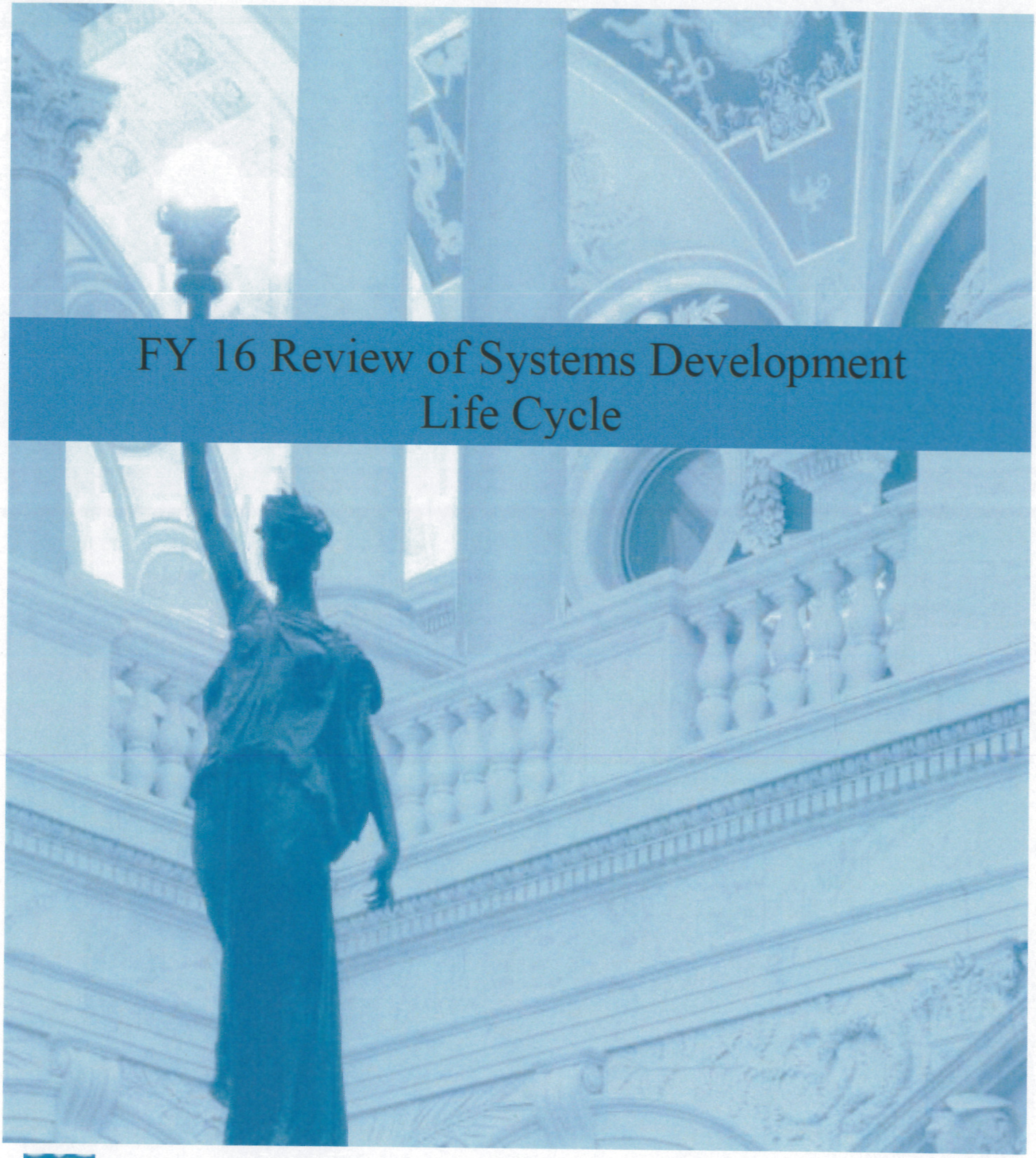


FY 16 Review of Systems Development Life Cycle

Library of Congress Office of the Inspector General

NOT FOR PUBLIC RELEASE

2016-IT-102

February 2017

OFFICE OF THE INSPECTOR GENERAL

LIBRARY OF CONGRESS
101 INDEPENDENCE AVE.
WASHINGTON, D.C. 20540

February 17, 2017

MEMORANDUM FOR: Dr. Carla D. Hayden
Librarian of Congress

FROM: Kurt W. Hyde
Inspector General

SUBJECT: Audit Report No. 2016-IT-102, *FY 2016 Review of Systems Development Life Cycle*

This transmits the audit report summarizing the results of Kearney & Company (Kearney) *FY 16 Review of Systems Development Life Cycle.* The Executive Summary begins on page *i,* and the full text of Kearney's report begins in Appendix A. Management's response to the recommendations appears in Appendix B. This report is not for public release.

Based on management's written responses to the draft report, we consider all of the recommendations resolved. Please provide, within 30 calendar days, a corrective action plan addressing implementation of the recommendations, including an implementation date, in accordance with LCR 2023-9, *Rights and Responsibilities of Library Employees to the Inspector General*, §7.A.

We appreciate the cooperation and courtesies extended by the Copyright Office, Library Services, the Office of the Chief Information Officer and its Web Services team, and other units within the Library during this review.

cc: Deputy Librarian

This page left blank intentionally

Table of Contents

Appendix A: Kearney & Company FY 16 Review of Systems Development Life Cycle 1
Appendix B: Management's Response 2

This page left blank intentionally

Appendix A: Kearney & Company FY 16 Review of Systems Development Life Cycle

This page left blank intentionally

Summary

For the Library of Congress (Library) to achieve a secure, efficient, and effective portfolio of business and program applications, its information system policies and procedures must establish a framework of sound System Development Life Cycle (SDLC) practices. Senior management must complement SDLC practices with an effective Project Management Life Cycle (PMLC) process that provides thorough development oversight, full investment transparency, and periodic variance analysis. As part of the Office of the Inspector General's (OIG) ongoing audit emphasis on the Library's information technology (IT) governance, operations, and best practices, OIG engaged Kearney & Company, P.C. (Kearney) to assess the Library's SDLC processes. This assessment involved a review of three recent system development efforts within the Library: the U.S. Copyright Office's (Copyright) Electronic Licensing System (eLi), Library Services Overseas Field Office Replacement System (OFORS), and the Office of the Chief Information Officer's (OCIO) Congress.gov[1].

Agencies with successful system development results employ SDLC practices that take new system concepts and products through clearly defined phases that include planning, requirements gathering, designing, building, and testing to deliver quality systems within investment and development targets. Inadequately developed IT systems expose agencies to waste throughout the system lifecycle (development, operations and maintenance, and retirement), and weaknesses in data confidentiality, availability, and integrity.

At the time the service units initiated each of the systems development efforts reviewed in this report (fiscal years 2010-2012), Library management began to implement disjointed elements of information systems governance. Those elements included establishing an IT Steering Committee, a Project Management Office website, and an SDLC/PMLC methodology. Despite establishing those elements, Library senior management at the time made it optional for service unit management to comply with prescribed SDLC/PMLC practices and requirements when funding new system development from their base budgets. In addition, top Library officials at that time did not hire a qualified CIO. These issues were identified in previous OIG reports.[2]

Beginning in FY 2014, new Library leadership reorganized its IT resources into an infrastructure service unit. The changes initiated by that reorganization continued with the recent Library Special Announcement 16-9 advising that the CIO reports directly to the Librarian. The re-alignment of the CIO role at the Library is consistent with the principles of the Clinger-Cohen Act[3] and should further serve to break down the silos that previously fostered waste and an absence of transparency for IT expenditures and investments. OIG believes this top down leadership approach should result in substantial benefits to the service units, such as greater accountability and performance. Progress in the delivery of efficient and secure information systems will demonstrate to Congress that appropriating funds to the Library for new system investments will deliver the promised investment results.

What the Assessment Found

In summary, Kearney determined that two of the three systems reviewed did not establish and utilize SDLC practices from the outset of development activities. As a result, key program and project

[1] Congress.gov was initiated in 2012 by the Library's Web Governance Board (WGB) and continues to be overseen by the WGB. Development and implementation has been managed by Web Services, originally part of the Office of Strategic Initiatives (OSI) and currently part of OCIO, since project inception.

[2] See: Audit Report No. 2014-IT-101 *Report on the Design of Library-wide Internal Controls for Tracking Information Technology Investments*, March 2015; Audit Report No. 2014-PA-101 *The Library Needs to Determine an eDeposit and eCollections Strategy*, April 2015; and Report No. 2015-IT-101 *Benchmarking the Library of Congress Information Technology Fiscal Year 2014 Budgetary Obligations and Human Capital*, March 2016.

[3] This act applies to DoD and executive agencies. The law requires each agency head to establish clear accountability for IT management activities by appointing an agency Chief Information Officer (CIO) with the visibility and management responsibilities necessary to carry out the specific provisions of the Act.

controls were not instituted early on in the eLi and OFORS projects. In contrast, Kearney observed SDLC practices being enforced and followed for the Congress.gov project, which was managed by the OCIO (formerly ITS).

Further, contracts for system development work for eLi and OFORS did not require vendors to comply with systems development best practices. Without SDLC compliance requirements, contractors with fixed price contracts may seek to strictly meet contractual requirements and save costs on internal controls and quality compliance. At the time the Service Units let the contracts, the Library's contracts office and Contract Officer Representatives did not demonstrate the knowledge, skills, and abilities to enforce best practices for system development projects.

Specifically, Kearney found that:

Copyright did not follow sound SDLC methodologies which resulted in it scrapping the eLi project development after six years and $11.6M in project expenditures. The eLi project began in 2010 with a budget approval of $1.1M, and increased to approximately $2M for full implementation in 2012. Ultimately, Copyright spent over $11.6M through 2016 when it decided to terminate the contracts and abandon development activities. During that six-year period, Copyright continued to report in eLCplans (the Library's performance management system) that eLi development was occurring near or on schedule.

Neither Copyright Licensing nor its contractors made use of appropriate SDLC standards during the eLi development. Continuous failure of vendor developed software to meet Copyright Licensing requirements was attributed to poor requirements and software code management, both key elements of effective SDLC management.

Most evident in the eLi project was a lack of demonstrated project management skills. Copyright did not ensure it properly controlled the project and its contractor. Additionally, Copyright did not employ an earned value management approach to proactively identify cost overruns and plan corrective actions.[4]

Library Services did not follow sound SDLC methodologies which resulted in late and incomplete deployment of OFORS with inadequate security. Library Services initiated the OFORS development program in 2010 with an approximate budget of $1.7M. An additional $.5M congressional budget request was denied in 2011, leaving Library Services to provide that additional funding from base program sources. Library Services did not mandate the use of SDLC standards during the OFORS development efforts internally or by the contract firms performing the work.

The absence of SDLC requirements management and product testing led to the vendor delivering an incomplete system resulting in legal action by the Library. The expected completion of all the requirements in the originally designed system is now forecasted for the end of 2017.

Although the development work for OFORS remains relatively near budget to date, the absence of the required functionality and delays until the end of 2017 to complete will contribute to additional internal project costs along with undelivered operating improvements. During the six years of development, Library Services was not consistently reporting in eLCplans the system development status and performance.

Because of incomplete security requirements and controls implementation, security issues relating to OFORS were further identified for remediation. The most significant security issues identified related to inconsistent server configurations and vulnerability scanning across the foreign offices. The remediation activities required were agreed to with the systems owner and project team.

[4] Appendix J of OMB Circular A-11 defines earned value management as a management tool used to mitigate risks in developing capital assets.

OCIO's development of Congress.gov resulted in system delivery on time, within investment budget, and with limited post implementation security repairs required. Congress.gov development was initiated in 2010. As part of the OCIO (formerly ITS), the project team adopted the available SDLC and PMLC policies and standards. Congress.gov development was performed using an iterative (or Sprint) methodology, which delivers packages of incremental functionality in a manner prioritized and communicated with users providing their requirements. ITS adequately monitored the development and implementation of requirements for completeness and user acceptance.

Recommendations

With the recent Library reorganization placing all IT oversight under the OCIO, the CIO should focus on improving the Library's system development practices and compliance. The CIO should undertake a review of all systems development work currently in planning or in progress and compile an inventory of the projects and evaluate their compliance with Library technology investment, SDLC, and PMLC standards. The CIO should share the review's results and evaluation with the Strategic Planning and Performance Management Office, Budget Office, and Financial Reports Office, as well as with the Librarian's Office and Executive Committee. While not noted in this report as a non-compliance issue, the OIG has stated in various reports that improvement opportunities exist for capturing and reporting full time employee costs related to specific development projects. OCIO, Office of the Chief Financial Officer, and Human Resource Services should collaborate on finding solutions for financial system tracking of employee costs involved in new system development.

Management's Response

In response to the draft report (see Appendix B), the Library's senior leadership agreed with all of the recommendations. Our office acknowledges and appreciates the comments from the Copyright office on the recommendations along with their concurrence. With regard to Copyright's comments, the review and conditions noted are clear that Copyright executives at that time did not disclose in the Library's performance management system (eLCplans) and annual Congressional Budget Justifications the magnitude of issues and cost overruns related to the project. As a result, Congress and Library executives did not have adequate information to timely act on and address the issues.

This page left blank intentionally

Library of Congress

Performance Audit of the System Development Life Cycle Practices and IT Security Assessments

Report Date: January 4, 2017

KEARNEY& COMPANY

Points of Contact:
William Kubistal, Partner
Phil Moore, Partner
1701 Duke Street, Suite 500
Alexandria, VA 22314
703-931-5600, 703-931-3655 (fax)
wkubistal@kearneyco.com
phil.moore@kearneyco.com

TABLE OF CONTENTS

Page #

COVER LETTER....1
OBJECTIVES....3
BACKGROUND....3
SUMMARY OF AUDIT RESULTS....4
LIBRARY-WIDE (SYSTEMIC ISSUES)....5
ELECTRONIC LICENSING SYSTEM (ELI)....8
OVERSEAS FIELD OFFICE REPLACEMENT SYSTEM (OFORS)....15
CONGRESS.GOV....22
AUDIT METHODOLOGY AND SCOPE....26
DETAILED AUDIT FINDINGS – ELI....30
DETAILED AUDIT FINDINGS – OFORS....46
DETAILED AUDIT FINDINGS – CONGRESS.GOV....63

KEARNEY&
COMPANY

1701 Duke Street, Suite 500, Alexandria, VA 22314
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

COVER LETTER

January 4, 2017

Kurt W. Hyde
Inspector General
Library of Congress
101 Independence Ave SE
Washington, D.C. 20540

Dear Mr. Hyde,

Kearney & Company, P.C. (Kearney) has conducted an audit of the Library of Congress' (LOC) System Development Life Cycle (SDLC) practices and Information Technology (IT) Security of the Copyright Office's Electronic Licensing System (eLi), the Library Services Overseas Field Office Replacement System (OFORS), and the Congressional Research Service's Congress.gov website and supporting applications. This performance audit, conducted under Contract No. LCOIG16C0009, was designed to meet the objectives identified in the "Objectives" section of this report.

Kearney conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), 2011 Revision, issued by the Government Accountability Office (GAO). The purpose of this report is to communicate the results of Kearney's performance audit, as well as our related findings and recommendations. This report includes language that is intended solely for the information and use of LOC and is not intended to be and should not be used by anyone other than these specified parties.

An audit involves performing procedures to obtain evidence about the performance of a program. The procedures selected depend on the auditor's judgment, including an assessment of the risks of system development and IT security, whether due to fraud or error. An audit also includes evaluating the appropriateness of policies used and the reasonableness of decisions made by management, as well as evaluating the overall presentation of assertions made by management.

Based on our audit work, we concluded that the Copyright Office did not have the appropriate project management and contracting procedures in place to ensure system development delivery of required technical elements within the development timeframe and project budget. The Copyright Office did not have a project oversight function to evaluate development delays, additional funding requests, and recommended courses of action. The Copyright Office did not define project management oversight responsibilities of third-party vendors and did not contractually define vendor technical deliverables, timelines, and project management activities.

As a result, the Copyright Office ceased current development activities in October 2016 after six years and approximately $11 million of expenditures.

Kearney also concluded that the Library Services service unit did not have the appropriate project management and contracting procedures in place to ensure system development delivery of required technical elements within the development timeframe and project budget. In addition, the Library Services service unit did not have a project oversight function to evaluate development delays, additional funding requests, and recommended courses of action until fiscal year (FY) 2016. Library Services did not define project management oversight responsibilities of third-party vendors and did not contractually define vendor technical deliverables, timelines, and project management activities. Library Services has halted development efforts, and they are requesting a project remediation plan from the vendor for missing and/or late deliverables. While the vendor delivered the base product functionality, the vendor has not delivered key user functional requirements related to the Printing, Binding, and Managing Suppliers Inventory and In-Transit processes.

Kearney also concluded that the Congress.gov project team did have the appropriate project management and contracting procedures in place to ensure system development delivery of required technical elements within the development timeframe and project budget.

Kearney appreciates the cooperation provided by LOC's personnel during our audit.

Kearney & Company

Kearney & Company, P.C.
January 4, 2017

OBJECTIVES

The Library of Congress's (referred to as "LOC" or "the Library") Office of Inspector General (OIG) contracted Kearney & Company, P.C. (referred to as "Kearney," "we," and "our") to conduct a performance audit on three LOC system development efforts:

- The Electronic Licensing System (eLi) managed by the Copyright Office (USCO)
- The Overseas Field Office Replacement System (OFORS) managed by the Overseas Operation Division (OvOp) of Library Services
- The Congress.gov website, formerly managed by the Congressional Research Service and now managed by the LOC Office of the Chief Information Officer (OCIO).

During the performance audit, Kearney evaluated the Library's information technology (IT) system development practices, known in industry as the Systems Development Life Cycle (SDLC), as well as reviewed critical IT security elements for the programs mentioned above, using Federal standards and industry best practices as a benchmark.

Additionally, Kearney evaluated the appropriateness of LOC's IT-related policies against recognized industry best practices, the reasonableness of management decisions, and the performance of SDLC and IT security programs to LOC's own policy framework.

BACKGROUND

USCO – The USCO is one of LOC's eight service units. The USCO administers United States copyright laws, including: registration; the recordation of title and licenses; a number of statutory licensing provisions; and the collection, investment, and disbursement of copyright fees. The USCO employs approximately 420 employees, including 25 IT employees assisting with IT oversight and daily operations, business analysis, and project and contract management.

The USCO receives funding from two different sources: annual appropriations and a congressionally mandated ceiling of collected fees under Title 17 of the United States Code (U.S.C.). In fiscal year (FY) 2016, Congress appropriated $23 million and authorized expenditures up to a $36 million fee ceiling under Title 17.

The USCO is exempt from complying with LOC OCIO system development policies when funding of that development is from USCO's base budget. The USCO manages and operates 17 applications in support of its mission. The service unit last managed a system initial development project in 2008.

Library Services – Library Services is one of LOC's eight service units and supports the mission of LOC through the acquisition, cataloging, preservation, and referencing services of traditional and digital collections. Library Services employs approximately 1,300 employees, including 60 IT employees.

Library Services receives funding via annual appropriations. In FY 2016, through congressional appropriations, LOC allotted Library Services $214 million.

Library Services is exempt from complying with LOC OCIO system development policies when funding those systems out of its base budget. Library Services manages and operates 33 applications in support of its mission.

OCIO – OCIO[1] supports the mission of LOC by providing IT strategic direction, leadership, services and capabilities. OCIO employs approximately 295 employees.

The LOC OCIO receives funding via annual appropriations. In FY 2016, through congressional appropriations, the LOC allotted OCIO $85 million.

SUMMARY OF AUDIT RESULTS

While Kearney conducted performance audits for each of these three systems (i.e., eLi, OFORS, and Congress.gov) individually, we noted the following overarching factors that affected some, if not all, of the programs reviewed:

- LOC did not have fully developed SDLC policies, procedures, and oversight practices established at inception of eLi and OFORS development activities. As LOC developed a more specific SDLC, the new policies were not applied retroactively to existing development activities
- The eLi and OFORS projects were not subject to the oversight and mandates of OCIO guidance at the time they were initiated. The system owning service units had the authority to develop these systems on their own and, therefore, moved forward without requesting guidance from OCIO or its IT Steering Committee (ITSC), or developing comparable project oversight policies
- The eLi and OFORS-related contracts did not have clearly defined requirements, deliverables, or timelines, indicating a lack of standardized IT-related contract templates or coordination with OCIO or the Library's Office of Contracts and Grants Management
- The eLi and OFORS projects did not define required project management and contractor oversight responsibilities
- The eLi and OFORS projects did not create a management body to evaluate development delays, additional funding requests, and recommended courses of action. eLi and OFORS project management and respective service units did not clearly and timely report project delays and funding needs in excess of approved amounts to LOC management and the budget office.

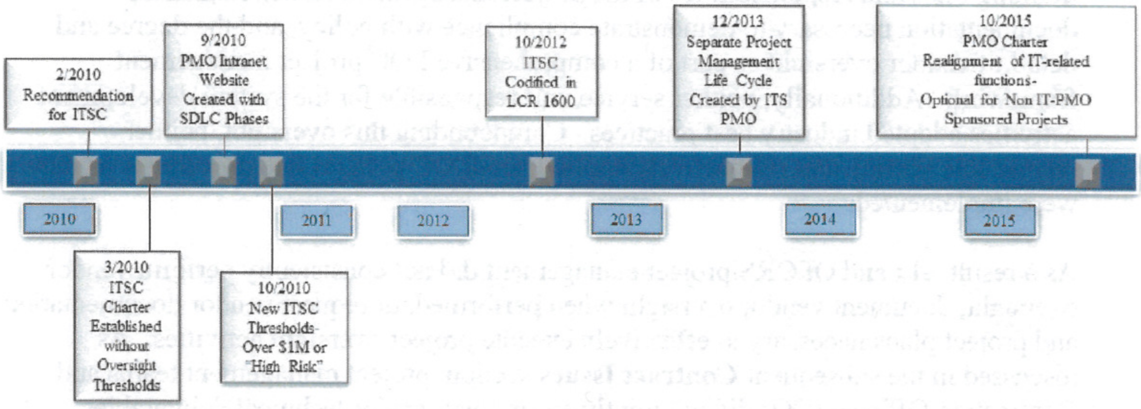
Below is a summary of audit findings, broken out by system. Detailed findings for each audited system are listed in **Appendix A**.

[1] Web Services, which manages Congress.gov, began under the Office of Strategic Initiatives (OSI), which later became OCIO. OCIO was initially aligned as a unit under the Office of the Librarian/Office of the Chief Operating Officer (OCOO) in FY 2015. In September 2016, OCIO became its own service unit directly reporting to the Librarian of Congress.

Library-Wide (Systemic Issues)

LOC created the ITSC in 2010 by establishing a charter and broadly defined processes, roles, and responsibilities of the Committee and service units related to IT system development activities. The following timeline identifies key milestones in LOC's development of IT system development authorities, responsibilities, and oversight activities.

Exhibit 1: ITSC Development Timeline


2/2010
Recommendation for ITSC
9/2010
PMO Intranet Website Created with SDLC Phases
10/2012
ITSC Codified in LCR 1600
12/2013
Separate Project Management Life Cycle Created by ITS PMO
10/2015
PMO Charter Realignment of IT-related functions- Optional for Non IT-PMO Sponsored Projects
2010
2011
2012
2013
2014
2015
3/2010
ITSC Charter Established without Oversight Thresholds
10/2010
New ITSC Thresholds- Over $1M or "High Risk"

Program Management

- At the inception of the eLi and OFORS development process, LOC did not have fully developed SDLC oversight policies, procedures, and practices. As LOC developed more specific SDLC policies and procedures, the new policies were not applied retroactively to existing development activities.

  Because of this policy gap, both system development activities proceeded without the structure of a comprehensive LOC oversight framework. Additionally, neither service unit responsible for the system development activities adopted industry best practices. Compounding this oversight, neither responsible service unit retroactively applied new LOC policies and procedures as they were implemented.

  As a result, eLi and OFORS project management did not report development delays, vendor performance issues, key contract modifications (i.e., terms, billing conventions, technical milestones, and contract value), and cost increases to LOC, budget oversight, and the service units. Currently, both project management teams have halted development activities and neither project team has deployed systems that met user-defined functionality.

Project Management

- At the inception of the eLi and OFORS development process, LOC did not have fully developed SDLC project management policies, procedures, and practices. As LOC developed more specific SDLC project management policies and procedures, the new policies were not applied retroactively to existing development activities.

  Because of this policy gap, both system development activities proceeded without clearly defining roles and responsibilities of the project management teams, minimum documentation necessary to demonstrate compliance with policy, and the degree and detail of vendor oversight as part of a comprehensive LOC project management framework. Additionally, neither service unit responsible for the system development activities adopted industry best practices. Compounding this oversight, neither responsible service unit retroactively applied new LOC policies and procedures as they were implemented.

  As a result, eLi and OFORS project management did not consistently perform vendor oversight, document vendor oversight when performed, or request vendor documentation and project plans necessary to effectively execute project oversight activities. As discussed in the subsequent **Contract Issues** section, project management teams and Contracting Officers (CO) did not jointly ensure that vendor technical deliverables, project timelines, and milestones were appropriately included in vendor contracts. Currently, both project management teams have halted development activities and neither project team has deployed systems which met user-defined functionality.

Contract Issues

- The following key contracting elements were not present to establish vendor accountability for the eLi and OFORS projects:
  - Requirements for project management best practices, customer oversight, and acceptance
  - Technical requirement details to ensure user functionality
  - Contractor deliverable details (e.g., software source code, programmer's documentation)
  - Vendor oversight requirements
  - Interim and final review criteria (e.g., milestones and expectations for development at those milestones)
  - Clearly defined technical framework, resulting in the inability to match technical requirements to deliverables.

Security Issues

- There were no significant Library-wide (systemic) findings in this audit area.

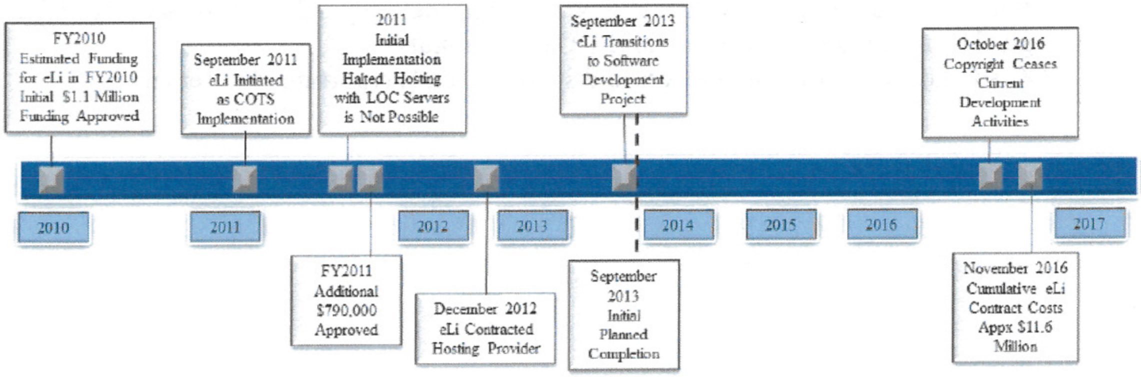
Recommendations

1. LOC should compare current SDLC policies and procedures to industry best practices to ensure development risks are actively monitored and managed
2. LOC should monitor current SDLC activity and environmental factors as part of a structured risk assessment framework to ensure policies and procedures identify and address emerging issues/new risks
3. COs and Contracting Officer's Representatives (COR) should collaboratively identify standard SDLC contract elements, including vendor timelines, technical deliverables, required documentation, and internal review and acceptance procedures, as well as ensure that SDLC contracts contain these elements
4. LOC should develop policies that clearly delineate required oversight approval for additional funding requests, contract modifications, delivery delays, and inability to meet original technical requirements in all LOC service units
5. LOC should clarify funding sources and status of funds reporting requirements.

Electronic Licensing System (eLi)

The USCO's Licensing Division began development of the eLi system in 2010. eLi is intended to streamline the receipt of Copyright royalty paments and management of Copyright royalty investment accounts. The initially approved contract budget was approximately $1.1 million, which was subsequently increased to approximately $2 million in 2011. To date, the USCO has spent over $11.6 million with third-party vendors to develop this system. In October 2016, the USCO cancelled the developer's contract prior to deployment of this project. The USCO is currently evaluating the options regarding development of the next steps, including identifying what elements are functional or recoverable.

Exhibit 2: eLi Development Timeline


FY2010 Estimated Funding for eLi in FY2010 Initial $1.1 Million Funding Approved
September 2011 eLi Initiated as COTS Implementation
2011 Initial Implementation Halted. Hosting with LOC Servers is Not Possible
September 2013 eLi Transitions to Software Development Project
October 2016 Copyright Ceases Current Development Activities
2010
2011
2012
2013
2014
2015
2016
2017
FY2011 Additional $790,000 Approved
December 2012 eLi Contracted Hosting Provider
September 2013 Initial Planned Completion
November 2016 Cumulative eLi Contract Costs Appx $11.6 Million

The USCO embarked upon this development activity without specific and detailed policies, procedures, guidelines, and responsibilities related to program and project management. This lack of process guidance and accountability resulted from the USCO's failure to proactively address an existing gap in LOC's governance policies.

The USCO project management team did not demonstrate effective, proactive project cost management practices. Over the six-year development period, USCO project management expended $11.6 million in vendor costs. The USCO project management team received specific funding for approximately $1.9 million in the first two years of the project. USCO project management did not update project budgets for the subsequent six years of development activity, nor perform an analysis of estimated cost overruns. Subsequent development funding activities occurred, inconsistent with initial funding requests. As discussed below, the USCO had no management body to evaluate and approve additional funding requests in conjunction with experienced development delays, analyses, and recommended courses of action. Additionally, the USCO did not have an oversight body with authority to halt project activities based on cost overruns, delivery delays, and/or lack of functionality until appropriate remediation plans or project management structure was in place.

Further, the USCO annual budget requests did not convey the eLi development challenges. Below is a summary of the USCO's annual Congressional Budget Justifications (CBJ) regarding eLi. These project status summaries are inconsistent with the actual project delays, cost overruns, and the eventual halt in development activities.

Exhibit 3: Licensing Division Reporting for eLi in the CBJ

CBJ FY	Priority Activities Comments Licensing Reengineering/eLi in CBJ
2010	Begin business process reengineering project to be fully implemented in FY 2012.
2011	Licensing will continue its reengineering efforts with the goal of fully implementing the process in FY 2012.
2012	Licensing will continue implementing and refining the reengineered processes and system.
2013	Licensing will continue implementing and refining the reengineered processes and system.
2014	Licensing will continue implementing and refining the reengineered processes and system.
2015	Licensing will continue implementing and refining the reengineered processes and eLi.
2016	Licensing will continue to work toward a fully automated system for receiving and examining Statements of Account.
2017	Licensing will continue to work toward a fully automated system for examining and making available Statements of Account.

From 2010 to 2016, the USCO reported eLi strategic planning information to the Library's planning office via eLCplans. eLCplans is a centralized database tool that houses strategic planning information and annual performance data, automating the annual planning and performance process. In 2010, 2014, and 2016, the USCO reported no performance metrics or goals for eLi. ***Exhibit 4*** provides a summary of the years in which the USCO reported performance metrics for eLi in eLCplans. These self-reported metrics are inconsistent with actual project delays, cost overruns, and the current halt in development activities.

Exhibit 4: eLi Annual Reporting in eLCplans

Year	Goal	Results	Rating/Metric
2011	Develop functional requirements documents for online cable licensing interface by September 30, 2011	Functional Requirements Document for project has been developed.	**Green**[2]
2012	Pilot systems and processes for online cable licensing by September 30, 2012	The USCO successfully launched the pilot of the cable Statement of Account submission system in September. For the first time, users of statutory licenses were allowed to see and comment on an electronic system for submitting statements and paying royalties to copyright owners. Implementation of other relevant system components (e.g., IT security, training, procedure manuals, Licensing Division System data migration) was also begun. Completion of user acceptance testing/piloting and finalization of e-system build for cable Statements of Account and fees are planned for completion in FY 2013.	**Amber**[2]
2013	Host online licensing system for filing cable Statements of Account in the cloud with an Approval to Operate (ATO) by September 30, 2013	USCO accomplished the milestones of the project: • **December 31:** Awarded hosting contract • **March 31:** Successfully completed proof of concept in Amazon Cloud (AWS) • **June 30:** Completed development environment in AWS • **September 30:** ATO granted for next phase of pilot.	**Green**[2]

[2] eLCplans used a three-color coded rating scheme. Green indicated that the service unit was on track to accomplish its annual goal; amber indicated that the service unit was behind its plan targets but adjustments could result in accomplishing the plan; and red indicated that the service unit would not accomplish the plan's annual target.

Year	Goal	Results	Rating/Metric
2015	Complete FY 2015 scheduled reengineering phases	Planned milestones were completed (i.e., eLi batch submission pilot, pilot results analyzed and communicated to stakeholders, fiscal requirements for eLi). The Independent Assessment was reviewed and, as a result, subsequent steps have been taken and other steps are planned for implementation. The ownership of the eLi project is transitioning to the Copyright Technology Office, which will manage its development and new targets/milestones for FY 2016 and after.	**Green**[2]

The USCO began eLi development as current SDLC policy began development and maturation. As the current policy developed, LOC did not require a retroactive application to existing development efforts. In essence, the USCO developed eLi without an LOC policy framework. The USCO did not voluntarily adopt the matured LOC OCIO's SDLC policy, nor did it develop a comparable framework based on industry best practices. The USCO did not establish a program oversight function similar to LOC's IT Investment Board, nor did the USCO regularly review project management and development activities. No management body existed to evaluate development delays, additional funding requests, and recommended courses of action. The USCO did not have an oversight body with authority to halt project activities based on cost overruns, delivery delays, and/or lack of functionality until appropriate remediation plans were in place.

The USCO also failed to develop in detail the roles and responsibilities of project management. Project management practices exhibited several gaps from best practices, including not establishing accountability for specific project management activities, failing to perform and document oversight on recurring basis, inconsistently documenting the matching of system requirements to development activities, failing to create and track project plan milestones, and not performing an analysis of additional funding requests. This lack of specific oversight activity precluded project management from identifying missing system functionality and cost overruns early in the development cycle. Early remediation efforts are more cost-effective as rework efforts are minimalized.

Additionally, vendors' contracts did not contain technical requirements, specific deliverables, or timelines to support program and project management oversight. These missing elements amplified the issues resulting from the lack of specific project management procedures (i.e., the specific contractor deliverables necessary to complete project management tasks).

Significant challenges identified in the eLi program audit include:

Program Management at the Service Unit Level

- The USCO failed to develop service unit-level policies and procedures to establish accountability and clearly define required program and cost management activities including:
  - Project schedule monitoring
  - Project budget approval processes
  - Regularly scheduled project budget reporting
  - Cost variance analysis
  - Accountability for project contractor oversight
  - Tracking of corrective actions.

- The USCO did not conduct periodic service unit management reviews of project progress, variances, and development breakdowns. As a result, USCO was unable to make assessments to continue, alter, or cease project development.

- Additionally, there was no evidence of service unit management reporting to LOC management on capital project development.

Project Management at the Functional Level (Development Activity)

- The eLi project did not have a thorough project management framework to ensure all phases of the development project were thoroughly planned and executed (i.e., Planning, Analysis, Design, Deployment, and Maintenance).

- There was no evidence of a comprehensive Project Management Plan (PMP) to define how the project is to be executed, monitored, and controlled, which would enable accurate reporting, planning, and project adjustments. Additionally, project managers did not build a Risk Management Plan and Risk Register, therefore, they were unable to identify and recognize potential events or conditions (risks) which could negatively effect one or more project objectives, such as scope, schedule, cost, and quality.

- Project management did not effectively track scope and schedule changes to closure, as they stopped tracking changes in 2014. Additionally, project managers failed to document departures from the planned project schedule (with associated justification) in the project log, resulting in numerous and significant scope changes affecting the schedule and increasing the overall cost of the project.

- Project managers did not create a concept proposal or PMP to capture all human capital requirements. As a result, USCO management could not match the necessary human capital to project needs or properly assign roles/responsibilities, reporting relationships, availability, etc.

- There was no evidence of a standardized Requirements Management Plan used to elicit, document, and track development requirements; therefore;
  - The project team defined its own method for establishing and documenting requirements in multiple documents, formats, and locations
  - The project management team did not have a standardized process to validate technical requirements and verify whether stakeholder needs were fully defined and implemented, causing scope changes across the project
  - The project management team was unable to fully define requirements in supporting vendor contracts (See **Contract Issues**).

- There was no evidence that an Analysis of Alternatives (AoA) was conducted to ensure selected project direction was the best solution to meet user needs with minimal cost and complexity. The resulting system is not operational at a cost of $11.6 million, $9.7 million over budget.

- eLi did not have an observable system requirements baseline providing a defined, confirmed, and validated set of system requirements needed to ensure user needs were met.

- There was no evidence of a System Development Plan or "blueprint" for eLi which defines development methodologies and work standards. Without a solid System Development Plan as a reference, project managers were unaware of how contractors were constructing the system (i.e., coding standards, testing schedules, and tools used) and could not validate if the system was built using industry-acceptable standards. Furthermore, without this reference document, the project management team could not properly monitor the development, testing, deployment, and verification of software in the operational environment, creating a dependency of the government on the vendor for support.

- There was no evidence of change management processes to receive, analyze, and validate proposed system changes before implementation and avoid unnecessary or potentially harmful changes to the system. Additionally, there was no evidence to support that system changes made were verified for accuracy and compliance with operational and security requirements.

- Although system development for eLi began in 2010, the USCO did not approve the eLi project charter until May 2016.

Contract Issues

- The following key contracting elements were not present to establish vendor accountability for the eLi project:
  - Requirements for project management best practices, customer oversight, and acceptance
  - Technical requirement details to ensure user functionality

- Contractor deliverable details (e.g., software source code, programmer's documentation)
- Vendor oversight requirements
- Interim and final review criteria (e.g., milestones and expectations for development at those milestones)
- Clearly defined technical framework, resulting in the inability to match technical requirements to deliverables.

Security Issues

- Security testing was not performed on eLi, as the system is not operational.

Summary of Project Results Culminating from the Above Deficiencies

1. Project terminated after six years
2. Initial project plan and contract vehicle significantly modified after inception; existing Library server infrastructure did not have capacity to meet technical requirements and upgrading was not feasible or cost-effective
3. No transparency to LOC or Congress regarding the funds used or time lost
4. $11.6 million in wasted costs due to mismanagement of the project development and resultant excessive expenditures without delivery of a functioning system.

Recommendations

1. For all future system development activities, USCO should ensure that current LOC policies and relevant industry best practices are adopted by service unit oversight and project management teams
2. USCO should clearly define technical requirements and functionality of the systems
3. USCO should clearly define vendor timelines, technical deliverables, and required documentation as part of the contract and Statement of Work (SOW)
4. USCO should develop reasonable and reliable cost estimates for subsequent development activities and obtain LOC oversight approval
5. USCO should clarify funding sources and status of funds reporting
6. If development activities for eLi resume, USCO should assess elements of exisiting development work products for possible reuse.

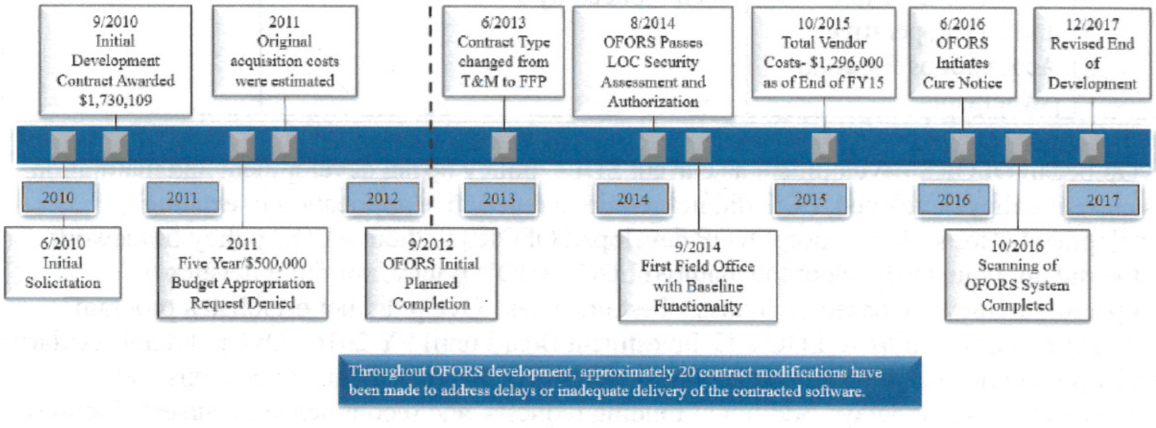
Overseas Field Office Replacement System (OFORS)

The Overseas Operation Division (OvOp) of Library Services initiated the OFORS development program in 2010. OFORS is designed to support acquisition activities of the six LOC field offices around the world. OFORS functionality includes ordering and receiving claims for missing and overdue items, recording financial obligations, and documenting payments, as well as credits for LOC and participants in the Cooperative Acquisitions Programs.

The initial September 2010 awarded contract value was $1,730,109, which was subsequently increased to $1,771,000 in 2016. In May 2013, the contract type was changed from a "Time and Materials with Firm Fixed Unit Pricing" to "Firm Fixed Price" with an unchanged total contract value. OvOps submitted a five-year, $500,000 annual funding request in FY 2011. Congress did not fund this request. Instead, OvOp has funded development costs from the Acquisitions and Bibliographic Access (ABA) Directorate and the six field offices' operating funds (Cooperative Acquisitions Program System). Additionally, OvOp did not include OFORS in the LOC strategic reporting and planning process until 2015.

Several contract modifications have been issued to extend the period of performance, correct dates, add funding, change the CO, change the COR, and for various other reasons. The system is currently deployed and operational; however, it is missing key functionality identified to support overseas office activities, including binding, shipping, inventory, and managing suppliers. Full feature capability is now expected by December 2017. To date, over $1,296,000 in contract costs have been invested in this system development project.

Exhibit 5: OFORS Development Timeline


9/2010 Initial Development Contract Awarded $1,730,109
2011 Original acquisition costs were estimated
6/2013 Contract Type changed from T&M to FFP
8/2014 OFORS Passes LOC Security Assessment and Authorization
10/2015 Total Vendor Costs- $1,296,000 as of End of FY15
6/2016 OFORS Initiates Cure Notice
12/2017 Revised End of Development
2010
2011
2012
2013
2014
2015
2016
2017
6/2010 Initial Solicitation
2011 Five Year/$500,000 Budget Appropriation Request Denied
9/2012 OFORS Initial Planned Completion
9/2014 First Field Office with Baseline Functionality
10/2016 Scanning of OFORS System Completed

Throughout OFORS development, approximately 20 contract modifications have been made to address delays or inadequate delivery of the contracted software.

OvOp project managers embarked upon this development activity without specific and detailed policies, procedures, guidelines, and responsibilities related to program and project management. This lack of process guidance and accountability resulted from OvOp's failure to proactively address an existing gap in LOC's governance policies.

Library Services did not consistently report OFORS strategic planning information via eLCplans from FY 2010 to 2016. eLCplans is a centralized database tool that houses strategic planning information and annual performance data, automating the annual planning and performance process. In 2010-2014, Library Services reported no performance metrics or goals for OFORS. Below is a summary of the years in which Library Services reported OFORS performance metrics in eLCplans. These self-reported metrics are inconsistent with actual project delays, cost overruns, and the current halt in development activities.

Exhibit 6: OFORS Annual Reporting in eLCplans

Year	Goal	Results	Rating/Metric
2015	Implement OFORS in the Jakarta, Islamabad, Nairobi, and Rio De Janeiro offices.	In FY 2015, LOC implemented OFORS in all six overseas offices in Brazil, Egypt, India, Indonesia, Kenya, and Pakistan. The new system enables the Library to retire its disparate, obsolete systems for accounting, billing, and tracking in the overseas offices and will improve its service to Cooperative Acquisitions Program customers.	**Green**
2016	Optimize OFORS in all six offices and reduce use of legacy systems by 70% to achieve efficiencies and improve service to the Library and its Cooperative Acquisitions Program participants.	OFORS was optimized in all six offices, and use of legacy systems has been reduced by 90%.	**Green**

OvOp began OFORS development as current SDLC policy began development and maturation. As current policy developed, LOC did not require a retroactive application to existing development efforts. In essence, OvOP developed OFORS without a LOC policy framework. OvOp did not voluntarily adopt the matured LOC OCIO's policy, nor did it develop a comparable framework based on industry best practices. OvOp did not establish a program oversight function similar to LOC's IT Investment Board until FY 2016. OvOp did not regularly review project management and development activities. No management body existed to evaluate development delays, additional funding requests, and recommended courses of action. OvOp did not have an oversight body with authority to halt project activities based on cost overruns, delivery delays, and/or lack of functionality until appropriate remediation plans were in place.

OvOp also failed to develop in detail the roles and responsibility of project management. Project management practices exhibited several gaps from best practices, including not establishing accountability for specific project management activities, failure to perform and document oversight on a recurring basis, inconsistently documenting the matching of system requirements to development activities, a lack of project plan milestones, and missing analysis of additional funding requests. This lack of specific oversight activity precluded project management from identifying missing system functionality and cost overruns early in the development cycle. Early remediation efforts are more cost-effective, as rework efforts are minimized.

The Project Manager did not identify the ramifications of the deployment of OFORS in six dissimilar operating environments until late in the Testing Phase. Project management did not complete initial security testing because they did not identify testing methods and assign adequate time and resources to complete security testing in all six environments. Testing identified four different operating system versions with varying levels of security patching for OFORS without security testing completed prior to our audit. Similarly, project management encountered delays in deploying OFORS in different operating environments. Project management had not identified the resources and skill sets necessary to customize OFORS for each operating environment. Initial plans scheduled completion of the OFORS development in September 2012, but multiple delays and non-performance by the contractor resulted in numerous contract modifications, including a change in the contract type in May 2013 from Time and Materials to Firm Fixed Price. Finally, because the contractor had not delivered key functionality, a cure notice was issued in June 2016, which resulted in an agreement to provide all development functionality by December 2017.

Additionally, the vendor's contracts did not contain technical requirements, specific deliverables, and timelines to support program and project management oversight. These missing elements amplified the issues resulting from no specific project management procedures (i.e., the specific contractor deliverables necessary to complete project management tasks).

Significant challenges identified in the OFORS program audit include:

Program Management at the Service Unit Level

- Library Services failed to develop service unit-level policies and procedures to establish stakeholder accountability and clearly define required program and cost management activities including:
  - Development and tracking of a PMP
  - Project budget approval processes
  - Regularly scheduled project budget reporting
  - Cost variance analysis
  - Accountability for project contractor oversight
  - Tracking of corrective actions.

- Library Services did not conduct periodic service unit management reviews of project progress, variances, and development breakdowns. As a result, Library Services was unable to make assessments to continue, alter, or cease project development.

- Additionally, there was no evidence of service unit management reporting to Library management on capital project development.

Project Management at the Functional Level (Development Activity)

- The OFORS project did not have a thorough project management framework to ensure all phases of the development project are thoroughly planned and executed (i.e., Planning, Analysis, Design, Deployment, and Maintenance).

- There was no evidence of a comprehensive Project Management Plan (PMP) to define how the project is to be executed, monitored, and controlled, which would enable accurate reporting, planning, and project adjustments. Additionally, project managers did not build a Risk Management Plan and Risk Register, therefore, they were unable to identify and recognize potential events or conditions (risks) which could negatively effect one or more project objectives, such as scope, schedule, cost, and quality.

- Project management did not effectively track scope and schedule changes to closure. Additionally, project managers failed to document departures from the planned project schedule (with associated justification) in the project log, resulting in numerous and significant scope changes affecting the schedule and increasing the overall cost of the project.

- Project managers did not create a concept proposal or PMP to capture all human capital requirements. As a result, OvOp management could not match the necessary human capital to project needs or properly assign roles/responsibilities, reporting relationships, availability, etc.

- There was no evidence of a standardized Requirements Management Plan used to elicit, document, and track development requirements; therefore:
  - The project team defined its own method for establishing and documenting requirements in multiple documents, formats, and locations, limiting clarity and enhancing risk of delays and extra expense of adding functionality later in development
  - The project management team did not have a standardized process to validate technical requirements and verify whether stakeholder needs were fully defined and implemented, causing scope changes across the project
  - The project management team was unable to fully define requirements in supporting vendor contracts (See **Contracts Issues**).

- OFORS did not have an observable system requirements baseline providing a defined, confirmed, and validated set of system requirements needed to ensure user needs were met. Accordingly, OFORS project managers were unable to verify that system requirements were appropriate for unique operating enviornments (six different locations).

- There was no evidence of a System Development Plan or "blueprint" for OFORS which defines development methodologies and work standards. Without a solid System Development Plan as a reference, project managers were unaware of how contractors were constructing the system (i.e., coding standards, testing schedules, and tools used) and could not validate if the system was built using industry-acceptable standards. Furthermore, without this reference document, the project management team could not properly monitor the development, testing, deployment, and verification of software in the operational environment, creating a dependency of the government on the vendor for support.

- There was no evidence of change management processes to receive, analyze, and validate proposed system changes before implementation and avoid unnecessary or potentially harmful changes to the system. Additionally, there was no evidence to support that system changes made were verified for accuracy and compliance with operational and security requirements.

Contract Issues

- The following key contracting elements were not present to establish vendor accountability for the OFORS project:
  - Requirements for project management best practices, customer oversight, and acceptance
  - Technical requirement details to ensure user functionality
  - Contractor deliverable details (e.g., software source code, programmer's documentation)
  - Vendor oversight requirements
  - Interim and final review criteria (e.g., milestones and expectations for development at those milestones)
  - Clearly defined technical framework, resulting in the inability to match technical requirements to deliverables.

Security Issues

- There were inadequate system access control policies and procedures in place for OFORS. LOC management failed to finalized and approve account management and system monitoring control procedures affecting the six overseas OFORS implementations. This resulted in the following:
  - Users being granted system access prior to formal approval
  - Privileged users with system access without the required documentation
  - No procedures to recertify privileged users
  - Sixty-nine user accounts, inactive for over 30 days, were not disabled
  - No application audit logging functionality or review of server or network logs for privileged user activity.

- LOC management did not implement adequate Security Assessment procedures for OFORs. Specifically, the Security Program Manager did not prepare the Security Control Assessment documentation, the Security Control Assessor did not produce a Security Assessment Report, and LOC management did not approve the Security Assessment Plan for OFORS.

- OFORS program management did not implement adequate Configuration Management (CM) procedures:
  - LOC management did not finalize and approve OFORS's CM Plan
  - The System Owner did not clearly map changes to OFORS to the Test Plan
  - Security impact assessments of proposed changes were not accomplished prior to change implementation
  - There was no documentation of Supervisory or management review and approval for the OFORS releases prior to being put into production.

- The OFORS System Security Plan (SSP) was not fully developed:
  - The System Owner did not include documentation of the system boundary
  - The System Owner did not update SSP references and alignment with current guidance (National Institute of Standards and Technology [NIST] Special Publication [SP] 800-53, Revision [Rev.] 4 *Recommended Security Controls for Federal Information Systems and Organizations*)
  - The System Owner failed to ensure the SSP included sufficient details on implemented security controls and residual planned actions to address any weaknesses
  - The System Owner failed to include security planning updates based on results from the continuous monitoring process.

- OvOp management failed to register OFORS in the centralized IT risk management and security documentation repository.

- OFORS System Owner did not implement adequate vulnerability management and configuration management as evidenced below:
  - Of the six OFORS instances, four different Linux operating systems were identified
  - Vulnerability scanning/continuous monitoring was not completed prior to October 2016, although the "Approval to Operate" was issued in August 2014
  - The System Owner inadequately performed the initial certification and accreditation testing. System Owners are currently re-performing
  - The OFORS Contingency Plan was not finalized; it is still a draft document.

Summary of Project Results Culminating from the Above Deficiencies

1. Initial expected project completion of September 2012 extended to December 2017
2. Key user-defined functionality not provided; standard application functionality has been deployed. Development and deployment of specific modules to support and streamline LOC field office operations has not implemented

3. OvOp did not obtain specific funding for OFORS development. OvOp used the ABA and six field office appropriations to fund the project. $500,000 of original development contract of $1,700,000 remains to fund delivery of the five remaining modules. Active project management is needed to ensure the original budget is not exceeded and original planned functionality is delivered
4. Security management is not consistently documented and lacks continuous monitoring and update
5. Insecure and inconsistent system configurations.

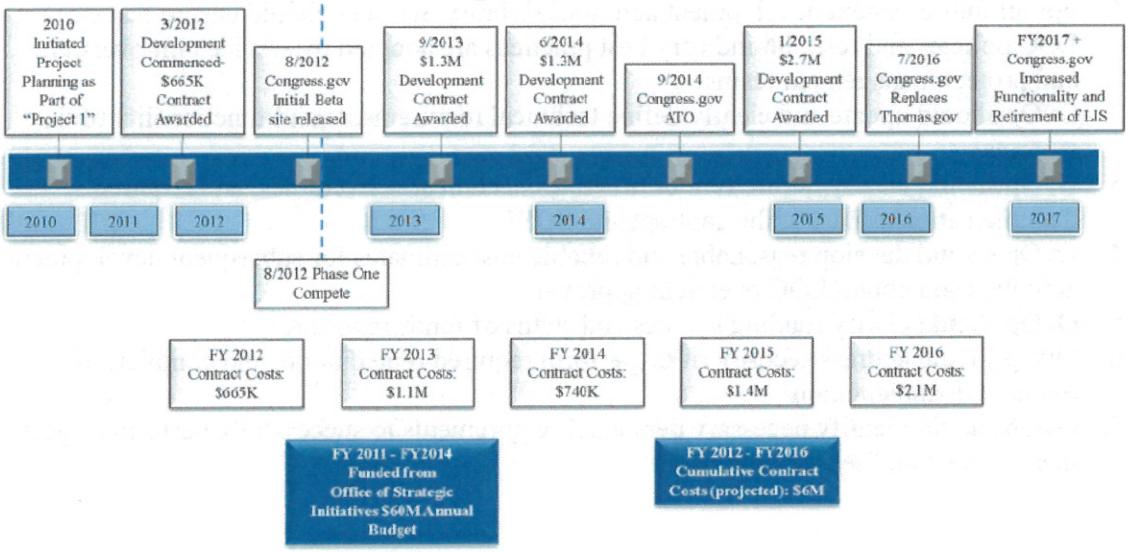
Recommendations

1. For all future system development activities, Library Services should ensure that current LOC policies and relevant industry best practices are adopted by service unit oversight and project management teams
2. OvOp should update and clearly define technical requirements and functionality of the systems
3. OvOp should clearly define vendor timelines, technical deliverables, and required documentation as part of the contract and SOW
4. OvOp should develop reasonable and reliable cost estimates for subsequent development activities and obtain LOC oversight approval
5. OvOp should clarify funding sources and status of funds reporting
6. OvOp should address security risks, perform required remediation, and complete all required documentation
7. OvOp should identify necessary personnel requirements to successfully perform project management and security oversight.

Congress.gov

Initiated in 2010, the development of Congress.gov sought to modernize aging legislative information platforms. Congress.gov provides current and historical information about Congress, legislation, and the legislative process. As part of a permanent program to provide service enhancements and support for this authoritative website, LOC has invested $15 million from 2012 through 2016. Currently, the system is operational with additional development planned for feature enhancements and eventual replacement of the Legislative Information System (LIS).

Exhibit 7: Congress.gov Development Timeline


2010 Initiated Project Planning as Part of "Project 1"
3/2012 Development Commenced- $665K Contract Awarded
8/2012 Congress.gov Initial Beta site released
9/2013 $1.3M Development Contract Awarded
6/2014 $1.3M Development Contract Awarded
9/2014 Congress.gov ATO
1/2015 $2.7M Development Contract Awarded
7/2016 Congress.gov Replaces Thomas.gov
FY2017 + Congress.gov Increased Functionality and Retirement of LIS
2010
2011
2012
2013
2014
2015
2016
2017
8/2012 Phase One Compete
FY 2012 Contract Costs: $665K
FY 2013 Contract Costs: $1.1M
FY 2014 Contract Costs: $740K
FY 2015 Contract Costs: $1.4M
FY 2016 Contract Costs: $2.1M
FY 2011 - FY2014 Funded from Office of Strategic Initiatives $60M Annual Budget
FY 2012 - FY2016 Cumulative Contract Costs (projected): $6M

The LOC OCIO develops policies and procedures governing system development consistent with many best practices. The Office of Web Services within OCIO was able to comply with the policy using a recognized development method that stresses a quick iterative approach to challenges, while reducing the volume of project documentation. OCIO maintains Congress.gov in its hosting environment. OCIO's IT Security Group (ITSG) identified hosting environment security vulnerabilities through scans; currently, OCIO ITSG is in the process of determining if these vulnerabilities impact Congress.gov.

LOC reported in the Management Discussion and Analysis (MD&A) section of its annual financial report that Congress.gov's development progress against annual objectives from FY 2012 to 2016. Below is a summary of LOC's discussion of Congress.gov's progress. These discussions are consistent with Congress.gov's development efforts and on-time Phase I delivery.

Exhibit 8: Congress.gov MD&A Discussion Summary

FY	Objective	Accomplishment
2012	LOC initiates development of next generation legislative information system platform	LOC's multi-department team successfully accomplished initial release of beta.congress.gov
2012	LOC's web presence based on new architecture has been built and tested	Congressional web presence culminated in the release of beta.congress.gov
2012	LOC has developed and implemented plans for improving user online experience and access	Web metrics policies and Key Performance Indicators were implemented in the releases of beta.congress.gov
2012	Launch Law.gov with guidelines for proofs of concepts and best practices standards	Congress.gov Beta, a mobile friendly system for legislative materials, was successfully launched on September 19, 2012
2013	LOC has completed development of next generation legislative information system platform and services	Users of Congress.gov have more effective access to growing body of legislative content, including legislation post-1993, Congressional Record post-1995, Committee reports post-1995, and enhanced search functions
2013	Legacy content has been migrated to new web presence	Congress.gov has expanded with additions of legislation, Congressional Record, and Committee reports.
2014	Complete the planned web design and development tasks related to Congress.gov	All planned design and development tasks completed with five major releases
2015	Complete the planned web design and development tasks related to Congress.gov	All planned design and development tasks completed with six major releases
2016	Complete the planned web design and development tasks related to Congress.gov	Congress.gov continues to be enhanced to replace Library Information Service and Congress.gov replaced THOMAS

Program Management at the Service unit Level

- There were no significant findings in this audit area.

Project Management at the Functional Level

- There were no significant findings in this audit area.

Contract Issues

- There were no significant findings in this audit area.

Security Issues

- The System Owner failed to fully document the Congress.gov SSP:
  - System interconnections were not identified
  - The SSP references and tests controls are consistent with outdated guidance
  - The SSP is missing details regarding implemented security controls and any residual actions planned to address remaining weaknesses
  - Security planning lacks updates based on results from the continuous monitoring process.

- The System Owner failed to register Congress.gov in the centralized IT risk management and security documentation repository

- There were inadequate Security Assessment procedures:
  - The Information Systems Security Officer (ISSO) did not retain a Congress.gov Security Assessment Plan
  - The ISSO failed to document planned remedial actions in the 10 sampled Plan of Action and Milestones (POA&M) items
  - The ISSO failed to attach evidence to support one closed POA&M.

- Inadequate System Access control policy and procedures:
  - The System Owner did not ensure procedures for account management and monitoring controls for Congress.gov were finalized and approved
  - The ISSO failed to recertify privileged users (i.e., administrators who manage applications, database servers, and other hardware) access during FY 2016

- Inadequate Configuration Management documentation:
  - The System Owner failed to develop and maintain a CM Plan specific to Congress.gov and did not detail configuration items to be managed by the CM Plan
  - The System Owner failed to complete security impact assessments prior to updated Congress.gov versions being released to production

- System security vulnerabilities not corrected in the allocated time set by LOC policies:
  - OCIO lacks automated methods to patch Linux servers in the LOC Application Hosting Environment (AHE), which hosts Congress.gov
  - OCIO failed to remediate over 40% of vulnerabilities present on the AHE servers for over 90 days.

Summary of Project Results Culminating from the Above Deficiencies

1. Project Phase I placed in service on schedule and on budget
2. Vendor is addressing Phase II requirements according to project plan
3. Security issues related primarily to documentation; some hosting environment vulnerabilities may impact Congress.gov.

Recommendations

1. OCIO should ensure that continuing development activities incorporate current LOC policies and relevant industry best practices are adopted by service unit oversight and project management teams
2. OCIO should address security issues for all operating systems and environments, develop timeliness for remediating deficiencies, and monitor progress towards resolution.

AUDIT METHODOLOGY AND SCOPE

The objective of this performance audit is to evaluate the effectiveness of LOC's system development and information security policies, programs, and practices. Kearney addressed these objectives by directing testing at LOC's project, cost, change management, and related information security policies, procedures, standards, and guidelines.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), as presented in the Government Accountability Office's (GAO) Yellow Book (2011).

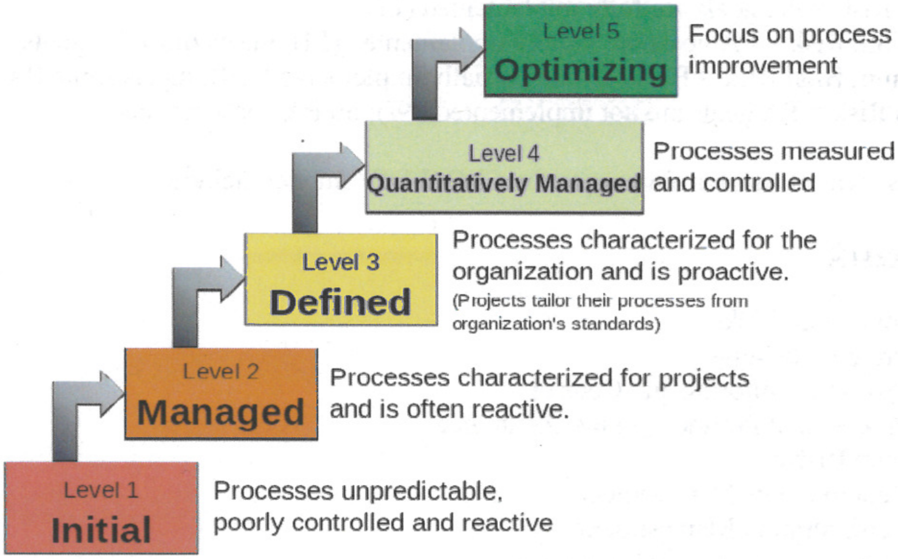
Kearney's testing approach is based upon the LOC procedures, Federal criteria, Federal best practices, and best practice methodology found in the Capability Maturity Model Integration Institute's Capability Model Maturity Integration (CMMI) process models and Project Management Institute's (PMI) Project Management Book of Knowledge (PMBoK®). These criteria include the following:

- LOC's Information Technology Security Directive (ITSDir) 01 *General Information Technology Security*, June 3, 2016
- LCR 1620, *Information Technology Security Policy of the Library of Congress*
- PMI's *A guide to the project management body of knowledge: (PMBoK® guide)*, 2013
- CMMI for Development, Guidelines for Process Integration and Product Improvement, 3rd Edition
- E-Government Act of 2002
- NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems; A Security Life Cycle Approach*
- NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix J, *Privacy Control Catalog*
- Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*
- Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Systems Development Life Cycle (SDLC) Maturity

Kearney conducted a risk assessment of LOC's system development process maturity based on CMMI for Development (CMMI-DEV) guidelines for process integration and product improvement. CMMI-DEV contains practices that cover project management, process management, software/system engineering, and other supporting processes used in development and maintenance. The practices specific to software/system development include: requirements development, technical solution, product integration, verification, and validation. Basic project management practices address the activities related to project planning, project monitoring and control, requirements management, risk management, integrated project management, and supplier agreement management. Support process areas focus on activities that support product development and maintenance. These include process and product quality assurance, configuration management, measurement and analysis, and decision analysis and resolution. CMMI capability maturity levels are used in CMMI-DEV to describe a progressive maturity path for an organization that seeks to improve its processes for software/system development. There are five maturity levels in CMMI-DEV model:

Exhibit 9: Characteristics of the Maturity Levels


Level 5
Optimizing
Focus on process improvement
Level 4
Quantitatively Managed
Processes measured and controlled
Level 3
Defined
Processes characterized for the organization and is proactive.
(Projects tailor their processes from organization's standards)
Level 2
Managed
Processes characterized for projects and is often reactive.
Level 1
Initial
Processes unpredictable, poorly controlled and reactive

- Maturity Level 1 (Initial) – Processes are considered performed but do not follow specific organization policy or a defined set of standard processes
- Maturity Level 2 (Managed) – Requires that an organization has policies in place that mandate the use of a specific process
- Maturity Level 3 (Defined) – Requires that standard processes for each process exist at the organization level and can be tailored for use to meet specific project needs. The goal is to have standard defined processes that are applied consistently across the organization
- Maturity Levels 4 (Quantitatively Managed) and 5 (Optimizing) – Are considered "high-maturity" process areas that focus on improving processes already in use through statistical and other quantitative methods.

The mapping of processes to process areas enables an organization to assess and track its progress against the CMMI-DEV model, as well as plan for process improvements over time. For this audit, Kearney assessed LOC processes for alignment with the following CMMI Maturity

- Level 2 and Level 3 Process Areas (PA):
  - Maturity Level 2 – Requirements Management (RM), Project Planning (PP), Project Monitoring and Control (PMC), Supplier Agreement Management (SAM), and Process and Product Quality Assurance (PPQA)

- Maturity Level 3 – Requirements Development (RD), Technical Solution (TS), Product Integration (PI), Verification, Validation, Integrated Project Management, and Risk Management.

Kearney assessed LOC processes across three systems: eLi, OFORS, and Congress.gov. We assessed each system individually, then summarized the risks to indicate the overall risks of LOC's alignment with the CMMI-DEV maturity model. Risks are identified as follows:

- Low Risk = PA goals are fully implemented (FI)
- Medium Risk = PA goals are largely implemented (LI); meets most PA goals
- Medium High Risk = PA goals are partially implemented (PI); meets some PA goals
- High Risk = PA goals are not implemented (NI); no PA goals are met.

LOC process areas at risk for aligning to the CMMI-DEV model include:

Maturity Level 2

- Medium High Risks:
  - Project Planning
  - Project Monitoring and Control
  - Process and Product Quality Assurance
- Medium Risks:
  - Requirements Management
  - Configuration Management
  - Supplier Agreement Management.

Maturity Level 3

- Medium High Risks:
  - Validation
  - Integrated Project Management
  - Risk Management
- Medium Risks:
  - Requirements Development
  - Technical Solution
  - Product Integration
  - Verification.

The following list includes the status of PAs in Maturity Model Levels 2 and 3 as discussed above, and depicted in the chart below:

- F1 – Low risk, PA goals are fully implemented
- LI – Medium risk, PA goals are largely implemented and meet most PA goals
- PI – Medium high risk, PA goals are partially implemented and meet some PA goals
- NI – High Risk, PA goals are not implemented and no PA goals addressed.

The assessment indicates that Congress.gov had successfully addressed Levels 2 and 3 PA risks; therefore, the process is organized and proactively addresses risks. The assessment also indicates that eLi and OFORS had not successfully addressed Levels 2 and 3 PA risks; therefore, the process is unpredictable, poorly controlled, and reactive.

Exhibit 10: CMMI Assessment by System

CMMI Level 2 Process Area	eLi	OFORS	Congress.gov
Project Planning	PI	PI	FI
Project Monitoring and Control	PI	PI	FI
Process and Product QA	PI	PI	FI
Requirements Management	PI	LI	LI
Configuration Management	LI	LI	FI
Supplier Agreement Management	LI	LI	FI
Validation	PI	PI	FI
Integrated Project Management	PI	LI	FI
Risk Management	PI	PI	FI
Requirements Development	LI	LI	LI
Technical Solution	PI	LI	FI
Product Integration	LI	LI	FI
Verification	PI	LI	FI

NIST, an agency of the U.S. Department of Commerce, is an internationally recognized leader in IT security, with benchmark publications leveraged by Federal agencies and industry alike. Much of the IT security evaluation was based on NIST publications.

For the following areas for each application, Kearney:

- Assessed LOC's application development and IT delivery methods against existing LOC policy requirements and CMMI best practices
- Conducted a gap analysis of the system cost sufficiency analysis against CMMI and PMI best practices
- Assessed the design, development, and implementation of the application/systems project management practices
- Assessed whether project deliverables met objectives and functionality defined in design documents
- Conducted a gap analysis of LOC security procedures and against industry best practices
- Evaluated security and privacy controls based on NIST SP 800-53 best practices
- Evaluated access controls effectiveness in limiting and/or detecting inappropriate access.

APPENDIX A: DETAILED AUDIT FINDINGS

During the course of the performance audit, Kearney evaluated program elements using the criteria listed above, along with industry best practices. As deficiencies were identified, Kearney used a "Notification of Findings and Recommendations (NFR)" process to highlight the Background (relevant and/or historical information), Condition (the specific deficiency), Criteria (laws, legislation, and standards we measured against), and Effect (the result) that the deficiency creates, along with Recommendations for corrective actions.

These NFRs are generated by the audit team, evaluated by the OIG, and reviewed with the auditee for factual accuracy before formal release. The following sections describe the detailed findings/issues we identified in our performance audit.

Detailed Audit Findings – eLi

1.1.1 Requirements Definition Improvements

Condition: The eLi project is not using a standardized process or format for eliciting, documenting, or tracking development requirements. There are multiple different versions, formats, and levels of detail used in the documentation and tracking of system requirements.

The process of developing customer requirements into detailed product requirements is critical to ensuring customers' high-level needs are understood to the level needed to correctly implement new functionality that meets these needs.

The later in the process that requirements and changes are uncovered, the more expensive they are to fix, as it increases the amount of rework and time required to fulfill the customer requirements.

Effect: The eLi project was unable to demonstrate a repeatable or provable process that standardizes the requirements definition tasks needed to elicit, analyze, or establish requirements based on the customer's need. The information, where it exists, is contained in multiple documents and locations, and it does not provide a comprehensive, consolidated picture for a point in time. This has resulted in the inability of the USCO and contractors to:

- Confirm that the stakeholder requirements have been captured and delineated into detailed requirements
- Confirm that the functionality built meets the requirements
- Validate/verify the functionality during Testing and Acceptance Phases
- Have a single managed source for tracking the development of requirements.

The process of developing customer requirements into detailed product requirements is critical to ensuring customers' high-level needs are understood to the level needed to correctly implement new functionality that meets these needs. Through analysis, any additional requirements, interactions, and rules become apparent, which may not otherwise be found until after the incorrect product has been developed. The later in the process that requirements and changes are uncovered, the more expensive they are to fix, as it increases the amount of rework and time required to fulfill the customer requirements.

1.2.1 Source Control Configuration Management Improvements

Condition: The USCO does not require software vendors to conform to a well-defined process for managing and versioning the source control of the systems they have been contracted to build. The USCO has not established best practices, in accordance with the CMMI Configuration Management (CM) process area, for management and versioning of the source code for eLi.

The USCO eLi project management staff are aware that the contracted vendor performs fundamental program source code control, but they do not know the level of controls or compliance with best practices the source code library is achieving. Since minimum compliance expectations are not provided to vendors, the USCO is left unsure whether the developer is following industry best practices in the storage and management of the software, which the USCO will own at the end of the development contract.

Below, we noted examples of inconsistencies in source control and CM best practices.

To assess whether formal CM practices were implemented in accordance with CMMI best practices detailed above, Kearney reviewed several documents provided and noted that the eLi contractor uses Subversion software versioning tool for source control. However, we did not discover any documentation that explains *how* Subversion is used to manage source control. For example:

- What the branching (software code version control) strategy is
- How rollbacks to prior software code versions can occur
- Whether change sets (e.g., patches addressing multiple areas of the application code) are always tied to tickets (authorized requests).

Kearney provided a questionnaire to the eLi developers to gain more in-depth information about source code library practices used for the project. When asked about the branching strategy, the USCO stated: "To the best of our knowledge, in looking at the code repository, it doesn't appear that there was a strategy."

Because the source code library control process was never documented and provided to LOC, there is an unknown level of assurance that the software asset developed for the USCO has been stored in a manner that allows traceability back to functionality requirements. Lack of such information will hinder future alternate vendor or in-house abilities to support or alter the software code.

Kearney assessed the status of CM processes performed by the USCO in the "eLi Security Assessment Report (SAR)," dated January 24, 2015, which confirmed that key CM processes are not formally implemented or documented. The SAR document notes:

1. **CM-02 Baseline Configuration** – There currently is not a formal eLi application CM process that develops, documents, and maintains, under configuration control, a current baseline configuration of the eLi application environments (e.g., Proof of Concept, Development, Test, Staging, Production, Shared)
2. **CM-02(01) Baseline Configuration (Review and Updates)** – There currently is not a formal eLi application CM process for reviews and updates
3. **CM-02(03) Baseline Configuration (Retention of Previous Configurations)** – There currently is not a formal eLi application CM process to develop, document, and maintain the retention of previous configurations under configuration control
4. **CM-03 Configuration Change Control** – There currently is not a formal eLi application CM and configuration change control process
5. **CM-03(02) Configuration Change Control (Test/Validate/Document Changes)** – There currently is not a formal configuration change control process to test/validate/ document changes
6. **CM-09 Configuration Management Plan** – There currently is not a formal eLi application CM Plan.

In our review of the Requirements Traceability Matrix (RTM) documents, we noted that there does not appear to be any documentation that relates requirements to source control or explains how source control should be used by the development team. The eLi system design document has a section devoted to source control, which states:

> "Software AG Designer and webMethods Developer enable you to create, maintain, and manage custom integration packages for use by webMethods Integration Server. Often, many enterprise organizations employ a version control system (VCS) for the development of software solutions, providing automatic auditing, versioning, and security to software development projects.
>
> For eLi project Subversion 1.6 will be used as version control system."

Guidelines or requirements for how Subversion is to be used are not mentioned.

Kearney also noted that the documentation provided indicates that there is no documented baseline.

Effect: The following list describes the effects of the findings stated in this NFR:

1. Because the source control process is not documented, if there *is* any kind of traceability from requirements back to source code, the USCO is unaware of it. It is possible that eLi contractors are following best practices and could easily trace a requirement back to all

the change-sets that make up that requirement, but the USCO is not aware whether this is happening or not. Without this information:

a. It can be extremely difficult to deploy specific features or choose *not* to deploy those features
b. It is difficult to understand the history of source code and why a change was made
c. There is no guarantee that there is a documented reason for a change. If changes are required to be associated to requirements/bugs within the source control system, then each change is something that is ultimately within the purview of the USCO and not a change that a developer might complete on their own initiative
d. It becomes more difficult to gauge how complex a feature was to implement
e. It becomes more difficult to gauge how long a requirement took to implement (level of effort, costs)

2. It is not possible for the USCO to monitor and confirm that the CM processes are being followed
3. USCO has no insight into whether the vendor's Standard Operating Procedures (SOP), if they exist, are in accordance with LOC's SDLC process
4. Without documented baselines, software rollbacks may not be successful. Subversion *is* being used in the case of eLi; thus, rolling back to different versions of the software is possible, but the SOPs for accomplishing this process are not currently within the purview of the USCO
5. It is unknown whether any version of the software could be identified as a "baseline"
6. It is unknown whether questions could be answered, such as:

a. What were the implemented requirements during the last release and what are they during this release? From several of the eLi test documents, we noted that many bugs were listed as "FAIL-no change." This could be attributable to deploying the wrong version of the code because a proper version control branching system does not exist
b. Did this functionality work during the last release? Can we deploy that version and test it out?
c. What is every code change that has ever been associated to this requirement? Who wrote the code? Who reviewed it?

Overall, there is a risk that, in the event that the USCO replaces the original vendor, a replacement vendor cannot access the source code in a workable, organized manner (e.g., the code and the controls placed on it in Subversion [code library system] fully port over to the next vendor).

1.3.1 Design and Analysis of Alternative Improvements

Condition: The USCO did not have established policies and requirements to assure that an Analysis of Alternatives (AoA) is formally documented during the Technical Analysis, Design, and Architecture Phases of its SDLC. The absence of a proper AoA and an explanation of *why* a certain design is required can lead to overly complicated designs that may ultimately cause significant project delays, increased costs, and, in some cases, project failures. For the eLi project, we did not observe evidence that an AoA was performed during the Design Phase.

Below, we noted examples of inconsistencies in processes used for the design and analysis of alternative solutions when compared with CMMI best practices for Technical Solutions.

In the design documents provided, we did not observe any discussion of how alternatives were evaluated or how solutions were weighted against each other. For example, the webMethods Business Process Modeling tool suite was chosen as a Commercial Off-the-Shelf (COTS) product for eLi because it was expected that a significant amount of functionality would be available out of the box. However, there is no discussion about how determinations were made that a certain feature or functionality should be custom software development versus configuring webMethods components. None of the documents reviewed explored the idea that it might take more time to customize or configure webMethods versus creating a brand new component or using a different component to interface with webMethods. Additionally, the decision to build part of the system using webMethods and other parts of the system using custom development code (e.g., .NET or Java) came years after the start of the project. This exposed the USCO to time and costs associated with significantly re-addressing requirements to alternative solutions.

According to the COTS Selection Criteria Evaluation Worksheet completed in 2011 as part of the technical proposal by the selected contractor, zero customization was to be required for webMethods. That is, 100% of the functionality required by eLi was either considered "out of the box" or "configurable." Zero requirements were considered either "not met" or "need[ing] customization." Nevertheless, at some point during the development life cycle, it became evident that webMethods could not support the entire eLi system with zero customization. Kearney reviewed the documents provided as part of project management, system design, and system development documentation, but we could find no indication that the design team undertook the task of establishing criteria to help them determine the best course of action (e.g., customize, configure, reuse, build) for each requirement of the system.

A significant aspect that is not addressed in any solutions documentation we reviewed is the justification for provisioning the massive amount of infrastructure they built. According to the eLi SAR,[3] dated December 10, 2014, over 100 servers were originally proposed for eLi. This number was spread over five environments: Proof of Concept, Development, Test, Pre-Production, and Production. Averaging 20 servers per environment for an application that is expected to process 3,300 applications every six months appears to be an astonishing amount of computing power. For comparison, StackOverflow.com, one of the top 50 most popular sites on the internet, uses around 25 servers. StackOverflow.com receives roughly 66 million page loads *per day*. Additionally, for comparison purposes, Congress.gov has approximately 100 servers, including the backup recovery site. Ultimately, the number of servers for eLi was reduced to 46. Excluding the database servers in each environment, there remained nine servers used for production. That number still appears to be *significantly* higher than necessary for the amount of traffic eLi is expected to serve. In the eLi SAR the contracted developer noted that "there were possibilities that each of the nine servers/services for each environment did not have to reside on a separate physical server, resulting in less than nine physical servers required per environment." This being the case, and without decision analysis documentation, it is not clear why this multi-

[3] eLi Assessment Project Final eLi System Assessment Report Draft, December 10, 2014

server design was left in place. Traffic engineering or simulated "load" testing would provide a realistic estimate of the processing platforms required to support the application and users access. According to eLi management's response to Kearney's questionnaire, "[the] USCO doesn't believe that *any* load testing was done since the application was still in the development phase," which once again raises the question as to why the amount of servers in the design was considered necessary.

Kearney was not able to interview the vendor team to inquire why their documentation did not reflect the rationale for the initial number of proposed servers.

Again, we would note that for a system to have a design as complex as the one that was ultimately adopted for eLi, it should be expected that the design analysis documents justify why that amount of complexity is required.

Effect: The lack of a proper AoA and an explanation of why a certain design is required can lead to overly complicated designs that can ultimately cause significant project delays, increased costs, and, in some cases, project failures.

The fact that the document had to be completely rewritten is indicative of the complexity of the design proposed by the original contractors. With as complicated as the design and installation guides are, it is not surprising that the eLi SAR completed on December 10, 2014 states: "once [the developer] gets the go ahead to proceed, the remaining environments could be brought on-line within several months."

1.4.1 Development Phase Improvements

Condition: The USCO does not have adequate policies and procedures, as defined in the Project Management Life Cycle (PMLC) and SDLC guidance, for conducting oversight and monitoring of the Development Phase processes and practices of its contractors. Although the PMLC and SDLC include planning for and monitoring Development Phase activities, there is no specific language to require "flowdown" of the PMLC and SDLC processes to contractors performing development work for the USCO, nor guidance for USCO staff to monitor contractor adherence to LOC's PMLC and SDLC.

Monitoring of contractor's work is primarily tied to contract deliverables (end product) approvals via coordination between Project Managers and the COR. However, on the eLi project, there is a lack of oversight and knowledge of internal development methodologies of the software development contractor, including coding standards and procedures. Based on our inquiries and assessment of the Copyright eLi project team, there is little information known about how the contractors are developing code for systems and what practices they are following.

Below, Kearney noted examples of inconsistencies in processes used for the development and coding practices when compared with CMMI development best practices in Technical Solution processes.

Kearney requested documentation from the eLi project team intended to encompass "system development methodologies and work environment standards for eLi to include: development environment standards and tools, coding standards and procedures." Based on the documentation provided by the eLi project team, we were unable to confirm that the tools, standards, and procedures were in accordance with the standards required by the USCO's SDLC practice, as that level of detail was not maintained and monitored by the USCO eLi project team.

Specifically, the documentation provided does not contain information necessary to properly assess whether the vendor was following a proper SDLC. For example:

- What are the coding standards?
- Are there peer reviews of custom code?
- Are unit tests required?
- How often are tests run?
- Are tests automated to run upon check-in?
- Is there a Continuous Integration (CI)/Continuous Development (CD) pipeline?
- What tools are used by the development team?
- How is branching and merging of code done? For example, is it possible to work on bug fixes in the current production release, while simultaneously working on new features intended for the same release?
- Can a version of the code be deployed from any point in time?

Kearney was told that the information to answer the questions above was not provided to the USCO by the contractor. Without this information, the USCO cannot confirm whether LOC SDLC practices are being followed by the vendor. In response to our questionnaire, eLi management in the USCO noted: "Since development was outsourced to the contractor, the USCO is unaware of what toolsets were utilized for development, compiling, and deployment. Since these items were not fully specified within the software Architecture Design Document (ADD), we assume that there was no automated build and deployment."

Kearney reviewed the eLi SAR[4] and noted the following consistent responses from Copyright eLi project team members recorded in that assessment:

- "Copyright Technology Office (CTO) is not aware of any existing unit test data, but it is assumed that unit tests were run. However, unit test reports were not specified as deliverables"
- "To the best of our knowledge, coding standards were neither defined *(at acquisition)* nor used on this project"
- "Since development was outsourced to the contractor, United States Copyright Office (USCO) is unaware of any existing development guides. None were provided as Government Furnished Information (GFI)"
- "Since development was outsourced to the contractor, USCO is unaware of any code reviews that were held. The software was a straight deliverable."

[4] Project Final eLi SAR Draft, dated December 10, 2014, developed by vCentra

Because the USCO does not have insight into the methods and practices used to develop eLi, it cannot have confidence that the software is built in a manner that is robust, well-tested, and easily maintainable. Additionally, software that follows development best practices (e.g., consistent unit testing, automated deployments, and continuous integration) ultimately saves significant time and money over software that is not developed using these practices.

Effect: The USCO is not able to confirm that its SDLC and the best practices outlined in the CMMI sub-practices are being followed by the vendor.

The effects and benefits of following best practices in software development have recently gained attention in the Federal Government. The Government has recently acknowledged that the processes within the Implementation Phase are critical for successful software. The activities within the Implementation Phase (or lack thereof/failure) determine the overall success of the project. The United States Digital Services Playbook (https://playbook.cio.gov/) reflects this fact by focusing no less than eight of its 13 "plays" on the Development/Implementation Phase of software.

Projects not following modern development best practices will result in:

- More bugs
- Significantly longer development times
- Difficult to maintain/fragile code bases
- More system downtime
- A system that is more expensive to maintain
- A system that performs poorly under load
- Difficulty in finding developers to maintain the system due to unconventional implementations.

1.5.1 Deployment and Operations Improvements

Condition: The USCO does not have adequate policies and procedures defined for deployment and operations or requirements defined in the contract and SOW, requiring contractors to provide detailed documentation explaining how custom software is deployed or how COTS products are integrated with custom components. In some cases, there is almost no information known about how the contractors are deploying, testing, and verifying the software deployed into an environment. Policies, contracts, and SOWs should specify that contractors provide a detailed deployment guide describing how changes are tested and deployed, as well as an installation guide explaining how to perform the customizations.

Below, Kearney noted examples of incomplete processes, including lack of documentation explaining procedures and processes related to testing and verifying deployed software and procedures for performing customizations.

We reviewed the contractor's system development testing procedures and noted that there are checklists, smoke tests (tests run to verify that an application's main features work properly before proceeding with more rigorous testing), and automated tests that are provided to ensure that an environment has been correctly configured. We did not observe, however, any documentation that explains how new code is deployed into an existing environment. Kearney also did not observe evidence that any kind of automated build, continuous integration, or continuous deployment system is in place.

Automating the deployment process has several important benefits, including:

- Significant cost and time savings. For complicated deployments, manual processes can take several hours. Automated deployments completely eliminate this cost
- The process is completely repeatable and immune to human error. This gives the team assurance that deployments will succeed in any environment and eliminates the cause of common production issues: forgetting to perform one or more deployment steps
- The knowledge of deployment is not limited to a few individuals. When deployments are automated, anyone on the team can perform deployments, as opposed to manual deployments, which are generally performed by one individual. If this individual leaves the team or is unavailable, the other team members have to learn the process, which costs significant time and money.

The eLi Test and Evaluation Master Plan explains that the development team:

- "Designs, develops, and updates the webMethods and Data Pro components
- Performs 'smoke' testing in the development environment prior to updating the testing environment
- Performs system testing for webMethods and Data Pro components
- Documents and resolves problems found during testing
- Reviews resolution entries in the test report."

The contract development team did not adequately correct, track, and communicate remediation of faulty code identified by Copyright acceptance testing. Kearney noted that test results for Contract Line Item Numbers (CLIN) 3 and 4 contain large numbers of test cases that are marked as "FAIL-no change." CLIN 3 had a 96% fail rate and CLIN 4 had a 74% fail rate.

This indicates that either: 1) bugs are not being properly resolved; 2) bug fixes are not being properly deployed to the test environment; 3) bug fixes that are actually being deployed to the test environment were not being communicated to the acceptance testing team; or 4) developers improperly managed source code library modules and builds.

Deficiencies in the software deployment processes (as evidenced by a high code failure rate) will result in additional costs and time necessary to complete the project.

Effect: The USCO is not able to confirm that the contractor is following internal best practices for product integration and deployment in accordance with the LOC SDLC Implementation Phase. In addition, the process of deployment was performed manually, which is costly, time-consuming, and more error-prone. Best practices recommend an automated CI/CD, which is less labor-intensive and results in fewer errors. Finally, the large number of "FAIL-no change" seems to indicate that deployments are failing to include all the bug fixes meant for a new deployment.

1.6.1 IT Governance Improvements

Condition: The USCO did not verify and monitor contracted system development work for alignment with LOC OCIO governance for project management and system development processes being performed by contracted development firms.

The USCO's eLi PMP, dated August 14, 2014, provided guidelines "to ensure alignment with the Project Management Institute's Project Management Body of Knowledge (PMI's PMBoK®) and the Library of Congress System Development Lifecycle (LoC SDLC) requirements." The PMP included project management guidance that aligned with the PMLC and deliverables aligned with the LOC SDLC. However, the eLi project team did not perform effective monitoring of contractor execution against the LOC SDLC, including:

- The USCO did not require or approve the contractor's SDLC practices to ensure alignment with the LOC SDLC
- The project management team did not proactively monitor the development contractor's execution to these standards, as evidenced by the project's lack of knowledge of the contractor's development practices.

Kearney observed an absence of requirements in contracts and SOWs for development contractors to adhere to SDLC practices and produce specified deliverables, as follows:

> "There is no mention of a requirement to adhere to an SDLC in the original contract for implementation of a configured version of webMethods, which is a COTS product, requiring extensive configuration. The omission of requiring contractor development work to be conducted in a structured, professional manner could lead to late or non-delivery of software products, or provide a contractor with lower cost options to deliver software, resulting in higher failure and non-compliance rates."

Effect: The lack of mature IT governance and monitoring processes leads to an inconsistent application of project standards and controls, causing potential issues with quality software development and implementation.

An absence of development standards may affect delivery of fully defined and properly implemented stakeholder requirements.

A lack of systems development governance oversight can result in inconsistencies with quality and standards of deliverables leading to cost overruns and missed project milestones.

1.10.1 USCO Project Oversight Policies

Condition: The USCO's project cost management procedures do not include effective cost monitoring and controls, including reporting and analyzing cost variances and their causes, as well as tracking corrective actions for IT investments. Cost tracking information was observed in multiple formats with varying levels of detail, but no evidence was provided of project cost monitoring and analysis of cost variances and corrective actions.

Below, we noted examples of inconsistencies in project cost management, including tracking, reporting, and analyzing cost variances, as well as managing corrective actions.

The USCO's cost information for eLi was available in various formats, including General Ledger postings, draft budget estimates, and total project costs by vendor. We did not observe life cycle analysis of variances of projected costs versus actual, including corrective actions. Without the cost analysis, variance explanations were not included in any cost information provided. Below, we detail cost information provided from various sources:

Exhibit 11: eLi Observed Funding and Costs

Funding Details	Costs
2010 Original funding (Copyright Licensing Division Congressional Budget Request)	$1,100,000
2011 Additional funding request (Copyright Licensing Division Congressional Budget Request)	$790,000
2011 Total approved funding	$1,890,000
2011 Estimated Acquisition costs in General Ledger ($613,000 personnel costs and $2,014,000 contract costs)	$2,627,000
Total expenditures in General Ledger through October 13, 2016	$11,623,000

Although we observed spreadsheets showing total project costs by vendor, contract value, and amounts expended, the eLi project management team recorded its analysis inconsistently, making it difficult to determine the correlation between cost increases and SDLC phases. The USCO oversight practices did not include a strategic review and approval of project cost increase and timeline extensions. With significant cost increases, project management should have used a formal cost analysis practice, such as earned value analysis, to forecast cost to complete based on work completed versus remaining work. Using a formal estimation process and analyzing variances in the schedule and budget as the project progresses provides more accurate estimates of cost to complete. Project management could not produce a formal cost tracking process for cost tracking, variance analysis, or review of corrective actions outside thresholds.

Effect: Lack of formal project cost analysis and tracking methodology at the project level and LOC policy requiring eLi to report investment activities to OCIO has several negative effects in relation to adequately assessing LOC's project costs and risks. These include:

- eLi project management has not adopted formal cost analysis techniques for tracking and reporting estimated and actual costs
- eLi has not applied formal cost variance analysis methods, including identifying causes and tracking corrective actions
- Without regular and frequent monitoring and reporting of costs, variances, and corrective actions, there is increased risk surrounding LOC's ability to make informed and timely decisions about IT investments.

3.1.1 Project Management Scope and Schedule Improvements

Condition: eLi project management did not have adequate scope and schedule management controls in place that aligned to PMI's PMBoK® best practices.

Below, we provide evidence of these conditions:

- Project management did not effectively manage risk that impacted the project scope and schedule. The Risk Register was last updated in 2014 and contains risks impacting scope and schedule that were not mitigated and tracked to closure
- Project management did not effectively track scope and schedule issue remediation to closure. The issue log was last updated in 2014, and it does not document issues that lead to scope and schedule changes
- Project management did not effectively manage changes to the scope and schedule following PMBoK®. Project management did not document departures from the planned project schedule in the project log with an associated justification/reason. The eLi project log documents "expanded scope to include certification;" however, we did not observe change requests documenting schedule and scope changes.

Effect: Mismanaged eLi scope changes directly affected the project schedule and increased the cost of the project. As PMBoK® states, controlling the project scope ensures all requested changes and recommended corrective or preventive actions are processed through the Perform Integrated Change Control process. PMBoK® also discusses how communications, risk, and unanticipated changes can impact the schedule and/or outcome of the project.

3.3.1 Human Resource Management Improvements

Condition: USCO project management did not have adequate Human Resource management in place that aligned with PMBoK® best practices.

Below, we provide evidence of these conditions:

- Project management did not follow the plans identified in the eLi PMP to review the project at each phase end, or at least quarterly, for accuracy and compliance with project documentation and update the project plans. Kearney observed outdated Resource Management Plans and PMPs. The Resource Management Plan was last updated in 2013 and the PMP was last updated in 2014

- Project management did not follow the PMBoK® guidance to document a plan for adjusting resources during the project Closeout Phase. As a result, it is unclear whether excessive or sufficient resources are assigned to complete closeout tasks.

Effect: If project team members do not possess required competencies and proper training is not provided to new resources, performance and success of the project can be jeopardized. When resource mismatches and changes are identified, proactive responses, such as training, hiring, schedule changes, or scope changes, and documentation updates should be initiated.

USCO project costs, schedules, risks, quality, and ultimate success may be significantly affected by inadequate resource management and a misunderstanding of required roles and responsibilities.

Without effective Human Resource planning and management, staffing issues may disrupt the project team from adhering to the PMP, causing the schedule to be extended or the budget to be exceeded. Key benefits of effectively managing the project team include influencing team behavior, managing conflict, resolving issues, and appraising team member performance.

Failing to formally plan the method and timing of releasing resources from a project can significantly increase the likelihood of Human Resources risk occurring during or at the end of the project and unnecessary resource cost being charged to the project.

Inefficient resource management planning may have been a key factor in the eLi project management team failing to properly maintain project documentation, track/meet deliverables, and report on the performance and requirements of project resources.

3.4.1 Communications Management Improvements

Condition: The USCO project did not follow the LOC PMLC guidance for maintaining a PMP and Communications Management Plan. The PMP and Communications Management plan was last updated in 2014. Per the eLi PMP, "project managers will review the project at each phase end, or at least quarterly for accuracy and compliance with project documentation."

Ineffective communication creates a gap between diverse stakeholders who may have different cultural and organizational backgrounds, levels of expertise, and perspectives and interests, which may impact or have an influence upon the project execution or outcome. Timely communication among diverse project team members should be addressed in a communications management plan for items such as requirements updates, design reviews, test readiness, and project status, including risks and issues.

Effect: The USCO's lack of a requirement for eLi to follow the LOC PMLC has several negative effects with regard to eLi project management maintaining a formal documented Communications Management Plan. As stated in *Section 2.3* of the LOC PMLC, "communications, risk, and unanticipated changes can impact the schedule and/or outcome of a project and it is important to plan in advance how these changes will be addressed." PMBoK®

also discusses how ineffective communication creates a gap between diverse stakeholders who may have different cultural and organizational backgrounds, levels of expertise, and perspectives and interests, which may impact or have an influence upon the project execution or outcome. The USCO also projects that lacking a formal Communications Management Plan may lead to conflicts with suppliers and internal team members, due to miscommunication.

3.5.1 Risk and Issue Management Improvements

Condition: The eLi project team did not follow the LOC PMLC requirement to deliver and maintain a Risk Management Plan describing how project risk assessments will be structured and performed. Additionally, the eLi project team did not follow the LOC PMLC requirement to maintain a Risk Register and issue log throughout the life cycle of the project. Although a Risk Register and issue log were created early in the project, they were not maintained and updated throughout the project; the eLi project management last updated these documents in 2015 and omitted issues related to project resources. Issues and risk were identified as findings in the 2014 eLi SAR, but not acknowledged and tracked for remediation on the Risk Register/issue log. The 20150701 Updated eGB (eLi Governance Board) Meeting Notes documents the concerns/issues with resources dating back to the beginning of the project; however, these issues are not captured in the Risk Register or issue log.

Effect: The USCO's lack of requirement for eLi to follow the LOC PMLC has several negative effects with regard to eLi maintaining Risk Management Plans, issue logs, and Risk Registers. As stated in *Section 2.3* of the LOC PMLC, "communications, risk and unanticipated changes can impact the schedule and/or outcome of a project and it is important to plan in advance how these changes will be addressed." Project risk is defined as an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives (e.g., scope, schedule, cost, quality).

The Risk Management Plan documented resource shortage risks, which eventually lead to project issues. The Risk Register stated that "if resource shortages are not addressed, project timelines and/or project quality will suffer (i.e., either agree to live with greater risks due to lower quality or lengthen timeline)." The Register does not document a mitigation strategy for this risk. Ineffective risk management may have been a factor in risk and issues not being addressed in a timely and formal manner.

4.2.1 Requirements Management Improvements

Condition: The USCO does not have guidelines, policies, or standardized processes for managing requirements throughout the SDLC or ongoing support and enhancement phases. Kearney observed requirements documentation in multiple formats with varying levels of detail with limited bidirectional traceability. Additionally, we did not observe requirement baselines, meaning that they either do not exist or have not been maintained as part of the ongoing project. A requirement baseline provides a defined, confirmed, and validated set of detailed requirements at specified checkpoints throughout a project life cycle. These baselines should be used to obtain metrics to show the amount of change (and when the changes occurred) throughout the project.

The cost of a project increases exponentially depending on when project additions or changes to requirements are discovered. By tracking changes to requirements against documented baselines, the USCO is better able to determine and manage risks to project schedules and budgets.

Below, we noted examples of inconsistencies in processes used for requirements management when comparing with best practices for project management.

While there was a requirements baseline and traceability for the eLi project, this baseline document was created in 2011, and we were unable to validate that this baseline has been maintained and managed since that time. Current processes for the eLi project appear to create a new RTM for changes with new numbering and limited context of where the requirements fall in the hierarchy of the overall system. The original baseline should have been maintained as a living document with iterations for subsequent releases that resulted in new baselines over time to show how the system has matured and changed over the life of the project. Subsequent RTMs and requirements documentation do not contain the same level of detail or traceability to detailed use cases or test cases, which are critical for management and validation of the requirements. Because new RTMs are created for each change, there is no way for the USCO to evaluate when changes are to implement new functionality, revise existing functions, or remove functionality no longer required. Kearney observed many different versions of RTMs containing a limited subset of requirements without the level of detail needed to properly implement the requirements. In addition, we were unable to observe how these requirements were validated and approved (statuses) or how changes were managed throughout the development life cycle for individual releases. Without a clear and formal process for validating and approving requirements, there is no way for the USCO to ensure that the stakeholder requirements have been fully or correctly defined into detailed product requirements for development. The lack of change management also results in an inability to track and manage impacts to schedule, scope, or final deliverables.

Effect: Lack of formal policy and guidance regarding the establishment of standard processes to manage requirements throughout the complete SDLC, including ongoing maintenance enhancement releases, resulted in the following:

- Inability to effectively view and manage project requirements
- Inability to fully trace requirements throughout the development process
- Inability to effectively manage changes to existing requirements or new requirements as they are developed.

4.3.1 Requirements Validation Improvements

Condition: The USCO does not have standard guidelines, processes, or templates across programs for ensuring requirements are fully refined and updated as needed during the Validation and Design Phases. Documentation is maintained in various formats and levels of detail across and within projects.

Below, we noted examples of inconsistencies in processes used for ensuring requirements are fully captured during validation.

The use case documentation, which is necessary to prepare validation test cases by showing exactly how requirements will be implemented, does not include traceability back to originating requirements. Traceability is needed to ensure that all requirements have been accounted for and will meet stakeholder needs. Additionally, the use cases provided for review are in multiple formats and do not provide enough detail to correctly determine how the functionality gets triggered or where it fits into the overall system. The impact of this deficiency was confirmed by review of the testing and test validation documents, which show where the application does not meet the requirements and what the shortcomings are but does not show how the product was validated to arrive at these conclusions. The test plan documentation reviews show references to the RTM and design document; however, although we requested those documents for audit purposes to verify how they interfaced or whether they contained the full information to validate the product, the USCO was unable to produce them as requested. Therefore, we concluded they did not exist or the USCO did not have document control in place.

Effect: Lack of defined processes and policies to validate the requirements through detailed design (e.g., use cases, wireframes, functional design) results in the USCO being unable to verify whether stakeholder requirements have been fully defined and implemented throughout the release cycle. This lack has resulted in the inability of the USCO and contractors to:

- Validate stakeholder requirements have been captured in the detailed requirements
- Verify that the functionality built meets the requirements
- Validate/verify the functionality during the Testing and Acceptance Phases.

4.4.1 Requirements Verification Improvements

Condition: The USCO does not use LOC SDLC standard guidelines, processes, or standard templates for verifying that requirements are fully tested and implemented during the Verification Phase. Documentation is maintained in various formats and levels of detail across the project.

Below, we noted examples of inconsistencies in processes used for requirements verification when comparing with best practices for requirements management and quality assurance for the eLi system.

Documentation provided for review on the eLi project shows where the application does not meet the requirements and what the shortcomings are, but it does not show how the product was validated to arrive at these conclusions. The provided test plan references a RTM and design document; however, these associated documents were not available for review to verify how these documents work together or if they contain full information needed to validate the product. Based on responses to the auditor's questionnaire and the work products provided, we were unable to determine whether any peer reviews were conducted throughout the development life cycle.

Effect: Each program at the USCO has implemented its own formats and processes for requirements verification to differing levels of success. There is no clear way for the USCO to review individual projects against the stakeholder requirements to verify what has been implemented against the stakeholder and detailed product requirements.

Detailed Audit Findings – OFORS

1.1.2 Requirements Definition Improvements

Condition: Library Services is not using a standardized process or format for eliciting, documenting, or tracking development requirements. The stakeholder requirements are well-defined in the tickets/issues and gap analysis documentation; however, the decomposition of these into detailed product development requirements was not apparent in the specifications provided. While the stakeholder requirements trace to work items, these work items and deliverables are split out into multiple documents and formats, hindering a traceable view of the stakeholder requirements to specific required code changes and releases.

The process of developing customer requirements into detailed, traceable product development requirements is critical to ensuring that customers' high-level needs are understood to the level needed to correctly implement new functionality that meets these needs.

The later in the process that requirements and changes are discovered, the more expensive they are to fix, as it increases the amount of rework and time required to fulfill the customer requirements.

Effect: The OFORS project was unable to demonstrate a repeatable or provable process that standardizes the requirements definition tasks needed to elicit, analyze, or establish requirements based on the customer's need. The information, where it exists, is contained in multiple documents and locations and does not provide a comprehensive, consolidated picture for a point in time. This has resulted in the inability of Library Services and contractors to:

- Confirm that the stakeholder requirements have been captured and delineated into detailed requirements
- Confirm that the functionality built meets the requirements
- Validate/verify the functionality during the Testing and Acceptance Phases
- Have a single managed source for tracking the development of requirements.

The process of developing customer requirements into detailed product requirements is critical to ensuring that customer's high-level needs are understood to the level needed to correctly implement new functionality that meets these needs. Through analysis, additional requirements, interactions, and rules become apparent, which may not otherwise be found until after the incorrect product has been developed. The later in the process that requirements and changes are uncovered, the more expensive they are to fix, as it increases the amount of rework and time required to fulfill the customer requirements.

1.2.2 Source Control and Configuration Management Improvements

Condition: Library Services does not require contractors to conform to a well-defined process for managing and versioning the source control of the systems they have contracted to have built.

It is not known whether source control and, therefore, CM is being employed whatsoever. For example, the practice of code check-in/check-out procedures and branching/source code CM strategies (critical elements of version control) were only enforced for in-house development efforts. Also, there was no knowledge of development guides used by the contractor and no requirement in the contract for any type of development guide. The lack of formal CM practices (i.e., check-in and check-out procedures and branching strategies) impacts the ability to safely control changes, which poses significant risk to the ability to maintain the integrity of the code and control changes to prevent unauthorized changes

To assess whether formal CM practices were implemented in accordance with CMMI best practices detailed above, we reviewed the CM Plan which, while explaining the process for adding a change to the system, does not speak to procedures for performing the actual updates to the software. Under "Perform Update," the document simply states: "The *OFORS* Project Manager at VTLS (development contractor) will assign a responsible party to perform the system update in accordance with *VTLS* Standard Operating Procedures."

Critical elements of a CM Plan should include details about the source control system and procedures for using it, branching strategy that defines the process for integrating code, and rollback procedures for returning code to a previous version. The CM Plan did not include the following elements:

- What, if any, source control system is used
- What the branching (software code version control) strategy is
- How rollbacks to prior software code versions can occur.

Further, if the VTLS Standard Operating Procedures (SOP) are documented, it was not provided to LOC. Kearney was told that this was not any kind of official document; rather, it was just a promise from VTLS (the OFORS developer) to follow their SOPs.

The CM Plan indicates that there is a sound change control process in place when changes are reviewed, approved, and deployed. However, Kearney could not verify how baselines, or archives, could be retrieved in the case a rollback is necessary. None of the documentation we received explains how or even *if* VTLS is using source control. The CM Plan states: "If *[sic]* the *OFORS* Project Manager does not override a negative ISSO recommendation *[sic]*, the changes to the production systems must be rolled back in accordance with *OFORS* Standard Operating Procedures." The reference to rolling back changes implies that there *is* a kind of source control being used, but how that source control is used is not currently within the purview of LOC. The SOPs of VTLS were never provided to LOC.

Effect: The following list describes the effects of this finding:

1. Because the source control process is not documented, if there *is* any kind of traceability from requirements back to source control, Library Services is unaware of it. It is possible that OFORS contractors are following best practices and could easily trace a requirement back to all the change-sets that make up that requirement, but LOC is not tracking whether this is happening or not. Without this information:
   a. It can be extremely difficult to deploy specific features or to choose *not* to deploy those features
   b. It is difficult to understand the history of source code and why a change was made
   c. There is no guarantee that there is a documented reason for a change. If changes are required to be associated to requirements/bugs within the source control system, then each change is ultimately within the purview of Library Services and not a change that a developer might complete on his/her own initiative
   d. It becomes more difficult to gauge how complex a feature was to implement
   e. It becomes more difficult to gauge how long a requirement took to implement. With change-sets associated to requirements, it can offer Library Services a rough idea of how long each requirement took to implement. This information can be used to determine whether the contractor's Level of Effort (LOE) estimates are accurate or not. Combined with regular sprints in an agile SDLC, this can be an extremely effective early warning system for determining whether LOEs are significantly off base and, therefore, if the project schedule or manpower needs to be adjusted
2. It is not possible for Library Services to monitor and confirm the CM processes are being followed
3. LOC has no insight into whether the vendor's SOPs (if they exist) are in accordance with Library Service's SDLC process
4. Without documented baselines, software rollbacks may not be successful. In the case of OFORS, it is unknown if source control is being used at all
5. It is unknown whether any version of the software could be identified as a "baseline"
6. It is unknown whether questions could be answered, such as:
   a. What were the implemented requirements during the last release and what are they during this release?
   b. Did this functionality work during the last release? Can we deploy that version and test it out?
   c. What is every code change that has ever been associated to this requirement? Who wrote the code? Who reviewed it?

Overall, there is a risk that, in the event Library Services replaces the original vendor, a replacement vendor cannot access the source code in a workable, organized manner (e.g., the code and the controls placed on it in Subversion [code library system] fully port over to the next vendor).

1.4.2 Development Phase Improvements

Condition: Library Services does not have adequate policies and procedures, as defined in the LOC PMLC and SDLC, for monitoring the Development Phase processes and practices of its contractors. Although the PMLC and SDLC include planning for and monitoring Development Phase activities, there is no specific requirement to "flowdown" processes to contractors performing development work for LOC, nor guidance for LOC staff to monitor contractor adherence to best practices in its PMLC and SDLC.

Monitoring of contractors' work is primarily tied to deliverables approvals via coordination between Project Managers and the COR. However, for OFORS, there is a lack of oversight and knowledge of internal development methodologies of the software development contractor, including coding standards and procedures.

We observed in the assessments of the OFORS, there is little information known about how the contractors are building systems and what practices they are following.

Similarly, the OFORS project team did not receive details from the contractor regarding development, compilation, and deployment toolsets. The contractor may be following best practices, but without the agency requiring implementation documentation, this cannot be confirmed. It is critical for Library Services to assess what toolsets contractors plan to use for developing, compiling, and deploying, such as coding standards, unit testing procedures, and development guides, as well as to monitor the contractor's implementation of these development standards and procedures during the Development Phase. Without knowledge and approval of contractors' development methodologies and toolsets, it is difficult for Library Services to confirm alignment with LOC's SDLC, Enterprise Architecture, and CMMI best practices for development.

Below, Kearney noted examples of inconsistencies in processes used for the development and coding practices when compared with CMMI development best practices in Technical Solution processes.

Kearney requested documents for the assessment of Development Phase best practices that encompass "system development methodologies and work environment standards for OFORS to include: development environment standards and tools, and coding standards and procedures." Based on the documentation provided, we intended to confirm that the tools, standards, and procedures were in accordance with best practices or the requirements in LOC's SDLC. The documentation provided, however, does not provide that level of detail. The documentation provided includes a requirements gap analysis and a vision document, which, while helpful, do not explain how the development team builds OFORS.

Because LOC staff did not obtain details of the contractor's development methodologies and toolsets, the answers to the following questions posed in our audit questionnaire for developers are not known:

- What are the coding standards?
- Are there peer reviews of custom code?
- Are unit tests required?
- How often are tests run?
- Are they automated to run upon check-in?
- Is there a CI/CD pipeline?
- What tools are used by the development team?
- How is branching and merging of code done? For example, is it possible to work on bug fixes in the current production release, while simultaneously working on new features intended for the same release?
- Can a version of the code be deployed from any point in time?

Kearney was told that information supporting the questions above was not provided to Library Services by the contractor. Best practices for assessing and monitoring contractor's development methodologies to ensure alignment with the best practices or LOC SDLC and CMMI best practices were not in place.

Effect: Library Services is not able to confirm that SDLC procedures and the best practices outlined in the CMMI sub-practices are being followed by the vendor. Library Services is simply relying on the vendor to follow terms, such as SOPs, mentioned in the change management document of OFORS.

The effects and benefits of following best practices in software development have recently gained attention in the Federal Government. Historically, the Federal Government has taken a waterfall approach to software development and focused primarily on the Requirements Phase. The Government has recently endorsed that the processes within the Implementation Phase are critical for successful software. The activities within the Implementation Phase (or lack thereof/failure) determine the overall success of the project. The U.S. Chief Information Officer (CIO) and the Federal CIO Council's Digital Playbook (https://playbook.cio.gov/) reflects this fact by focusing no less than eight of its 13 "plays" on the Development/Implementation Phase of software. Specifically:

Projects not following modern development best practices will result in:

- More bugs
- Significantly longer development times
- Difficult to maintain/fragile code bases
- More system downtime
- A system that is more expensive to maintain
- A system that performs poorly under load
- Difficulty in finding developers to maintain the system due to unconventional implementations.

1.5.2 Deployment and Operations Improvements

Condition: Library Services does not have adequate policies, procedures, or SOW requirements for contractors to provide detailed documentation explaining how custom software is deployed or how COTS products are integrated with custom components. For OFORS, there is little information within the project team on how the third-party vendor assembles the custom OFORS deployment packages and scripts. Policies and SOWs should specify that contractors provide a detailed deployment guide describing how changes are tested and deployed, as well as an installation guide explaining how to perform the customizations.

There is no specific language in contracts to require "flowdown" of SDLC processes or best practices to contractors performing deployment and operations work for Library Services or guidance for Library Services staff to monitor contractor adherence to deployment and operations best practices.

Below, Kearney noted examples of incomplete processes, including lack of documentation explaining procedures and processes related to testing and verifying deployed software and procedures for performing customizations.

The OFORS implementation plan explains that Phase III (including customization) "is the most important phase of the OFORS implementation plan. This phase deals with the actual details of how OFORS is set-up for each office, transitioning of the data and preparing the system so the offices can begin using OFORS for some, if not all operations." Additionally, the document states: "This phase can be summarized into a few categories and may take anywhere between a couple of weeks to a month to be completely ready to start operating in OFORS." Kearney agreed that the Customization Phase of Virtua, the vendor-proposed software, is the most important phase. However, we did not observe any documentation explaining what procedures and processes are used during this phase.

Kearney also reviewed the OFORS System Administration Manual (SAM), which states:

> "The Systems Administration Manual contains key information and Standard Operating Procedures (SOPs) necessary to maintain the system effectively. The manual provides the definition of the software support environment, the roles and responsibilities of the various personnel, and the regular activities essential to the support and maintenance the system." However, we noted that this document appears to be in draft mode. There are several sections that appear to be questions posed to the development contractor. For example, the document has comments such as "Can Virtua [software] report account inactivity? Can Linux provide a clue?"

In all of the documents provided for the audit team to review, there is little to no information on the tools, coding languages, or procedures the development contractor uses in assembling the custom OFORS deployment packages and scripts.

We did not observe evidence that OFORS has an automated software build or CI/CD process as part of the product integration process. Automating the deployment process has several important benefits, including:

- Significant cost and time savings. For complicated deployments, manual processes can take several hours. Automated deployments completely eliminate this cost
- The process is completely repeatable and immune to human error. This gives the team assurance that deployments will succeed in any environment and eliminates the cause of common production issues: forgetting to perform one or more deployment steps
- The knowledge of deployment is not limited to a few individuals. When deployments are automated, anyone on the team can perform deployments, as opposed to manual deployments which are generally performed by one individual. If this individual leaves the team or is unavailable, the other team members have to learn the process, which costs significant time and money.

Effects: Library Services is not able to confirm that the contractor is following internal best practices for PI and deployment in accordance with the LOC SDLC Implementation Phase. In addition, the process of deployment was performed manually, which is costly, time-consuming, and more error-prone. Best practices recommend an automated CI/CD, which is less labor-intensive and results in fewer errors.

1.6.2 IT Governance Improvements

Condition: Library Services did not verify and monitor contracted system development work for alignment with best practices or LOC OCIO governance for project management and system development processes being performed by contracted development firms.

Kearney observed an absence of requirements in contracts and SOW for development contractors to adhere to SDLC practices.

There is no mention of a requirement to adhere to an SDLC in the original SOW. The omission of requiring contractor development work to be conducted in a structured, professional manner could lead to late or non-delivery of software products or provide a contractor with lower cost options to deliver software, resulting in higher failure and non-compliance rates.

Effect: The lack of mature IT governance and monitoring processes leads to an inconsistent application of project standards and controls causing potential issues with quality software development and implementation.

An absence of development standards may affect the delivery of fully defined and properly implemented stakeholder requirements.

A lack of systems development governance oversight can result in inconsistencies with quality and standards of deliverables, leading to cost overruns and missed project milestones.

1.10 Library Services Oversight Policies

Condition: Library Services' project cost management policies and procedures do not include effective cost monitoring and control, including reporting and analyzing cost variances and their causes, as well as tracking corrective actions for IT investments. Cost tracking information was observed in multiple formats with varying levels of detail, but no evidence was provided of project cost monitoring and analysis of cost variances to original estimates and corrective actions.

OFORS provided cost information in various formats, including internal consolidated payment histories, budgets based on CLINs, and acquisition costs schedule. We did not observe evidence that the project followed a formal process for analyzing costs, including variances, causes, and corrective actions. Original budget requests, estimated acquisitions costs, and General Ledger postings are listed below:

- 2011 Original Budget Appropriation request was $500,000 (total investment estimate of $2,500,000 over a five-year period)
- 2011 Original Acquisition costs (Schedule B Attachment 1) were estimated at $1,736,000
- 2016 General Ledger postings of invoices for the OFORS contract from the start of the project through to December 2016 totaled $1.23 million.

Library Services did not monitor OFORS under the OCIO's ITSC and IT Investment Management (ITIM) investment management process until the third quarter of FY 2016. Library Services did not follow LOC standard cost tracking and monitoring methodology prior to this point. As a Firm Fixed Price contract, there is no expectation on OFORS for projected versus actual variance reporting, since any cost variances are considered the vendor's concern and risk. Original delivery of the developed system with all functionality was planned for September 2012 and after ultimately having to take the contractor to a legal cure, the contractor has agreed to provide all functional requirements by December 2017. However, proactive monitoring of the contractor's actual work completed against costs and schedule might have provided earlier insight into the risks the contractor was experiencing, resulting in more effective risk mitigation of non-delivery.

Ultimately, the contractor did not deliver all the content required in the timeframe expected and a settlement had to be made. While contracting costs were contained by contractual agreements (Firm Fixed Price contract), product delivery was incomplete and delayed, as well as LOC's benefits from the envisioned end product. Additionally, as the investment continues past the planned completion dates, LOC incurs added internal costs related to contract oversight that were not initially identified.

Effect: Lack of formal policy and guidance regarding cost monitoring and control methodologies across the agency, including all service units, has several negative effects in relation to adequately assessing LOC's project costs and risks. These include:

- OFORS has not adopted proactive monitoring of the contractor's actual work completed against costs and schedule that might have provided earlier insight into risks for more effective mitigation
- OFORS has not applied formal cost variance analysis methods, including identifying causes and tracking corrective actions to closure
- Without regular and frequent monitoring and reporting of costs, variances, and corrective actions, there is increased risk surrounding LOC's ability to make informed and timely decisions about IT investments.

3.1.2 Project Management Scope and Schedule Improvement

Condition: OFORS did not have adequate scope and schedule management controls in place that aligned to best practices as identified in PMI's PMBoK®.

Below, we provide evidence of these conditions:

- OFORS project management did not document and track project scope/schedule risks and issues in a Risk Register or issue log
- OFORS project management did not effectively manage changes to the scope and schedule following the PMBoK® Scope Management process. We did not observe change requests documenting schedule and scope changes aligned with PMBoK® best practices.

Effect: The lack of plans for managing scope and schedule for OFORS poses risks can lead to mismanaged scope and schedule changes that could affect the project schedule and increase project costs. There is no documented process that guides the project in managing changes, risks, and issues related to scope and schedule. As PMBoK® states, "controlling the project scope ensures all requested changes and recommended corrective or preventive actions are processed through the Perform Integrated Change Control process."

3.3.2 Human Resources Management Improvements

Condition: Library Services project management did not have adequate Human Resource Management processes in alignment with best practices.

Kearney noted the following conditions for OFORS:

- Project management did not develop a Human Resource Management Plan that aligned with PMBoK® standards. Project management did not outline roles, responsibilities, required skills, and reporting relationships using techniques such as a RACI chart, which is a matrix clarifying roles and responsibilities most typically used: Responsible, Accountable, Consulted, and Informed
- Project management did not follow the PMBoK® guidance to document a plan for adjusting resources during the Project Closeout Phase. As a result, it is unclear if excessive or sufficient resources are assigned to complete closeout tasks.

Effect: If project team members do not possess required competencies and proper training is not provided to new resources, performance and success of the project can be jeopardized. When resource mismatches and changes are identified, proactive responses, such as training, hiring, schedule changes, or scope changes and documentation updates should be initiated.

Library Services project costs, schedules, risks, quality, and other project areas may be significantly affected by inadequate resources and misunderstanding of roles and responsibilities. According to PMBoK®, effective Human Resources planning should consider and plan for the availability of or competition for scarce resources. Having a clear understanding of project resources requirements can help avoid conflicts with other projects competing for Human Resources with the same competencies or skill sets. Project roles should be designated for teams or team members, and those teams or team members can be from inside or outside the organization performing the project.

Without effective Human Resource planning and management, staffing issues may disrupt the project team from adhering to the PMP, causing the schedule to be extended or the budget to be exceeded. Key benefits of effectively managing the project team is that it influences team behavior, manages conflict, resolves issues, and appraises team member performance.

Failing to formally plan the method and timing of releasing resources from a project can significantly increase the likelihood of Human Resources risk occurring during or at the end of the project and unnecessary resource costs being charged to the project.

Inefficient resource management planning may have been a key factor in LOC projects failing to properly maintain documentation, track/meet deliverables, and report on the performance of the project resources.

3.4.2 Communications Management Improvements

Condition: Library Services projects did not follow the LOC PMLC guidance for delivering and maintaining a Communications Management Plan.

Project management did not follow best practices or LOC PMLC guidance to create and maintain a Communications Management Plan. The Communications Management Plan was listed as a project deliverable due 14 days after award in the base contract. Project resources communicate through various status meetings, utilize tools to manage project deliverables and schedules, and prepare project reports. Project communications requirements were not centrally documented and maintained.

A Communications Management Plan facilitates effective and efficient communications with the various audiences who have a major stake in the project. Effective two-way communication between stakeholders is key for the success of the project. Good communication limits surprises, prevents duplication of effort, and helps reveal omissions and misallocation of resources early enough to permit corrections.

Effect: Library Services' lack of a requirement for OFORS to follow the LOC PMLC has several negative effects with regard to OFORS project management maintaining a formally documented Communications Management Plan. As stated in *Section 2.3* of the LOC PMLC, "communications, risk and unanticipated changes can impact the schedule and/or outcome of a project and it is important to plan in advance how these changes will be addressed." PMBoK® also discusses how ineffective communication creates a gap between diverse stakeholders who may have different cultural and organizational backgrounds, levels of expertise, and perspectives and interests, which may impact or have an influence upon the project execution or outcome. Library Services projects lacking a formal Communications Management Plan may experience conflicts with suppliers and internal team members due to miscommunication.

3.5.2 Risk and Issue Management Improvements

Condition: The OFORS project team did not follow the best practices or the LOC PMLC requirement to deliver and maintain a Risk Management Plan that describes how project risk assessments will be structured and performed.

Additionally, the OFORS project team did not follow best practices or the LOC PMLC requirement to deliver and maintain a Risk Register, which serves as a record of risk, mitigation strategy, contingency plan, and resolutions throughout the life cycle of the project.

Although an issue log was created, it was not maintained and updated throughout the project. The issue log was last updated in 2015 and did not include project management issues. Interviews with OFORS staff revealed that project issues occurred related to the vendor not meeting deliverable requirements; these issues were not included in the issue log and tracked to closure.

Effect: LOC's lack of enforcement of requirement for OFORS to follow the LOC PMLC has several negative effects with regard to OFORS maintaining Risk Management Plans, issue logs, and Risk Registers. As stated in *Section 2.3* of the LOC PMLC, "communications, risk and unanticipated changes can impact the schedule and/or outcome of a project and it is important to plan in advance how these changes will be addressed." Project risk is defined as an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives, such as scope, schedule, cost, and quality.

Project management relied on the vendor to maintain project documentation, but they did not include a Risk Management Plan as a deliverable. The vendor's PMP did not address managing risk or maintaining issue logs and Risk Registers. OFORS project management did not ensure that critical risks impacting scope, schedule, budget, business performance, and/or change management were proactively identified, communicated, mitigated, and escalated in a timely manner.

4.2.2 Improvements to Requirements Management

Condition: Library Services does not have guidelines, policies, or standardized processes for managing requirements throughout the SDLC or ongoing support and enhancement phases.

Kearney observed requirements documentation in multiple formats with varying levels of detail with limited bidirectional traceability. Additionally, we did not observe requirement baselines, meaning that they either do not exist or have not been maintained as part of the ongoing projects. A requirement baseline provides a defined, confirmed, and validated set of detailed requirements at specified checkpoints throughout a project life cycle. These baselines should be used to obtain metrics to show the amount of change (and when the changes occurred) throughout the project. The cost of a project increases exponentially depending on when project additions or changes to requirements are discovered. By tracking these changes against documented baselines, Library Services is better able to determine and manage project risks to schedules and budgets.

Below, we noted examples of inconsistencies in processes used for requirements management when comparing with best practices for project management.

OFORS did not provide an observable baseline for the overall system. Requirements documentation provided for the evaluation is contained in many disjointed documents of varying types and formats. The lack of cohesion in the documentation provided is a result of the lack of an organization-wide policy or guidance on what the development team needs to deliver and how this information should be managed. The OFORS program creates detailed functional specifications, which capture requirements and provide detailed implementation guidelines; however, the requirements are not documented in a format that facilitates overall requirement tracking or change management. This practice of progressing to detailed design without fully documenting and linking requirements does not provide a demonstrable way for Library Services stakeholders to validate that their requirements are understood and complete prior to moving into the Design Phase. This increases the risk of missing requirements. By having requirements embedded into the functional specifications, the OFORS requirements are not manageable. There is no way to track when changes are made or when new requirements are added or removed. Currently, documents must be reviewed individually and require reviewers to have extensive system knowledge or hold multiple meetings to understand and ensure the documentation captures all system functionality.

Effect: Lack of formal policy and guidance regarding the establishment of standard processes to manage requirements throughout the complete SDLC, including ongoing maintenance enhancement releases, resulted in the following:

- Inability to effectively view and manage project requirements
- Inability to fully trace requirements throughout the development process
- Inability to effectively manage changes to existing requirements or new requirements as they are developed.

4.4.2 Requirements Verification Improvements

Condition: Library Services does not use best practices or LOC SDLC standard guidelines, processes, or standard templates for verifying that requirements are fully tested and implemented during the Verification Phase. Documentation is maintained in various formats and levels of detail across and within projects.

Below, we noted examples of inconsistencies in processes used for requirements verification when comparing with best practices for requirements management and quality assurance for OFORS.

Documentation provided for review (e.g., use cases, release requirements, release notes, tickets/issues, test cases) is disjointed and requires management or peer reviewers to track information in multiple sources. The use cases do not contain enough detail to ensure correct implementation or verification. Based on information provided by the project team, peer review meetings were conducted as needed, but evidence was not available to confirm or verify output from these meetings.

Effect: Each program at Library Services has implemented its own formats and processes for requirements verification to differing levels of success. There is no clear way for Library Services to review individual projects against the stakeholder requirements to verify what has been implemented against the stakeholder and detailed product requirements.

5.1.1 Inadequate Access Control Policy and Procedures

Condition: The OFORS Information Technology Security Program Manager (ITSPM), in coordination with the System Owner, did not formally approve and ensure consistent implementation of documented procedures for account management and monitoring controls across the six OFORS overseas offices.

The Library Services OFORS Operations SAM was not finalized and formally approved and has not been updated since 2014. The SAM includes the settings and procedures to follow for controls, including regular and privileged user account management.

The lack of clear guidance compounds system administration issues, as OFORS operates in loose coordination across multiple remote staff offices, making consistent and current administration documentation critical to maintaining a secure systems landscape.

Improper or inconsistent application of account management controls can lead to unauthorized system access and changes to the data within the system.

We identified the following specific violations of LOC policy and non-compliance with the NIST Security Guidance:

- Two of eight new users added during FY 2016 from all six OFORS overseas offices were not properly approved prior to their system access

- Eleven of all 14 privileged users did not have Privileged User Rules of Behavior forms approved by the System Owner
- Sixty-nine out of a total of 397 user accounts user accounts have been inactive for over 30 days, but they were not disabled as required by LOC directives
- The OFORS ITSPM, in coordination with the System Owner, has not implemented, and monitored procedures for periodic recertification of users' continued access. Recertification includes validating that each user's permissions are still required based on their job function
- The OFORS ITSPM, in coordination with the System Owner, did not ensure periodic reviews were performed on audit logs containing privileged user activity through either application or network/server audit logs.

Effect: Failure to implement and follow the system access controls policies identified in LOC's ITSDir 01 would lead to unauthorized access to OFORS, including unauthorized transaction entries and approvals. Failure to periodically review and update the OFORS SAM, including system-specific security measures, contributes to the risk of system compromise by unauthorized users.

The absence of appropriately completed/authorized OFORS Access Management Forms and Privileged User Rules of Behavior, along with a lack of annual user recertification, could lead to granting users access to unauthorized job functions. If inactive accounts are not reviewed and removed in a timely manner, these accounts provide an opportunity for malicious attacks and increase the risk of loss, theft, or misuse of OFORS resources. Lastly, failure to implement the audit logging and review procedures reduces the system's ability to identify attempted or completed actions and respond to adverse events affecting data managed by OFORS.

5.2.2 Lack of Security Control Assessment Documentation and Detailed Planned Remediation Procedures

Conditions: The OFORS ITSPM did not effectively oversee and maintain security assessment and authorization documentation. Documentation of LOC's most recent Security Control Assessment (SCA) for the OFORS application in Archer GRC did not include the following:

- A final and approved Security Assessment Plan (SAP) – LOC provided Kearney with the OFORS SAP draft with no approval signatures from the appropriate LOC management officials
- Evidence of a completed SAR.

The ITSPM did not effectively manage system POA&M vulnerabilities. In our evaluation of the OFORS POA&M, Kearney identified the following:

- No new POA&Ms have been added to the POA&M listing since the initial accreditation for OFORS in 2014

- For a total of five POA&Ms, Kearney identified that one open, low-impact POA&M started on August 13, 2014 did not have documented planned remedial actions.

Effect: Failure to detail remediation actions required to address the weaknesses may lead to weaknesses lingering longer than necessary, thus increasing risk to the system. Further, these weaknesses might never receive attention from the agency's executives and System Owners, as the planned remedial actions are not documented in the POA&M.

The documented control assessment provides evidence of the current security posture of OFORS. Lack of documented control assessment results may hinder efforts to address any vulnerabilities identified. Thus, the SAR is a key requirement and serves as formal documentation for inclusion in a completed authorization package.

Finally, in order to make sound strategic decisions about enterprise-wide priorities and the allocation of resources, the agency's executives require a comprehensive understanding of all information security risks. Failure to perform assessments of the OFORS security posture weakens management's decision-making ability.

5.3.2 Lack of Configuration Management Plan and Security Impact Analysis

Conditions: LOC policy states that the System Owner shall develop and maintain a CM Plan for systems under his/her purview. The OFORS System Owner was unable to provide a finalized copy of the OFORS CM Plan, although one was in draft form.

Kearney assessed the process for testing and approving changes prior to release to production for OFORS. The OFORS draft CM Plan states that changes to any element covered by the plan must have a Technical Service Request (TSR) associated with these changes. Upon our testing of tracking OFORS system changes to TSRs, Kearney noted a lack of clear mapping between OFORS release test plans and TSRs. We could not reconcile from the documentation maintained that all functionality intended for the release within the TSRs were tested.

Kearney also noted that OFORS software releases did not have documented supervisory or management review and approval prior to being put into production. Improperly tested or unauthorized functionality may introduce failures or vulnerabilities to the system. The ability to research functionality introduced to authorized and tested requests is a key requirement in software development and deployment activities.

The System Owner did not ensure that configuration management processes under their purview included and considered the results of a Security Impact Analysis prior to OFORS releases. The LOC Chief Information Security Officer (CISO) stated that this was a recognized issue that is now being prioritized and incorporated into Change Advisory Board procedures.

Effects: Lack of a finalized CM Plan for OFORS may lead personnel to perform configuration or change management processes using an unauthorized draft plan. Without completing a security impact analysis, OFORS changes may have an adverse, unexpected impact on the security state of the system. Failure to trace TSRs to the test plan can lead to unauthorized changes to OFORS. Agreed changes to OFORS may go untracked or unmonitored by the ITSPM and CO, resulting in undelivered changes.

6.1.2 Incomplete Risk Management Framework (RMF)

Conditions: The OFORS System Owner did not ensure that the current OFORS SSP contains necessary detail to describe the management, operational, and technical safeguards or countermeasures for the information system. Specifically, the following deficiencies were identified:

- Lack of documentation of the system boundary for OFORS in the SSP provided during the Testing Phase of the audit. Updates to the OFORS SSP were in progress towards the end of the Testing Phase and into the Reporting Phase of the audit
- Reference and control testing consistent with outdated guidance (NIST SP 800-53, Rev. 3 *Recommended Security Controls for Federal Information Systems and Organizations*)
- Lack of detailed descriptions as to how OFORS management (i.e., ISSO, Control Assessor, Common Control Provider, and System Owner):
  - Has applied security controls, including detail of implemented security controls and residual planned actions to address any weaknesses
  - Updated the system's Archer record based on results from the continuous monitoring process that occurs on a monthly basis.

Kearney determined that the OFORS System Owner did not ensure completion of the steps within Archer to register the system with appropriate organizational program/management offices. Specifically, OFORS's Archer entry noted that the Parent/Child Relationship[5] section was not addressed.

Effect: Improper documentation of an information system's system boundary and identification of the scope of protection for the information system can lead to a failure in communicating the required internal/external control measures. The lack of a clearly defined system description, including system boundaries, could lead to ineffective determination or prioritization of controls to adequately safeguard that system.

The use of outdated NIST guidelines can lead to inadequate assessment of the controls needed to prevent system vulnerabilities as threat landscapes change; using current guidance ensures the latest countermeasures are in place, such as inclusions to consider advanced persistent threats.

Completion and documentation of the RMF for OFORS in the SSP would help mitigate against risks to the system, including those inherent to its use overseas. Specifically, the lack of consistent guidelines for the six overseas offices and LOC in Washington, D.C. increases the risk to confidentiality, integrity, and availability of information and data managed by OFORS.

[5] A "parent/child relationship" is defined as a governing organization (parent) that owns, manages, and/or controls a system (child).

The RMF is a process where each step is critical to the outcome of the subsequent step. Within each step are separate tasks (e.g., Task 1-3: *IS Registration*, which is part of RMF Step 1: *Categorize IS*). If the information system categorization step is not completed correctly, System Managers may not adequately apply succeeding steps, such as the selection of controls to implement for the system.

7.1.1 Inconsistency of Operating System Platforms and Inadequate Vulnerability Management

Conditions: The System Owner failed to ensure that OFORS instances are securely and consistently configured. OFORS has a complex operating environment, as it is configured and managed from the LOC Office in New Delhi, India. However, the ISSO sends updated versions to offices located in Cairo, Egypt; Islamabad, Pakistan; Jakarta, Indonesia; Nairobi, Kenya; and Rio de Janeiro, Brazil. According to the Project Manager, these updates would be installed on comparable server configurations at the other locations to keep all OFORS software instances running free of defects and security issues as the initially approved New Delhi instance. However, this was not the case; scanning completed in October 2016 identified that OFORS implemented the following four different versions of the Linux operating system (OS) across the six offices at varying levels of security patching:

[redacted]

Additionally, Kearney found that vulnerability scanning/continuous monitoring has not been completed for the OFORS instances prior to October 2016. Further, OFORS POA&Ms available in the Archer Governance, Risk, and Compliance (GRC) tool were created by the ISSO in 2014, and there is no evidence of the ongoing identification of vulnerabilities through other means and their inclusion in the POA&M listing.

In the October 2016 testing, the vulnerabilities for the four servers had varying levels of patch and configuration weaknesses, demonstrating the need for improved vulnerability management. Below is a table containing a summary of the results of the latest vulnerability scan performed for OFORS, which provides the count and severity of vulnerabilities on each server:

Exhibit 12: OFORS Server Vulnerabilities by Severity

OFORS Server Vulnerabilities by Severity						
OS/IP	Urgent	Critical	Serious	Medium	Minimal	Grand Total
[redacted]			4	3	3	10
[redacted]			4	3	3	10
[redacted]	39	90	301	10	7	447
[redacted]	13	25	117	3	2	160
[redacted]	12	24	76	1	1	114

OFORS Server Vulnerabilities by Severity						
OS/IP	Urgent	Critical	Serious	Medium	Minimal	Grand Total
[redacted]	14	41	108	6	4	173
[redacted]		**1**	**3**	**3**	**4**	**11**
[redacted]		1	3	3	4	11
[redacted]	**5**	**48**	**70**	**10**	**4**	**137**
[redacted]	5	48	70	10	4	137
Grand Total	44	139	378	26	18	605

Effect: Maintaining multiple configurations reduces cost-effective management of the security posture because LOC has to ensure tests for each system are separately planned, executed, and remediated. As evidenced by the table above, the deviations in configuration have led to system instances having multiple urgent and critical vulnerabilities, while others have none. Adding weaknesses to the POA&M ensures tracking and allows LOC to coordinate actions. A lack of constant updates lessens the attention provided from the agency's executives and System Owners, as the planned remedial actions are not documented in the POA&M. Without implementing the vulnerability identification and remediation process, the OFORS System Owner is unable to determine if high severity vulnerabilities could lead to compromise of LOC systems and data. If critical or high-risk vulnerabilities remain unmitigated on OFORS servers, there is an increased risk that the system instances could experience a loss of confidentiality, integrity, or availability.

Detailed Audit Findings – Congress.gov

5.1.2 Lack of Privileged User Account Review

Condition: The ITSG within the OCIO did not recertify Congress.gov privileged user accounts in FY 2016, as required by LOC policy. Recertification includes validating that each privileged user's privileges are still required based on his/her job function.

Kearney noted that administrative accounts have compensating controls, as they are tied to the Active Directory accounts which are managed at the network level. Active Directory accounts should be deactivated or removed within 48 hours upon a user's voluntary separation from the LOC and immediately for involuntary termination.

Regular recertification helps ensure that system users do not accrete access inconsistent with current position responsibilities resulting from new positions and temporary assignments. Regular recertification policies ensure that users are only provided with authorized access to accomplish assigned tasks.

Effect: The absence of appropriately completed/authorized privileged user recertification could lead to or continue granting users access to unauthorized Congress.gov job system capabilities and functions. This, in turn, could result in authorized access to Congress.gov.

5.2.2 Lack of Security Assessment Plan and Detailed Planned Remediation Procedures

Conditions: Kearney identified the following conditions in our evaluation of LOC's Congress.gov POA&M management and security assessments:

- The Congress.gov ISSO did not retain a SAP (The Congress.gov SCA and SAR were available and reviewed)
- Twenty-two of 23 total POA&M items were listed as open and ongoing. For 10 of the ongoing POA&Ms sampled, we noted the following:
  - The ISSO did not document planned remedial actions in the 10 selected ongoing Congress.gov POA&M items
- For one closed low-priority POA&M, Kearney identified the following:
  - The ISSO did not attach the Scanning/Pen Test results used as evidence to close the completed POA&M.

Effect: Failure to detail remediation actions required to address the weaknesses may lead to weaknesses lingering longer than necessary, thus increasing risk to the system. Weaknesses without planned remedial actions documented in the POA&M would not be considered as started when assessing current security performance metrics.

Without a finalized assessment plan, System Managers do not know that an effective or complete control assessment has been performed as advised by the CISO and Security Control Assessor. The System Owner may not be able to assess whether the procedures followed to perform the control assessment were according to a pre-approved scope and consistent with approved roles and responsibilities.

5.3.1 Lacks Configuration Management Planning and Security Impact Analysis

Condition: LOC did not have a CM Plan specific to Congress.gov. CM controls ensure that processes are in place to document changes made to a system's hardware, software, and documentation throughout the development and operational life of the system. Kearney noted that the Congress.gov System Owner did not follow the LOC security policy to develop and maintain the Congress.gov CM Plan. We also noted that the Congress.gov System Owner failed to comply with NIST guidance directing organizations to identify and document information system configuration items to be managed in a CM Plan. LOC uses the OCIO's *Change Management Process* document as the Congress.gov CM Plan, which is not specific to the Congress.gov system and does not contain Congress.gov configuration items.

Additionally, the System Owner did not follow the LOC security policies to ensure a security impact analysis was performed prior to releases of Congress.gov into the operational environment. The LOC CISO stated that the lack of a pre-production security impact analysis is a recognized issue that is currently being prioritized.

Effect: Congress.gov configuration items are not documented due to the lack of a CM Plan specific to Congress.gov. Configuration items refer to the various components of the Congress.gov system under configuration control, and they are important for planning for effective management of the system. Without identification of configuration items within the Congress.gov CM Plan, it may be unclear to all stakeholders the potential impact of changes to the Congress.gov system. LOC may not be able to determine the extent to which changes, vulnerabilities, or operations will affect the security state of the Congress.gov system.

6.1.1 Incomplete Risk Management Framework

Conditions: The System Owner has not fully developed the Congress.gov SSP. Specifically, the following deficiencies were identified:

- The SSP does not identify system interconnections for Congress.gov
- The SSP refers to and control testing is consistent with outdated guidance (NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*)
- There is a lack of detailed descriptions regarding how Congress.gov management (i.e., ISSO, Control Assessor, Common Control Provider, and System Owner):
  - Has applied security controls, including detail of implemented security controls and residual planned actions to address any weaknesses
  - Performs periodic updates to Archer (OCIO system inventory system) based on results from the continuous monitoring process that occurs on a monthly basis.

Kearney determined that the Congress.gov System Owner did not ensure completion of the steps within Archer to register the information system with appropriate organizational program/ management offices. Specifically, for the Congress.gov Archer entry, we noted that entries for network architecture and data flow documentation were not addressed.

Effect: The SSP outlines the security controls in place for the system and provides explanations of the reasons for those protections. The Interconnection Security Agreement (ISA) describes the risks posed by creating trusted connections and transmissions of data between systems. Without clear identification of the systems connecting to Congress.gov, security professionals may not be aware of the protections needed to mitigate potential vulnerabilities. Describing interconnections and taking a coordinated approach allows System Owners to carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements.

The use of outdated NIST guidelines can lead to inadequate assessment of the controls needed to prevent system vulnerabilities, as threat landscapes change; using current guidance ensures the latest countermeasures are in place, such as inclusions to consider advanced persistent threats.

Non-completion and lack of documentation of the RMF for Congress.gov in the SSP elevates risks to the ongoing operations of the Congress.gov system. Specifically, it is important that Congress.gov stakeholders understand their roles and responsibilities, from documented references in the SSP to procedures for security control assessment and system continuous monitoring, which are key processes for the management of risk to the Congress.gov system. The RMF is a process where each step is critical to the outcome of the subsequent step. Within each step are separate tasks (e.g., the *IS Registration* task is part of RMF Step 1: *Categorization*). If the information system categorization step is not completed correctly, System Managers may not adequately apply succeeding steps, such as the selection of controls to implement for the system.

7.1.2 Lack of Timely Vulnerability Mitigation for the OCIO Application Hosting Environment (AHE)

Condition: In coordination with the System Owner, IT security staff failed to remediate vulnerabilities in a timely manner for the AHE servers on which Congress.gov resides. The ISSO failed to ensure that vulnerabilities are remediated in a timely manner.

Condition: In coordination with the Congress.gov System Owner, the AHE System Owner failed to ensure vulnerabilities were remediated in a timely manner for Congress.gov servers hosted in the AHE.

The LOC uses Qualys, an enterprise systems scanning tool, to identify vulnerabilities within the LOC systems environments. Qualys reports elevated vulnerabilities discovered in a ranked format – "Urgent," "Critical," and "Serious." Based on the initial discovery of the elevated security vulnerabilities, as reported by the Qualys tool, Kearney noted that vulnerabilities have not been resolved for Red Hat Enterprise Linux (RHEL) servers used for Congress.gov, dating back to June of 2016. Kearney's analysis shows that over 40% of these vulnerabilities have been present on the AHE servers on which Congress.gov resides for over 90 days and have not been remediated.

Below is a table of the AHE vulnerabilities with a rating of severity (based on the Qualys scanner rating) and the age of each vulnerability grouped by operating system:

Exhibit 13: AHE Vulnerabilities

AHE Vulnerability Aging: (by OS, Severity)	< 30 Days	31–90 Days	91–180 Days	181–212 Days	Grand Total
[redacted]	24	12	34	306	376
[redacted]	2		2	10	14
[redacted]	16	8	20	73	117
[redacted]	6	4	12	223	245

AHE Vulnerability Aging: (by OS, Severity)	< 30 Days	31–90 Days	91–180 Days	181–212 Days	Grand Total
[redacted]	**457**		**22**		**479**
[redacted]	47		10		**57**
[redacted]	180				**180**
[redacted]	230		12		**242**
[redacted]	**104**		**40**		**144**
[redacted]	1		4		**5**
[redacted]	65				**65**
[redacted]	38		36		**74**
Grand Total	**585**	**12**	**96**	**306**	**999**

LOC has reviewed the weaknesses on the AHE servers and is in the process of implemented automated functions for patch management. A POA&M tracking this issue was initially created in October 2014. On November 28, 2016, the AHE System Owner requested a waiver, which was accepted on December 14, 2016, granting an extended remediation date of June 14, 2017. While LOC is managing the process, the systems residing on the AHE servers continue operations with elevated threat of compromise due to highly exploitable vulnerabilities. This threat increases over time, as published security weaknesses are available to the public and automated attacks are created and disseminated.

Effect: Without timely remediation of identified vulnerabilities, the Congress.gov System Owner is unable to determine whether high severity vulnerabilities could lead to compromise of LOC systems and data. If critical or high-risk vulnerabilities remain unmitigated on Congress.gov servers, there is an increased risk that the system servers and data could experience a loss of confidentiality, integrity, or availability.

A lack of constant updates decreases the attention provided from the agency's executives and System Owners, as the planned remedial actions are not documented in the POA&M. This can lead to increased risk of compromise of confidentiality, integrity, and, availability.

This page left blank intentionally

Appendix B: Management's Response

This page left blank intentionally

LIBRARY OF CONGRESS

OFFICE OF THE LIBRARIAN

MEMORANDUM

DATE February 9, 2017

TO Kurt W. Hyde, Inspector General

FROM David S. Mao, Deputy Librarian of Congress David S. Mao

SUBJECT Comments on Draft OIG Audit Report No. 2016-IT-102, *FY16 Review of System Development Life Cycle (SDLC)*

Thank you for the opportunity to comment on the subject draft report. We appreciate Kearney & Company's review, which includes an assessment of the Library's system development life cycle processes and a detailed review of three development efforts: Congress.gov, the Library Services Overseas Field Office Replacement System (OFORS), and the U.S. Copyright Office Electronic Licensing System (eLi).

As described on the attached chart, the Library concurs with the report's findings and recommendations. In the past 18 months, the Library has made significant improvements in the management of its information technology. Through our centralized Office of the Chief Information Officer, the Library is implementing (and documenting) standards and processes for managing IT investments, the system development life cycle, and the project management life cycle. These practices are enhancing the Library's ability to assess risks and make decisions at each stage of a system's development, including, importantly, the ability to identify quickly when a system has gone off track and to correct course.

Last summer, based on an independent third-party assessment of eLi ordered by the Copyright Office, and an internal assessment of OFORS by Library Services, the Library took action on the eLi and OFORS contracts. At the Copyright Office's request, the Library terminated eLi and accepted delivery of existing code. The Library also reduced OFORS scope to essential functionality. The Library will conduct a further review of these projects.

Please let me know if you have questions or would like to discuss this in greater detail.

Attachment

cc: Bernard A. Barton, Jr., Chief Information Officer
J. Mark Sweeney, Associate Librarian for Library Services
Karyn Temple Claggett, Acting Register of Copyrights
Elizabeth Pugh, General Counsel
Nicole L. Marcou, Special Assistant to the Deputy Librarian; OIG Audit Liaison

Management Comments on Draft OIG Audit Report No. 2016-IT-102, FY16 Review of System Development Life Cycle (SDLC)

Library-Wide (Systemic Issues)	
Recommendation	**Comments**
1. LOC should compare current SDLC policies and procedures to industry best practices to ensure development risks are actively monitored and managed.	**Concur.** **Library Approach:** As part of the current effort to ensure consistent use of SDLC and Project Management Life Cycle (PMLC) practices Library-wide, the Library, with consultant support, is developing directives which describe detailed SDLC and PMLC procedures and process steps, including risk management guidance. To develop the directives, the consultant is taking into consideration industry best practices as well as GAO guidelines on risk management and prior experience from other government agencies. The directives are expected to be completed by Q2 FY17.
2. LOC should monitor current SDLC activity and environmental factors as part of a structured risk assessment framework to ensure policies and procedures identify and address emerging issues/new risks.	**Concur.** **Library Approach:** As noted above, the Library is currently developing SDLC and PMLC directives which include procedures and process steps for ensuring project risks are identified, assigned an owner, tracked, and mitigated as part of an overall risk management plan. These directives are expected to be completed by Q2 FY17. In addition, the Library has recently established an annual independent verification and validation (IV&V) IT project review process through which the risk management process for all major projects will be regularly monitored by the Project Management Office (PMO).

3. COs and Contracting Officer's Technical Representatives (COTR) should collaboratively identify standard SDLC contract elements, including vendor timelines, technical deliverables, required documentation, and internal review and acceptance procedures, as well as ensure that SDLC contracts contain these elements.	**Concur.** **Library Approach:** The Library currently includes in all IT contracts a standard SDLC clause that requires contractors to follow the Library's SDLC and PMLC as described at https://loc.gov/about/doing-business-with-the-library/information-technology-related-business/. The Library will issue a policy and standard operating procedures to ensure that SDLC elements which are relevant to particular IT development projects are incorporated as scheduled deliverables into contracts and that internal review and acceptance procedures are clearly identified and described by Q2 FY17.
4. LOC should develop policies that clearly delineate required oversight approval for additional funding requests, contract modifications, delivery delays, and inability to meet original technical requirements in all LOC service units.	**Concur.** **Library Approach:** As part of the newly-implemented Information Technology Investment Management (ITIM) process at the Library, any changes to an approved IT investment must be submitted for review and approval by the Library's Information Technology Steering Committee (ITSC) and Executive Committee (EC). Also, the ITIM framework requires quarterly updates on every IT investment, with updates on investment cost estimates and variances, milestone status including current and anticipated milestone completion dates and delays, and an assessment of overall investment risks. An LCR requiring all service units to follow ITIM is currently under review and expected to be promulgated by Q3 FY17.
5. LOC should clarify funding sources and status of funds reporting requirements	**Concur.** **Library Approach:** The newly-implemented ITIM process at the Library includes identification of funding sources at the proposal phase, and a comparison of proposed budget to actual execution each quarter during implementation. In addition, with the enforcement of the SLDC processes for all Library IT projects, rather than just those within OCIO, all IT projects will be required to budget and report on the resources at the project level as well. LCRs requiring Library-wide compliance with the ITIM and SDLC processes are currently under review and expected to be completed by Q3 FY17.

Electronic Licensing System (eLi)

Recommendation	Comments
1. If development activities resume, ensure that current LOC policies and relevant industry best practices are adopted by service unit oversight and project management teams.	**Concur.** **USCO Approach:** USCO will ensure that future efforts to develop electronic submission of cable statements of account will be managed in accordance with Library guidance, and will follow the detailed SDLC and PMLC procedures and process steps that are being formulated by the Library. For broader context, USCO notes that this audit concerned only a single software project, eLi, which for most of its life was managed outside of the Copyright Technology Office (CTO). IT projects managed within CTO have consistently followed LOC-mandated SDLC methodology. Indeed, a 2015 Inspector General audit found that the USCO was "compliant with [LOC] SDLC methodology" with respect to its primary software applications, Electronic Copyright Office (eCO) and Copyright Imaging System (CIS), which support registration and recordation functions, and are managed by CTO. *See* Library of Congress Office of the Inspector General, *Report on the Maturity of the Library's System Development Life Cycle Processes and Procedures* 8 (Feb. 2015), at https://www.loc.gov/portals/static/about/documents/system-development-life-cycle-2-25-15.pdf. Accordingly, USCO does not understand this report to be opining on the SDLC practices of USCO as a whole. USCO also notes that of its own accord—and before this audit commenced—USCO ordered an independent third-party assessment of the eLi project, which was delivered to USCO in December 2014. Although the 2014 assessment found that the "eLi project ha[d] many artifacts that are required by a system development life cycle methodology," the assessment found problems with the SDLC practices used on the eLi project. As a result of the assessment, USCO took immediate steps to remedy these issues, including transferring management of the project to the Copyright CIO's office, which has expertise regarding SDLC management. In addition, USCO implemented numerous recommendations from the assessment to improve the eLi project, including the creation of a senior steering committee, and appointing the Director of CTO as the project manager. USCO's decision to terminate the eLi project was the direct result of these project management improvements adopted by USCO. After the eLi project came under Copyright CIO oversight, it became apparent that the contractor hired to develop eLi was not performing adequately, and that future operation and maintenance costs would well exceed anticipated costs. As discussed below, USCO has proposed to shift the effort to make an electronic submission system for statements of account in a more cost-effective and efficient direction.

2. USCO should update and clearly define technical requirements and functionality of the systems.	**Concur.** **USCO Approach:** USCO intends to update and define existing business and technical requirements for future efforts to develop electronic submission of cable statements of account, in accordance with Library guidance.
3. USCO should assess elements of existing development activity for possible reuse.	**Concur with comments.** USCO notes that developments subsequent to the close of the audit suggest an alternative approach may be more cost-effective and desirable to our external stakeholders. **USCO Approach:** As the audit report notes, before terminating the eLi project, USCO obtained a copy of the complete customized source code for eLi, so that if there was desire from stakeholders, USCO could continue with the eLi project. Accordingly, to the extent there is such a desire, USCO will ensure that the source code is assessed for reuse. Since the close of the audit, USCO submitted an Investment Proposal to the Library's IT Steering Committee (ITSC) to adopt a spreadsheet-based form for electronic submission of statements of account; many cable companies already prepare the current paper form using a spreadsheet tool. This solution is likely to be cost-effective and easy for the cable industry to implement. Although initially conceived of as an interim step, feedback from stakeholders regarding USCO's decision to terminate the eLi project and implement spreadsheet-based remittance has been extremely positive. For example, an attorney representing one of the companies that submits a significant number of statements of account described the USCO's solution as a "positive development" and a "smart approach." Accordingly, it may be that this solution will fully satisfy stakeholders.
4. USCO should clearly define vendor timelines, technical deliverables, and required documentation as part of the contract and Statement of Work (SOW).	**Concur.** **USCO Approach:** USCO will ensure that contracts and SOWs for any future efforts to develop electronic submission of cable statements of account clearly define vendor timelines, technical deliverables, and required documentation, in accordance with guidance from the Library.

5. Develop reasonable and reliable cost estimates for subsequent development activities and obtain LOC oversight approval.	**Concur.** **USCO Approach:** USCO will develop reasonable and reliable cost estimates for any future efforts to develop electronic submission of cable statements of account, in accordance with guidance from the Library. Like eLi, such efforts will be funded entirely out of the collected royalties (rather than taxpayer funds), and the Office will accordingly ensure adequate transparency regarding the impact of future development on the royalty pool. With respect to Library oversight of eLi, USCO's Licensing Division notes that it first briefed the ITSC about the eLi project in March 2012. As the audit report acknowledges, under then-prevailing Library policies, the eLi project was not selected by the ITSC for continued ITSC oversight, and was understood to be moving forward fully under direction of the USCO. Notwithstanding the understanding that the eLi project was to operate without ongoing Library involvement, USCO reported to various Library components about the status of the eLi project. In August 2015, the Copyright CIO briefed the ITSC on the eLi project to provide an update. Similarly, USCO reported on the eLi status to the Library's Strategic Planning Office (SPO) (now Strategic Planning and Performance Management) as a "secondary" performance target in 2014 and 2015, even though SPO does not require reporting of secondary targets. In addition, the Library's financial statements in 2014 and 2015 did not reference eLi merely because secondary targets are not included in those statements (*i.e.*, only "primary" performance targets are included).
6. USCO should clarify funding sources and status of funds reporting.	**Concur.** **USCO Approach:** USCO will ensure that funding sources and status of funds reporting are reported appropriately for any future efforts to develop electronic submission of cable statements of account, in accordance with guidance from the Library.

Overseas Field Office Replacement System (OFORS)

Recommendation	Comments
1. If development activities resume, ensure that current LOC policies and relevant industry best practices are adopted by service unit oversight and project management teams.	**Concur.** **Library Approach:** The Library issued a Cure Notice to the contractor on June 15, 2016. In lieu of a termination for default, development activities have resumed under revised requirements and delivery schedules. Library Services/Overseas Operations (LS/OvOp) will work with the OCIO PMO to ensure that Library policies are followed and relevant industry best practices are adopted for the remaining phases of the PMLC. The expected date for this to be completed is by Q1 FY18.
2. OvOp should update and clearly define technical requirements and functionality of the systems.	**Concur.** **Library Approach:** As part of the negotiated alternative to termination for default, the Library is revising the OFORS statement of technical requirements and functionality and modifying the contract accordingly. The Functional Design documents for the remaining modules of the system are expected to be completed is by Q2 FY17.
3. OvOp should clearly define vendor timelines, technical deliverables, and required documentation as part of the contract and SOW.	**Concur.** **Library Approach:** As part of the negotiated alternative to termination for default, the Library is revising the OFORS deliverables and delivery schedule and modifying the contract accordingly. LS/OvOp will provide the documentation for vendor timelines, technical deliverables that are defined as a part of the most recent modification to the contract in response to a Cure Notice. The expected date for this to be completed is Q2 FY17.

4. Develop reasonable and reliable cost estimates for subsequent development activities and obtain LOC oversight approval.	**Concur.** **Library Approach:** To ensure that there is appropriate and ongoing Library oversight of all development activities for this project going forward, LS/OvOp will prepare an IT investment package that includes all cost estimates currently projected for completion of the project. This package will be submitted to the IT Investment Management Portfolio Office (ITIMPO) for review by the ITSC. If recommended by the ITSC, the IT investment will be incorporated into the Library's IT Investment Portfolio and be provided to the EC and Librarian. As part of the ITIM process, LS/OvOp will report quarterly on the health of the IT investment in the areas schedule milestones, risks, and costs. The expected date to have this activity fully managed by LOC ITIM processes is Q3 FY17.
5. OvOp should clarify funding sources and status of funds reporting.	**Concur.** **Library Approach:** The LC Financial Reporting System (FRS) Status of Funds Report and Spending Lines reports give breakdowns of expenditures to the BOC level on each contract, but not down to the CLIN level of each contract. Therefore the funding sources and status of obligated contract funds will be established primarily from invoices paid through Momentum as well as from Spending Lines reports requested from the Office of the Chief Financial Officer (OCFO). It should also be noted that OCFO did not require or issue cost variance reports since the OFORS contract is firm fixed-price. As a corrective action, LS/OvOp will develop spreadsheets and/or other documentation to clearly indicate the source of funding for each CLIN as shown on vendor invoices and the CLIN list (Section B) in the contract. The expected date for this to be completed is by Q4 FY17.
6. OvOp should address security risks, perform required remediation, and complete all required documentation.	**Concur.** **Library Approach:** Library Services had recognized the need to address the security concerns and proper documentation for this project; hence the service unit had already initiated a re-accreditation process (A&A) starting August 2016. This process is currently underway under the guidance of OCIO/IT Security Group (ITSG). As a corrective action, LS/OvOp will cover aspects of security risks, required remediation and associated documentation via the A&A process. The culmination of this process will cover several aspects of risk by including it in the ITSG-approved Archer system and bringing the system under the purview of Qualys Continuous Monitoring process to identify and remediate risks wherever possible within the system limitations. Furthermore, LS/OvOp will also work with OCIO/ITSG to update all required documentation. The expected date for completion of the re-accreditation is Q4 FY17.

7. OvOp should identify necessary personnel requirements to successfully perform project management and security oversight.	**Concur.** **Library Approach:** As a corrective action, LS/OvOp will work with the OCIO PMO to ensure the necessary personnel requirements are reported and documented by clearly identifying and defining the project roles and subsequently aligning the project with OCIO PMLC steps and deliverables. Also, the security oversight of the project will be addressed by representing the system in the Library's security risk and compliance system (Archer) and completion of the re-accreditation process. The expected date for completion of the Project Roles documentation is Q2 FY17.

Congress.gov

Recommendation	Comments
1. OCIO should ensure that continuing development activities incorporate current LOC policies and relevant industry best practices are adopted by service unit oversight and project management teams.	**Concur.** **Library Approach:** Members of the Congress.gov project team have a direct role in several Library-wide initiatives to set policy and best practices, including Agile Software Development, Service Management, Change Management, and Project Management processes. The team will work with OCIO staff and management to ensure that the Congress.gov project adopts best practices and follows OCIO policy in all of these areas, including all elements related to security.
2. OCIO should address security issues for all operating systems and environments, develop timeliness for remediating deficiencies, and monitor progress towards resolution.	**Concur.** **Library Approach:** The System Owner and Information System Security Officer (ISSO) have reviewed the entire set of security-related processes, documents and controls. All open items in the plan of actions and milestones have either been addressed, or are being addressed. A new security evaluation process has been implemented by the project team and ISSO. This updated process will ensure that all relevant security documents and controls will be reviewed and revised both on a monthly basis and for all new releases. This process was put in place in January 2017. The Congress.gov project team is working with the infrastructure team to test the updated infrastructure. We expect to have the updates and tests completed Q3 FY17. Infrastructure changes to improve Linux patching include implementing a new server that is dedicated to patching all Unix operating systems in the LOC environment. This server will automate the pushing of security patches to the Unix systems and will be implemented by Q3 FY17. Additionally OCIO is updating a standard operating procedure for the management of security patches for all Library servers in conjunction with the ITSDIR01 guidance with an expected completed date of Q4 FY17. Below is a list of milestones. Implement new Unix Patching Server: December 2016 – April 2017 Develop Patching SOP: January – April 2017 Train Staff on Patching SOP process: April – May 2017 Implement new process: June –September 2017