The Library of Congress

Office of the Inspector General

Office of the Librarian

Survey of ccmMercury IT System

Survey Report No. 2011-IT-102
March 2012

FOR PUBLIC RELEASE

UNITED STATES GOVERNMENT LIBRARY OF CONGRESS

Memorandum ***Office of the Inspector General***

TO: James H. Billington
Librarian of Congress

March 28, 2012

FROM: Karl W. Schornagel
Inspector General

SUBJECT: Survey of ccmMercury IT System
Project No. 2011-IT-102

This transmits our final report summarizing the results of the Office of the Inspector General's survey of ccmMercury. The executive summary begins on page *i*, and the results of our audit survey appear on pages 4 and 5.

We appreciate the cooperation and courtesies extended by the Office of the Librarian during this audit survey.

cc: Chief of Staff
Chief Information Officer
Director, Information Technology Services

⏩ TABLE OF CONTENTS

⏩ EXECUTIVE SUMMARY

The Office of the Librarian is responsible for managing ccmMercury, a document and correspondence tracking software application. We initiated an audit to assess application controls and user access rights for this application.

Based on our audit survey,[1] we concluded that further review is unnecessary at this time. We may revisit this area after Library management performs a Certification and Accreditation (C&A)[2] on the major upgrade to ccmEnterprise,[3] tentatively scheduled for March 2012. Summaries of the survey work we performed are below.

The Library's Currently Installed Version of ccmMercury Cannot Address Some Overdue POAMs–A Plan of Action and Milestones (POAM) is the corrective action plan for addressing weaknesses identified during the C&A process. In 2009, a C&A of ccmMercury resulted in several POAMS, five of which remain unresolved. Three POAMS are due to system limitations with the current version of the application and two are due to inadequate management controls. This year's planned upgrade to ccmEnterprise will address three POAMs.

User Access Controls are Manually Intensive–The process of removing a user's access to ccmMercury is labor intensive and susceptible to human error. Similar to the management control POAMs, this weakness is not dependent upon an upgrade and adequately addressing it is management's responsibility. We identified one former employee with access to the system for over a year after their termination.

The Office of the Librarian and Information Technology Services submitted written comments on our draft report. Management concurred with the results of our audit survey. The full text of management's response is included in appendix A.

[1] A survey is a process for gathering information on the most significant audit areas so as to identify potential problems within the scope of the audit.

[2] The certification process identifies and evaluates controls in an application. Accreditation is the formal declaration that an automated information application is approved to operate in a particular security mode using a prescribed set of safeguards.

[3] The upgrade to ccmMercury will be ccmEnterprise.

⏩ BACKGROUND

ccmMercury is a commercial off-the-shelf (COTS) application designed to track documents of various types, such as correspondence. The application allows the Library to track all the activities associated with a document and to see the status of a record and its workflow. The Library first purchased ccmMercury in the mid 1990s. The developer, WorkDynamics, released various upgrades for ccmMercury, including version 5.3.2, in October 2009. The Library, however, installed version 4.0 in 2009 and is still operating with this version of the program. ccmMercury is a stand alone application with no interconnections with any internal or external systems and all service units are allowed access.

The Office of the Librarian, as system owner, is responsible for managing the application, while Information Technology Services (ITS) is responsible for securely housing the Application Hosting Environment and providing support and maintenance activities. ITS also mandates that information technology (IT) systems undergo Certification and Accreditation (C&A) as per Library of Congress Regulation 1620, *Information Technology Security Policy of the Library of Congress*, and IT Security Directive 01.

Certification and Accreditation Process

The certification process identifies security weaknesses in operating the application and evaluates potential vulnerabilities. The accreditation process is the formal declaration by the Designated Approval Authority (DAA)[4] that an application is approved to operate in a particular security mode using a prescribed set of safeguards. An Approval to Operate (ATO) is valid for three years unless a modification such as a major upgrade occurs, in which case recertification of the system is required prior to it being placed into production.

The C&A process often identifies a list of potential system vulnerabilities. The Plan of Action and Milestones (POAM) is

[4] The DAA is the individual responsible for the accreditation process, which consists of accepting the residual risk of an IT system on behalf of the Library of Congress and authorizing the system to operate in production.

the corrective action plan for addressing these weaknesses. It specifies the mitigation measures required to improve system security. At the Library, resolution of POAM items is dependent on available resources.

As part of the Library's IT Security Governance Program, the Information System Security Officer (ISSO)[5] reports any corrective action taken to the Designated Approving Authority (DAA) on a quarterly basis. Completed POAM items appear as closed on subsequent quarterly reports.

Of the several POAMs identified in the 2009 ccmMercury C&A, five remain open. An ATO issued in August 2009 allowed ccmMercury to operate until August 2012. However, ITS plans on implementing a major upgrade during the spring of 2012, which may address the open POAMs and will require an updated C&A.

[5] The ISSO performs the operational security aspects related to one or more IT systems. They are responsible for ensuring that management, operational, and technical controls for securing IT systems are in place and followed.

⏩ OBJECTIVES, SCOPE, AND METHODOLOGY

We initiated this audit survey to assess the application controls and user access rights associated with processing data in the ccmMercury application. We placed emphasis on the Disbursing Office's (DO) internal controls for data and deposit entry into the Momentum Financial System.

We reviewed C&A documentation and conducted interviews and discussions with staff responsible for system maintenance. We also observed DO check processing entries in ccmMercury.

We reviewed user application access to determine whether any ineligible individuals had system access. We compared the user access list to the active employee/contractor file and investigated exceptions with Human Resources Services and the Office of Contracts and Grants Management. We discuss the details of our testing in the *Results of Audit Survey* section.

Our fieldwork, interrupted by higher-priority projects, was conducted from May 2011 through March 2012 in accordance with generally accepted government auditing standards and LCR 211-6, *Functions, Authority, and Responsibility of the Inspector General*. Government auditing standards require that we plan and perform audit work to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions, based on our objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions, based on our objectives.

⏩ RESULTS OF AUDIT SURVEY

We found that several POAMs identified in the 2009 C&A process remained open. Since ITS plans on installing a major upgrade to ccmMercury this year, many of these open POAMs may close with the new version. Therefore, we may perform further review after the C&A and upgrade to ccmEnterprise[6] is completed. Summaries of the survey work we performed are provided in the following comments.

I. The Library's Currently Installed Version of ccmMercury Cannot Address Some Overdue POAMs

Five POAMS remain open since first identified during the 2009 C&A. C&A methodology requires ranking identified system vulnerabilities as high, moderate, or low depending upon their level of significance. Three POAMs were ranked as high and two as moderate risk. Three of these POAMs were noted as not supported by the current version of ccmMercury (Risk numbers 1, 2, and 4). We anticipate that these items will be resolved when ITS installs the latest ccmEnterprise Suite in the spring of 2012. The other POAMs relate to management controls independent of the application. Table 1 summarizes the overdue POAMs as of September 2011.

Table 1: Overdue POAMs as of September 2011

Risk	POAM
1. High	Implement controls such that Library and Library-owned COTS web applications advise the user to close the browser session to remove any session tokens in memory on the client system.
2. High	Implement technical controls such that the system must automatically notify (either using internal functions or a separate notification process) the ISSO whenever account creation, modification, disabling, or deletion actions occur.
3. High	Implement management controls such that all services and protocols necessary for operation must be explicitly identified and justified within the system security plan.
4. Moderate	Implement technical controls such that the IT system must provide the capability to report audit records for events of interest based upon selectable event criteria.
5. Moderate	Implement management controls such that each IT system must have at least one primary and one backup ISSO designated.

[6] The upgrade to ccmMercury will be ccmEnterprise.

Management Response

Management concurred with our results. ITS responded that it will support any subsequent efforts that may be necessary to remediate any POAM items that are not resolved by the upgrade.

II. User Access Controls are Manually Intensive

During our 2011 survey, we discovered an active ccmMercury user account of a former employee that separated from the Library in June 2010. IT Security Directive 01 – *General Information Technology Security Directive* requires system owners to disable user accounts within 48 hours of an individual's departure. In addition, it requires Library management to remove or rename all associated user accounts within 30 days of an individual's departure.

Our review found that the current process for disabling terminated user accounts is labor intensive and susceptible to human error. The process involves the ISSO manually comparing a monthly report of active ccmMercury users with a "terminators" list emailed from ITS. The ISSO must then request that an ITS system administrator manually disable ccmMercury accounts for users that appear on both lists.

With the upgrade version, the Library plans on using the Library's Active Directory user authentication service to improve user access controls, however, the manual process for managing accounts will most likely continue. Although an automated process would be less error-prone, such a solution may be cost-prohibitive for the Library.

Management Response

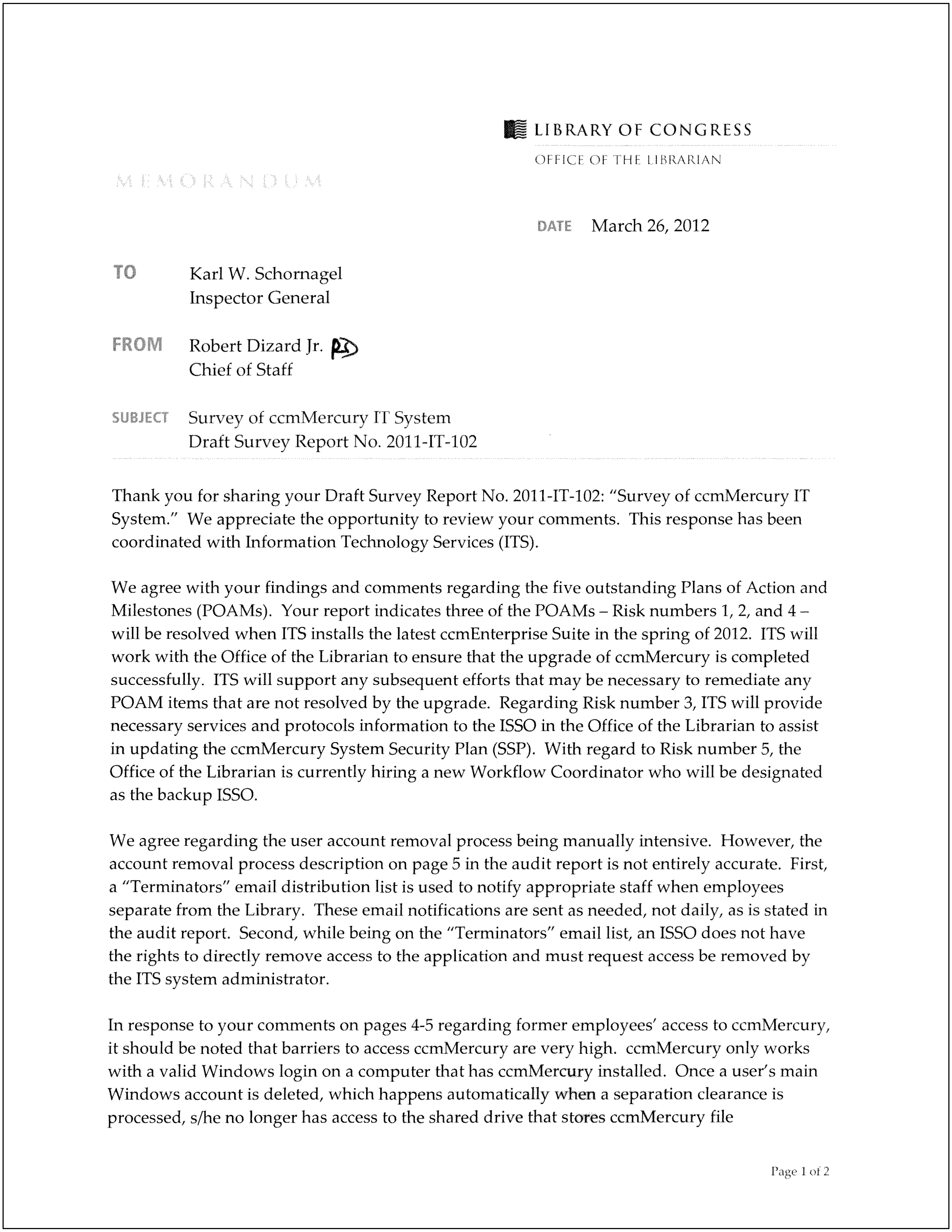
Management concurred with our finding.

CONCLUSION

Based on our work, we concluded that an audit was unnecessary at this time. The pending upgrade from ccmMercury to ccmEnterprise scheduled for March 2012 should address most of the current risks identified. Pending audit resources, we may revisit this area once management has properly identified any new risks with the upgrade.

Major Contributors to This Report:
Nicholas Christopher, Assistant Inspector General for Audits
John Mech, Senior Lead Auditor
Larry Olmsted, Information Technology Specialist
Walter Obando, Auditor

▸▸ APPENDIX A: MANAGEMENT RESPONSE



LIBRARY OF CONGRESS
OFFICE OF THE LIBRARIAN

MEMORANDUM

DATE March 26, 2012

TO Karl W. Schornagel
Inspector General

FROM Robert Dizard Jr.
Chief of Staff

SUBJECT Survey of ccmMercury IT System
Draft Survey Report No. 2011-IT-102

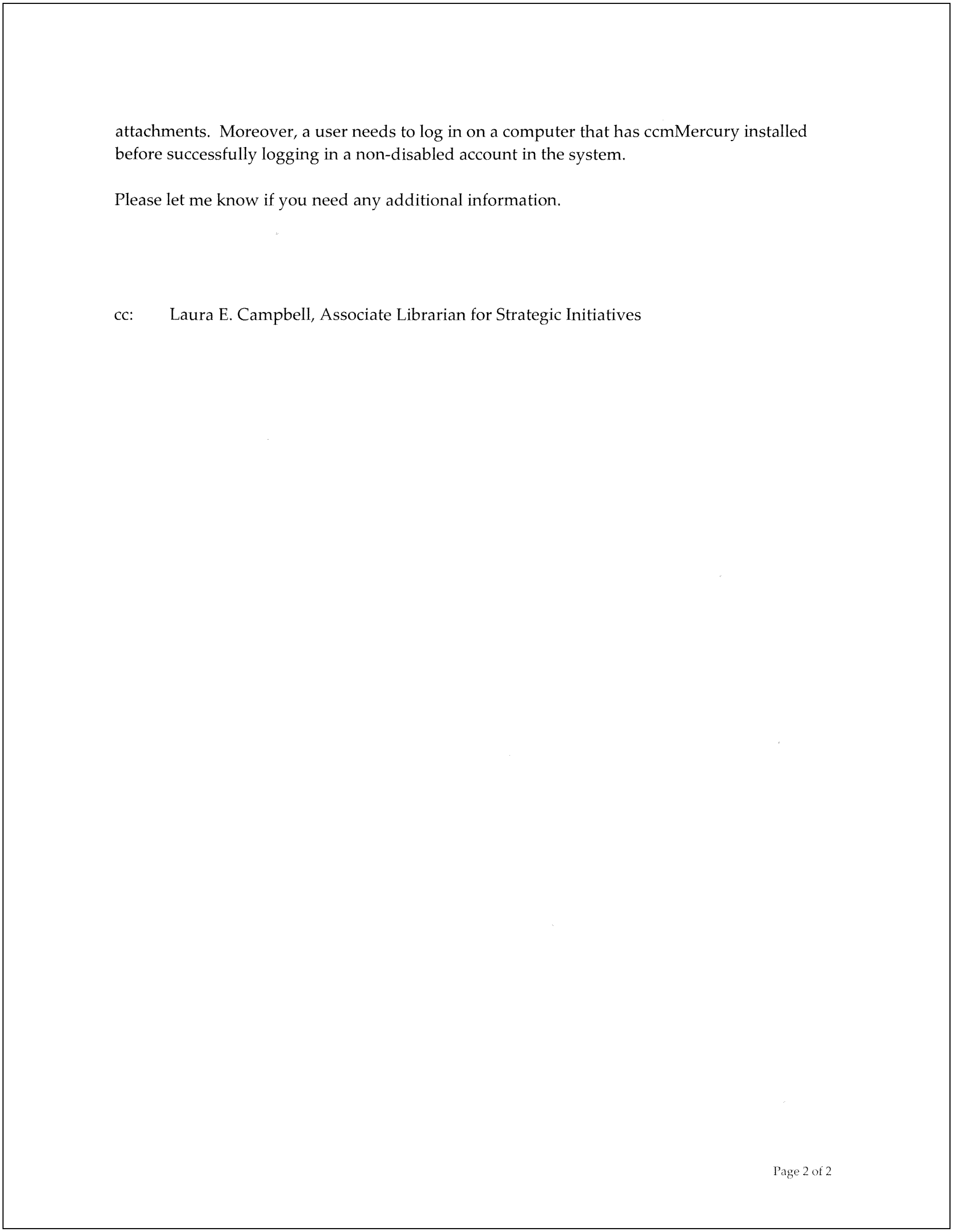
Thank you for sharing your Draft Survey Report No. 2011-IT-102: "Survey of ccmMercury IT System." We appreciate the opportunity to review your comments. This response has been coordinated with Information Technology Services (ITS).

We agree with your findings and comments regarding the five outstanding Plans of Action and Milestones (POAMs). Your report indicates three of the POAMs – Risk numbers 1, 2, and 4 – will be resolved when ITS installs the latest ccmEnterprise Suite in the spring of 2012. ITS will work with the Office of the Librarian to ensure that the upgrade of ccmMercury is completed successfully. ITS will support any subsequent efforts that may be necessary to remediate any POAM items that are not resolved by the upgrade. Regarding Risk number 3, ITS will provide necessary services and protocols information to the ISSO in the Office of the Librarian to assist in updating the ccmMercury System Security Plan (SSP). With regard to Risk number 5, the Office of the Librarian is currently hiring a new Workflow Coordinator who will be designated as the backup ISSO.

We agree regarding the user account removal process being manually intensive. However, the account removal process description on page 5 in the audit report is not entirely accurate. First, a "Terminators" email distribution list is used to notify appropriate staff when employees separate from the Library. These email notifications are sent as needed, not daily, as is stated in the audit report. Second, while being on the "Terminators" email list, an ISSO does not have the rights to directly remove access to the application and must request access be removed by the ITS system administrator.

In response to your comments on pages 4-5 regarding former employees' access to ccmMercury, it should be noted that barriers to access ccmMercury are very high. ccmMercury only works with a valid Windows login on a computer that has ccmMercury installed. Once a user's main Windows account is deleted, which happens automatically when a separation clearance is processed, s/he no longer has access to the shared drive that stores ccmMercury file

Page 1 of 2



attachments. Moreover, a user needs to log in on a computer that has ccmMercury installed before successfully logging in a non-disabled account in the system.

Please let me know if you need any additional information.

cc: Laura E. Campbell, Associate Librarian for Strategic Initiatives