The Library of Congress

Office of the Inspector General

Library-Wide

Information Technology Services
Integrated Support Services

Review of Underutilized Multifunction Devices

Report No. 2010-SP-101
April 2010

FOR PUBLIC RELEASE

UNITED STATES GOVERNMENT LIBRARY OF CONGRESS

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

TO: James H. Billington
Librarian of Congress

April 29, 2010

FROM: Karl W. Schornagel
Inspector General

SUBJECT: *Review of Underutilized Multifunction Devices*
Inspection Report No. 2010-SP-101

This transmits our final report summarizing the results of the Office of the Inspector General's review of the Library of Congress' utilization of its multifunction devices. The executive summary begins on page *i* and our complete findings and recommendations appear on pages 3 to 13. Management's responses to our draft report are briefly summarized in the Executive Summary and after individual recommendations. The complete responses are included as appendices A and B. This report will be publicly available.

Based on the written comments to the draft report, we consider all of the recommendations resolved. In accordance with LCR 211-6, Section 11.A, please provide, within 30 calendar days, an action plan addressing the implementation of the recommendations, including implementation dates.

We appreciate the cooperation and courtesies extended to our staff during this review by Information Technology Services and Integrated Support Services.

cc: Chief Operating Officer
Assistant Chief Operating Officer for Support Services
Associate Librarian for Strategic Initiatives
Director, Information Technology Services
Director, Integrated Support Services

⏩ TABLE OF CONTENTS

⏩ EXECUTIVE SUMMARY

The Office of the Inspector General conducted a review of the Library's underutilized multifunction devices (MFDs). MFDs are office machines that combine two or more document management functions, such as copying, scanning, printing, or faxing. Because MFDs have enhanced features and services, they are generally priced higher than standard copiers.

In October 2005, the Library entered into a five year, $5.8 million contract with a vendor for 234 MFDs and standard copiers for administrative, print shop, and public use. The Library's Information Technology Services (ITS) and Integrated Support Services (ISS) developed plans to network the MFDs to allow Library staff to utilize the enhanced features and services. However, those plans were never fully implemented.

Because ITS and ISS did not successfully network the MFDs, the Library paid for equipment and software that it did not fully utilize. In addition, the Library is contractually obligated to pay for pages printed (volume) allowances that exceed its actual usage. We estimate that the Library will have paid at least $563,000 over the life of the contract for features and services it did not use.

We found that the following factors contributed to ITS and ISS' unsuccessful efforts to network the MFDs:

- ***ITS and ISS did not follow IT security procedures***–When the contract was signed in 2005, the Library had policies and procedures in place for IT security and certification and accreditation (C&A). In addition, NIST 800-37 provided a detailed framework and best practices for the C&A process.[1] However, we found that neither ITS nor ISS followed the Library's own policies or federal best practices for the C&A process;

[1] National Institute of Standards and Technology (NIST) Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

- ***Unreasonable additional requirements***–ITS officials stated that the vendor was responsible for performing C&A activities and for providing an accreditation package for the MFDs. However, we found that ITS' requirements were not specified in the contract, which specifically stated that the vendor was not required to provide a C&A package; and

- ***Emerging priorities***–As several years passed without much progress being made toward networking the MFDs, ITS and ISS managers began to refocus staff on higher priority projects, such as the Facility Asset Management Enterprise project.

Finally, in the absence of a successful Library-wide plan to network the MFDs, several service units connected their MFDs to the Library's network without ITS' knowledge and without undergoing a formal security review. To help mitigate potential security risks, it is important to ensure that MFDs are properly configured and secured before they are connected to a network.

We recommend that ISS ensure that the cost structure for the next contract provides more transparency. We also recommend that ITS and ISS properly communicate security requirements to all stakeholders, and follow the Library's policies and best practices for systems security certification and accreditation.

The current contract term ends in September 2010 and ISS is in the early phases of the selection process for a new contract.

ITS and ISS management agreed with our recommendations. However, ITS disagreed with several points in our report. See appendices A and B.

⏩ BACKGROUND

A multifunction device (MFD) is an office machine that combines the functions of two or more document management devices, such as a copier, scanner, printer, or fax. Because MFDs have enhanced features and services, they are generally priced higher than standard copiers. MFDs must be connected to a network to allow users to fully utilize the enhanced features and services. High capacity commercial MFDs, like the one pictured below, have internal operating systems and hard drives that allow users to share documents over a network and store large amounts of data.

Commercial Multifunction Device

MFDs are described as "computers in-and-of themselves, running an embedded operating system, advertising a variety of network services, and sporting gigabytes of hard drive space."[2] Accordingly, the Library's Information Technology Services (ITS) has classified MFDs as an Information Technology (IT) system and requires MFDs to undergo a Certification and Accreditation (C&A) process before they are connected to the Library's network. The purpose of the C&A process is to identify and evaluate security risks and to help ensure that appropriate controls are in place to protect the Library's critical systems and data.

[2] SANS Institute Reading Room, *Auditing and Securing Multifunction Devices*, January 25, 2007.

⏩ OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this project were to (1) determine the reasons why efforts to fully utilize the MFDs were unsuccessful, (2) evaluate the impact of not fully utilizing the MFDs, including determining the cost difference between the MFDs and standard copiers, and (3) identify lessons learned and any needed recommendations for the new contract selection process.

We interviewed managers and staff from ITS and Integrated Support Services (ISS) – Office of Systems Services. In addition, we interviewed account managers and client representatives from the Library's current MFD/copier contract vendor. We also reviewed and evaluated internal correspondence, contract documentation, cost reports, project plans, equipment specifications, and security reports and studies related to MFDs.

We performed our work from January 19, 2010 through February 12, 2010. The scope of our inspection included the cost structure of the MFD/copier contract in effect from October 2005 through September 2010 and ITS' and ISS' attempts to network the MFDs from 2004 through 2007. The scope of our inspection did not include the original selection process or ongoing management of the contract.

We conducted this inspection in accordance with Quality Standards for Inspections, issued by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency, and with Library of Congress Regulation (LCR) 211-6, *Functions, Authority, and Responsibility of the Inspector General*.

⏩ FINDINGS AND RECOMMENDATIONS

I. The Library Entered into a $5.8 Million Contract to Use Multifunction Devices and Copiers

In October 2005, the Library entered into a 5 year, $5.8 million contract with a vendor to use 234 MFDs and standard copiers for administrative, print shop, and public use. ISS was responsible for coordinating the vendor selection process and for managing the contract after the selection was made. According to the contract's statement of work, "ISS/OSS seeks an enterprise wide solution for its copy and print needs that will provide the best operational and cost efficient copier/print service for the Library."

Under the terms of the contract, the vendor agreed to provide the equipment, supplies (excluding paper), services, and on-site staff necessary to support three main programs:

1. *Administrative Program*–This program provides standard and special use MFDs for the Library's service units, divisions, and administrative offices.

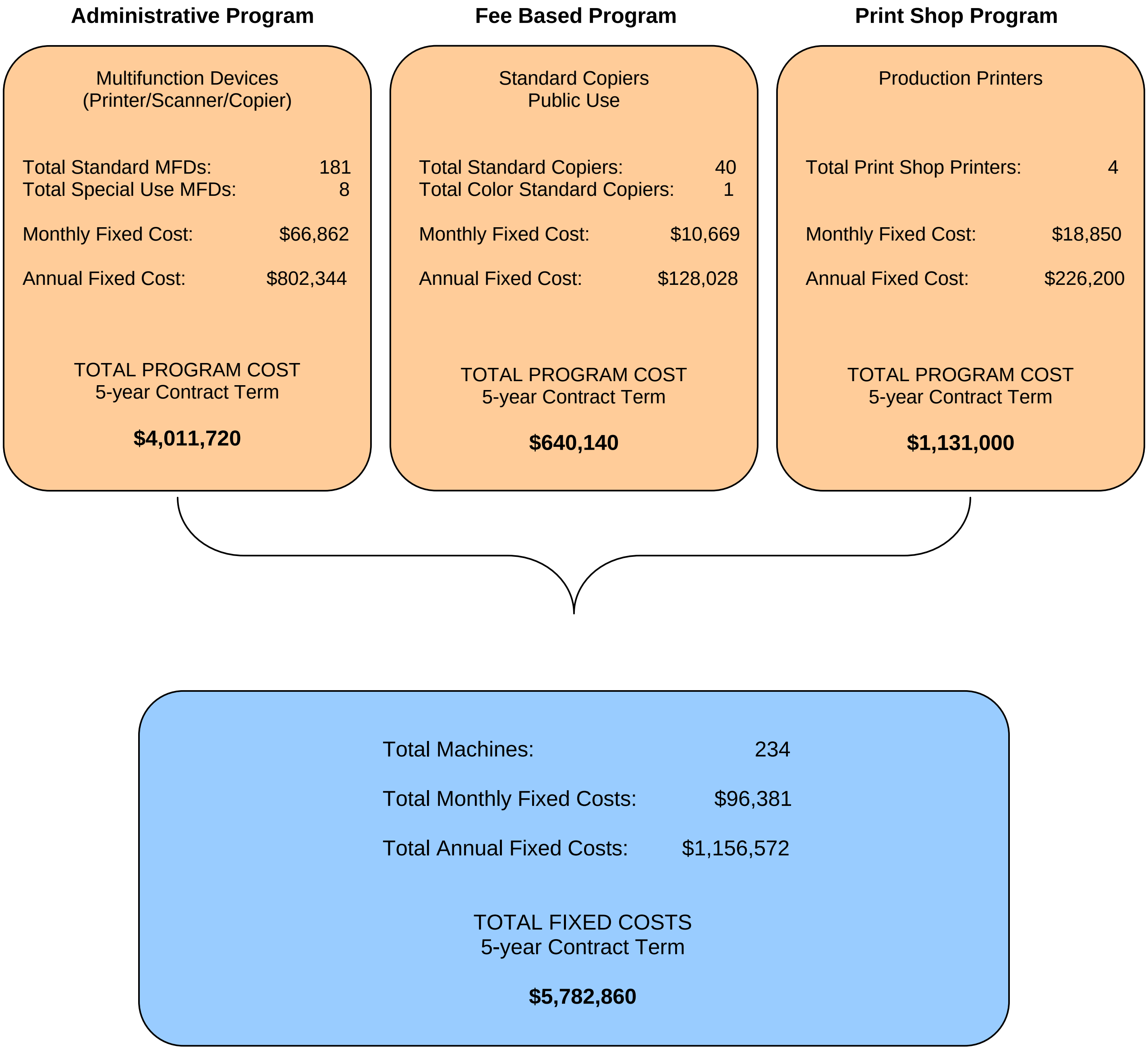
2. *Fee Based Program*–This program provides standard copiers for public use in the Library's reading rooms.

3. *Print Shop Program*–This program provides high capacity production printers for the Library's print shop, which offers limited in-house printing and photoduplication services.

The Library pays the vendor a monthly fixed amount based on the combined costs of the equipment, minimum allowance of pages printed (volume), on-site staff, and related services and supplies for each program. See Figure 1 on page 4 for a summary of the fixed costs for each program.

The MFDs, copiers, and production printers are the property of the vendor. The vendor is required to remove all equipment from the Library's premises at the end of the contract term, which ends in September 2010.

Figure 1: Summary of Contract Programs and Fixed Costs[3]



Administrative Program

Multifunction Devices
(Printer/Scanner/Copier)

Total Standard MFDs:	181
Total Special Use MFDs:	8
Monthly Fixed Cost:	$66,862
Annual Fixed Cost:	$802,344

TOTAL PROGRAM COST
5-year Contract Term

$4,011,720

Fee Based Program

Standard Copiers
Public Use

Total Standard Copiers:	40
Total Color Standard Copiers:	1
Monthly Fixed Cost:	$10,669
Annual Fixed Cost:	$128,028

TOTAL PROGRAM COST
5-year Contract Term

$640,140

Print Shop Program

Production Printers

Total Print Shop Printers:	4
Monthly Fixed Cost:	$18,850
Annual Fixed Cost:	$226,200

TOTAL PROGRAM COST
5-year Contract Term

$1,131,000

Total Machines:	234
Total Monthly Fixed Costs:	$96,381
Total Annual Fixed Costs:	$1,156,572

TOTAL FIXED COSTS
5-year Contract Term

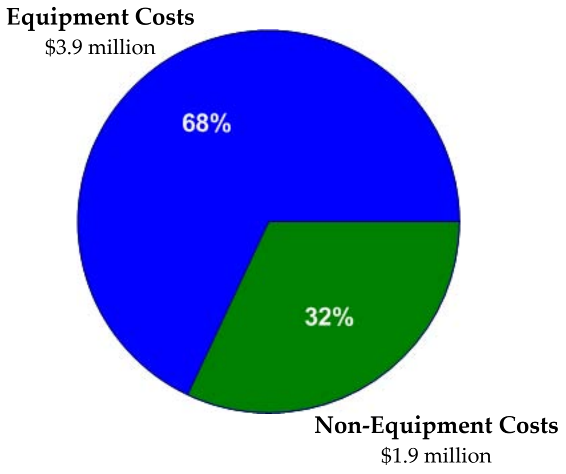
$5,782,860

[3] Fixed costs do not include pages printed (volume) overage charges and minor adjustments to the monthly fixed payments during the initial phase of the contract term.

II. The Library Paid for Underutilized Equipment and Services for the Duration of the 5-year Contract

Several key components of the contract's pricing structure were based on the assumption that the Library would network and fully utilize the MFDs' capabilities. However, because ITS' and ISS' efforts to network the MFDs were unsuccessful, the Library paid for equipment and services that it did not fully utilize. The Library also paid for estimated minimum volume allowances for pages printed despite the fact that actual volumes were well below the minimums.

Figure 2: Cost Breakdown
5-Year Contract Term



Underutilized equipment and software costs - The Library pays the vendor a monthly fixed amount for equipment costs (MFDs, standard copiers, print shop printers) and non-equipment costs (volume, services, and supplies). The breakdown of how much the Library pays for each component of the fixed amount is not specified in the contract. However, based on a detailed cost report provided by the vendor, we determined that approximately 68 percent of the Library's fixed amount is for equipment costs and 32 percent is for non-equipment costs (Figure 2).

The vendor's MFDs are priced higher than standard copiers because the MFDs have enhanced features and networking capabilities. According to the vendor, the Library received discounts during the initial contract negotiation process that offset the price differences between the MFDs and the standard copiers. However, based on an analysis of a detailed cost list provided by the vendor, we determined that the Library pays more for the MFDs than the standard copiers. As we discuss in Finding III, the Library primarily uses the MFDs as standard copiers because ITS' and ISS' efforts to network the MFDs were unsuccessful. We estimated the total cost difference between the 181 MFDs and the equivalent number of standard copiers to be approximately $506,000 over the 5 year contract term. We also found that the Library paid for document sharing software that was never used because the MFDs were not networked. We estimated the total cost of this software to be approximately $23,034 over the 5 year contract term (see Table 1 on page 6).

Table 1: Estimated Costs of Underutilized Equipment, Software, and Volume[4]

Equipment Cost Difference: 5-year Contract Term	506,914
Unused Software Cost: 5-Year Contract Term	23,034
Total Estimated Cost of Underutilized Equipment and Software	**$ 529,948**
Estimated Cost of Unused Volume Allowance	33,118
Total Estimated Cost of Underutilized Equipment, Software, and Volume	**$ 563,066**

Overestimated equipment usage – A portion of the Library's non-equipment costs includes usage of the MFDs, standard copiers, and print shop printers as measured by the number of pages printed (volume). The contract requires the Library to pay for pre-established minimum monthly volume allowances for each program. According to an ISS official, the minimum volume allowances were established in 2005 and were based on an estimate of predicted use. However, the actual volumes for the MFDs, copiers, and print shop printers were consistently less than the estimated minimums. The ISS official noted that volumes have dropped industry-wide. The average monthly volume for the print shop program ranged from 136,031 to 301,106 below the minimum volume for which the Library paid. The average monthly volume for the administrative program ranged from 43,988 to 209,544 below the minimum.

According to an ISS official, the print shop printers are not fully networked. Had the Library networked the printers, staff would have the ability to send print jobs directly to the print shop without using more costly desktop printers. The increased usage from networking the print shop printers would have increased the volume counts. Based on volume allowance cost information provided by the vendor, we estimate the cost of the unused volume allowance for the print shop and administrative programs to be at least $33,118.

[4] Cost estimates are based on actual equipment and software costs provided by the vendor and a straight-line proportional allocation of non-equipment costs. Unused volume cost estimates are based on a volume cost reduction proposal provided by the vendor and the average unused volume counts for calendar years 2006 to 2009.

Recommendation

We recommend that ISS ensure that the cost structure for the next contract provides more transparency regarding how much the Library pays for equipment, services, and supplies and allows for flexibility based on actual use rather than predetermined estimates.

Management Response

ISS agreed with our finding and recommendation. ITS did not comment specifically on this issue.

III. Misapplied IT Security Procedures and Emerging Priorities Hindered Efforts to Network the MFDs

LCR 1620 requires C&A for all information systems prior to implementation. Although ISS was the designated system owner and was responsible for overseeing C&A activities for the MFDs, ITS was actively involved in efforts to network the MFDs. Specifically, ITS managers:

- Served on the technical evaluation team that recommended the vendor,
- Developed the IT security and networking requirements for the original contract,
- Participated in meetings with the vendor to discuss IT security requirements and networking the MFDs, and
- Managed the ITS and ISS 2007 project to network the MFDs.

We found that the following factors contributed to ISS' and ITS' unsuccessful efforts to network the MFDs:

ITS and ISS did not follow IT security procedures–When the contract was signed in 2005, the Library had policies and procedures in place for IT security and C&A. In addition, NIST 800-37 provided a detailed framework and best practices for the C&A process. [5] However, we found that neither ITS nor ISS followed the Library's policies or federal best practices for the C&A process. Specifically, ITS managers expected the

[5] National Institute of Standards and Technology (NIST) Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

vendor to perform C&A activities for the MFDs and provide an accreditation package, which is neither in compliance with LCR 1620, nor in line with federal best practices. An accreditation package includes an approved system security plan, a security assessment report, and plan of action and milestones. NIST 800-37 states that the information system owner is responsible for preparing the system security plan and plan of action and the certifying agent is responsible for the security assessment report. LCR 1620 requires representatives from the service units, not system vendors, to serve as system owners.

Unreasonable additional requirements–ITS' requirements that the vendor perform C&A activities and provide an accreditation package were not specified in the contract, which specifically stated that the vendor was not required to provide a C&A package for the MFDs. The additional requirements caused delays in efforts to network the MFDs. Overall, we found that the vendor complied with key contract requirements for IT security and provided sufficient documentation and technical assistance to help the Library network the MFDs. Table 2 on page 9 summarizes key contract requirements and the vendor's compliance with those requirements.

Cross-walk of Contract Requirements to Vendor Actions

Contract Requirement	Vendor Action
The vendor must comply with the Library's IT security requirements for networked devices in accordance with ITS security directives.	According to a 2005 internal email, the ITS team that was responsible for evaluating the contract proposals stated, "[the vendor] did a good job of answering questions and addressing ITS' directives and security concerns."
The equipment must have the ability to meet all federal laws for securing information systems. The contract further states, "[t]his does not mean that a system security Certification and Accreditation package has to come with the devices."	The specific MFD models that the vendor provided were tested by the National Security Agency and have received Common Criteria Certification. Common Criteria Certification is a process that includes product testing by a third-party laboratory that has been accredited by the National Voluntary Laboratory Accreditation Program to perform evaluation of products against security requirements.
The equipment must have system documentation and be configurable to get to a security posture within 6 months of the contract award at an acceptable level of residual risk.	Representatives from the vendor indicated that their technical team provided the following documentation to ITS and ISS staff: • Information Assurance Disclosure Paper (provides detailed technical information regarding the MFDs) • Common Criteria Evaluation Questions and Answers • Presentation on Security and MFD Systems • Detailed diagram showing the integration of the MFDs with the Library's servers. Representatives from the vendor met with ITS staff after the contract was awarded. In addition, the vendor has extensive experience providing similar security documentation to its other federal clients including the Department of Defense, National Security Agency, and the White House, all of which have successfully networked the vendor's MFDs.

Other Emerging Priorities–In October 2007, two years after the inception of the contract, ITS and ISS developed a formal plan to network the MFDs. As several years passed without much progress being made toward networking the MFDs, ITS and ISS managers began to refocus key staff, including the ITS plan project manager, on other emerging priorities, such as the Facility Asset Management Enterprise project.

In March 2009, ITS and ISS initiated a new effort to network the MFDs. As of March 2010, that project is still in the testing phase and the Library's MFDs continue to be used primarily as standard copiers.

Recommendations

We recommend that ITS and ISS:

1. Ensure that security requirements for the new contract are clearly documented and communicated to the vendor before any future contract is signed, and

2. For the new contract, follow the Library's policies and procedures and federal best practices for systems security certification and accreditation.

Management Response and OIG Comments

ITS Response and OIG Comments – ITS agreed with our recommendations. ITS also agreed that the contract's IT security requirement language was inadequate. We reiterate that this fact contributed to a general misunderstanding between ITS and ISS regarding IT security requirements and roles and responsibilities.

However, ITS disagreed with several points regarding efforts to network the MFDs. Specifically, ITS stated that C&A was never attempted on the MFDs and that it never required the vendor to perform C&A on the MFDs. However, internal correspondence shows that ITS and ISS made several attempts to initiate the C&A process for the MFDs during the five year contract period. As we discuss on page 8, those attempts were not in line with the Library's polices or federal best practices because ITS managers expected the vendor to perform C&A activities that were actually the responsibility of the system owner (ISS). Specifically, the ITS Deputy Director and the ITS Assistant Director for Operations, who have been involved in efforts to network the MFDs since 2004, stated that they expected the vendor to perform C&A activities and to provide an accreditation package. However, the Library's contract specifically stated that the vendor was not required to provide a C&A package for the MFDs (see page 8 for additional information).

Finally, ITS stated that the vendor-provided documents listed in Table 2 were insufficient to assist with C&A on the MFDs. We disagree. These documents provided detailed technical information and security specifications for the MFDs. As we discuss in finding IV, the vendor complied with key contract requirements for IT security and provided sufficient documentation and technical assistance to help the Library network the MFDs. It was ultimately the responsibility of ISS, with assistance from ITS, to complete C&A on the MFDs. In its response, ISS also notes that due to its limited expertise in the field, "[it] deferred to ITS for their expertise and input during all phases of the … procurement…"

ISS Response – ISS agreed with our finding and recommendations.

IV. Network Security Concerns Should be Addressed Before Entering into a New Contract

To help mitigate potential security risks, it is important to ensure that MFDs are properly configured and secured before they are connected to a network. Security risks associated with MFDs include unauthorized disclosure of sensitive and confidential information.[6] For example, scanned, printed, and copied documents that are stored in logs and hard drives can be accessed and modified. In addition, individuals can gain unauthorized access to an organization's network, and by extension its critical systems and data, through Web servers that are used to manage MFDs or viruses and other malicious software disguised as print files in an MFD's print queue.

Despite the absence of a successful Library-wide plan to network the MFDs, several service units connected their MFDs to the Library's network without ITS' knowledge and without undergoing a formal security review. In November 2009, ITS discovered at least six unauthorized MFDs on the Library's network. Some of the MFDs had remained undetected on the Library's network for over nine months. According to a memo from ITS security staff to the Library's executive managers, "[t]hese devices constitute an IT system and must undergo Certification & Accreditation (C&A) before being placed on the [Library's network]. Connection of these devices is in violation of LCR 1620 and the IT Security Directives and is considered a Category 1 Security Incident."

A Category 1 incident is defined as unauthorized access and occurs when an individual gains access to a federal agency's network, systems, applications, data, or other resources

[6] California Office of Information Security and Privacy Protection, *Security Considerations for Multi-Function Devices (MFD,)* January 7, 2009.

without permission.[7] Despite the apparent severity of this incident, ITS granted security waivers to the service units responsible for the six unauthorized MFDs, and did not move the unauthorized MFDs to a secure network in accordance with best practices and as stated in the internal memo to the Library's executive managers. The ITS Security Operations Center reported that it began receiving weekly network scanning reports in December 2009 to help detect unauthorized MFDs on the Library's network.

The current contract term ends in September 2010 and ISS is in the early phases of the selection process for a new contract. Therefore, ITS should address network security concerns before the Library enters into a new contract.

Recommendation

We recommend that ITS strengthen network security controls over detecting unauthorized devices on the Library's network and follow established guidelines and best practices for configuring and securing MFDs, such as the Defense Information Systems Agency's *MFD Security Technical Implementation Guide*.

Management Response and OIG Comments

ITS agreed with our recommendation. However, it disagreed with several points. Specifically, ITS stated that the security incident regarding the unauthorized MFDs was not severe. This is inconsistent with the concept of a C&A, which is to assess the risk presented by a system. Without a risk assessment, ITS has no way of assuring the Library that this particular incident was "not severe." Further, ITS' statement is inconsistent with its November 2009 memo to the Library's executive managers, which stated, "[c]onnection of these devices is in violation of LCR 1620 and the IT Security Directives and is considered a "Category 1 Security Incident." The memo also stated that ITS would move the unauthorized MFDs to a secure network. As of April 2010, ITS had not yet done so.

[7] United States Computer Emergency Readiness Team (US-CERT), Federal Agency Incident Categories.

ITS also disagreed that there is risk in its inability to effectively detect unauthorized devices on the Library's network. We disagree. We believe that ITS' inability to detect unauthorized connections for as long as nine months does, in fact, pose a potentially significant risk to the Library's systems. We reiterate our recommendation for ITS to strengthen network security controls and to follow best practices for configuring and securing networked MFDs.

ITS further notes that "the waiver process was properly followed" with respect to the unauthorized connections. We disagree. A proper waiver process requires that a waiver be issued *prior* to the occurrence of the event in question. In this case, the waivers were not issued until well after the unauthorized connections occurred.

⏩ CONCLUSION

The lack of planning and coordination between ITS and ISS caused a significant waste of Library funds.

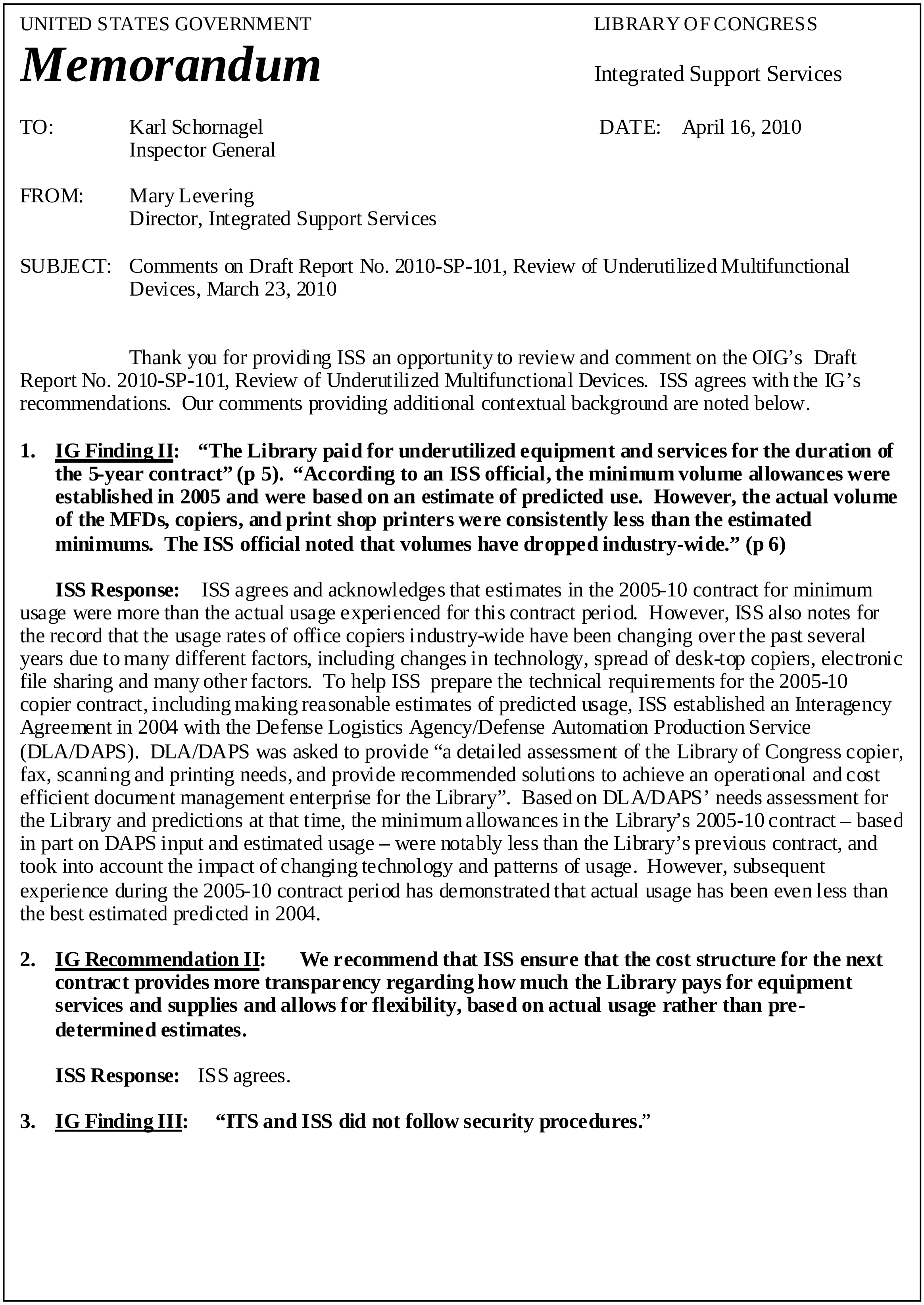
We are somewhat puzzled by ITS' response to this report, in which it disputes several key points. Namely, ITS contends that:

- A C&A was never attempted. This is clearly incorrect, as demonstrated by its own written correspondence on the subject, derived from both ITS and ISS;
- ITS never expected the vendor to perform a C&A; this is also clearly incorrect, as demonstrated by ITS' own documentation; and
- The undetected connection of the MFDs to the network resulted in a limited risk. However, its own memo contradicts this statement by characterizing the connections as a "Category 1 Security Incident" and requesting that the devices be removed from the network.

Finally, as a general observation, we believe that ISS made its best efforts to follow Library policy and procedure regarding the IT component of the contract. We recognize that ISS did not have sufficient expertise to conduct a C&A without significant guidance from ITS. We also recognize that at the time, the Library's IT security policies were relatively new. Since then, the Library has made progress in improving those policies (although, as is apparent by the failure to detect the unauthorized connections for nine months, the Library may have further to go in implementing those policies).

Major Contributors to This Report:
Nicholas Christopher, Assistant Inspector General for Audits
John Mech, Lead Auditor
Jessica Tucker, IT Auditor
Larry Olmsted, Information Technology Specialist (Information Security)
Peter TerVeer, Management Analyst

APPENDIX A: ISS RESPONSE



UNITED STATES GOVERNMENT LIBRARY OF CONGRESS

Memorandum Integrated Support Services

TO: Karl Schornagel DATE: April 16, 2010
Inspector General

FROM: Mary Levering
Director, Integrated Support Services

SUBJECT: Comments on Draft Report No. 2010-SP-101, Review of Underutilized Multifunctional Devices, March 23, 2010

Thank you for providing ISS an opportunity to review and comment on the OIG's Draft Report No. 2010-SP-101, Review of Underutilized Multifunctional Devices. ISS agrees with the IG's recommendations. Our comments providing additional contextual background are noted below.

1. **IG Finding II: "The Library paid for underutilized equipment and services for the duration of the 5-year contract" (p 5). "According to an ISS official, the minimum volume allowances were established in 2005 and were based on an estimate of predicted use. However, the actual volume of the MFDs, copiers, and print shop printers were consistently less than the estimated minimums. The ISS official noted that volumes have dropped industry-wide." (p 6)**

   ISS Response: ISS agrees and acknowledges that estimates in the 2005-10 contract for minimum usage were more than the actual usage experienced for this contract period. However, ISS also notes for the record that the usage rates of office copiers industry-wide have been changing over the past several years due to many different factors, including changes in technology, spread of desk-top copiers, electronic file sharing and many other factors. To help ISS prepare the technical requirements for the 2005-10 copier contract, including making reasonable estimates of predicted usage, ISS established an Interagency Agreement in 2004 with the Defense Logistics Agency/Defense Automation Production Service (DLA/DAPS). DLA/DAPS was asked to provide "a detailed assessment of the Library of Congress copier, fax, scanning and printing needs, and provide recommended solutions to achieve an operational and cost efficient document management enterprise for the Library". Based on DLA/DAPS' needs assessment for the Library and predictions at that time, the minimum allowances in the Library's 2005-10 contract – based in part on DAPS input and estimated usage – were notably less than the Library's previous contract, and took into account the impact of changing technology and patterns of usage. However, subsequent experience during the 2005-10 contract period has demonstrated that actual usage has been even less than the best estimated predicted in 2004.

2. **IG Recommendation II: We recommend that ISS ensure that the cost structure for the next contract provides more transparency regarding how much the Library pays for equipment services and supplies and allows for flexibility, based on actual usage rather than pre-determined estimates.**

   ISS Response: ISS agrees.

3. **IG Finding III: "ITS and ISS did not follow security procedures."**

ISS Response/Comment: ISS acknowledges that the ISS Directorate managers had very limited experience with, and understanding of, IT security requirements during 2003 and 2004 when the requirements were being developed for the 2005-10 Copier Contract and that ISS may not have adequately followed IT security procedures. Because of ISS limited experience with IT security requirements, ISS management deferred to ITS for their expertise and input during all phases of the 2005 copier procurement, from requirements determination all the way through to their being a member on the Source Selection Panel for the contract. Additionally, ISS worked closely with ITS security experts to obtain specific guidance concerning the myriad of ITS security requirements and directives which the system would need to meet in order to have the MFD's networked on the LCDN.

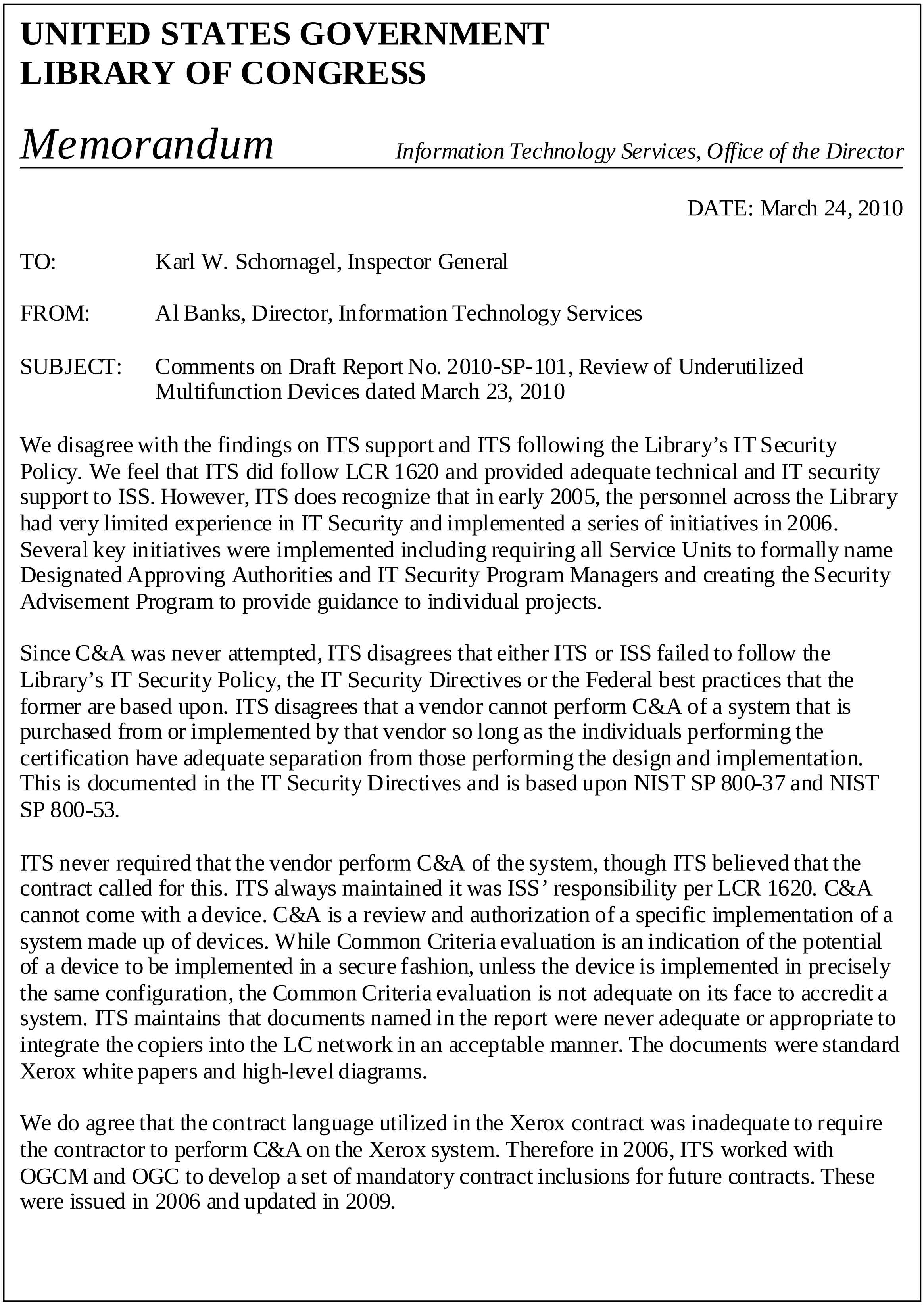
During this period, ISS management also recognized that a strong IT security program was needed for the ISS Directorate and the ISS director developed plans during 2005 for building a much stronger IT security program for the ISS Directorate. After analyzing the directorate's needs, the ISS Director created a new position description during 2005 for an ISS Chief Automation Officer at the GS-15 level, recruited for and hired an experienced IT professional in May 2006, one who had a particularly strong background in IT security. Subsequently ISS also provided funding for an expert IT security consultant during the period FY 07- FY 09 to help the ISS Chief Automation Officer build a strong, internal IT security program for ISS that is completely compliant with federal and LC IT security requirements. These initiatives led to successful completion of the C&A process (certification and accreditation) for 3 major ISS systems – Tririga's Space Planning System/Computer Aided Facility Management (CAFM) for the Facility Services division and Medgate's Medical Information Management System (MIMS) for the Health Services Office during that period, followed by successful completion of C&A for the Event Planning Suite during FY 09. Additionally, ISS and ITS working together during the past year just completed this month (April) the successful C&A process for placing the MFD's on the LCDN. As ISS has gained more understanding and experience with IT security requirements, the ISS IT security program has also grown much stronger and is now, we believe, fully compliant with all requirements.

4. <u>IG Recommendation II</u>: **We recommend that ISS and ITS: (1) Ensure that security requirements for the new contract are clearly documented and communicated to the vendor before any future contract is signed; and (2) for the new contract, follow the Library's policies and procedures and federal best practices for systems security certification and accreditation. (p 10)**

   ISS Response: ISS agrees.

cc: Nicholas Christopher, OIG
Lucy Suddreth, LIBN
Al Banks, ITS
Steve Elky, ITS
Robert Williams, ISS/OSS
Dingshin Yu, ISS/AUTO

APPENDIX B: ITS RESPONSE



UNITED STATES GOVERNMENT
LIBRARY OF CONGRESS

Memorandum *Information Technology Services, Office of the Director*

DATE: March 24, 2010

TO: Karl W. Schornagel, Inspector General

FROM: Al Banks, Director, Information Technology Services

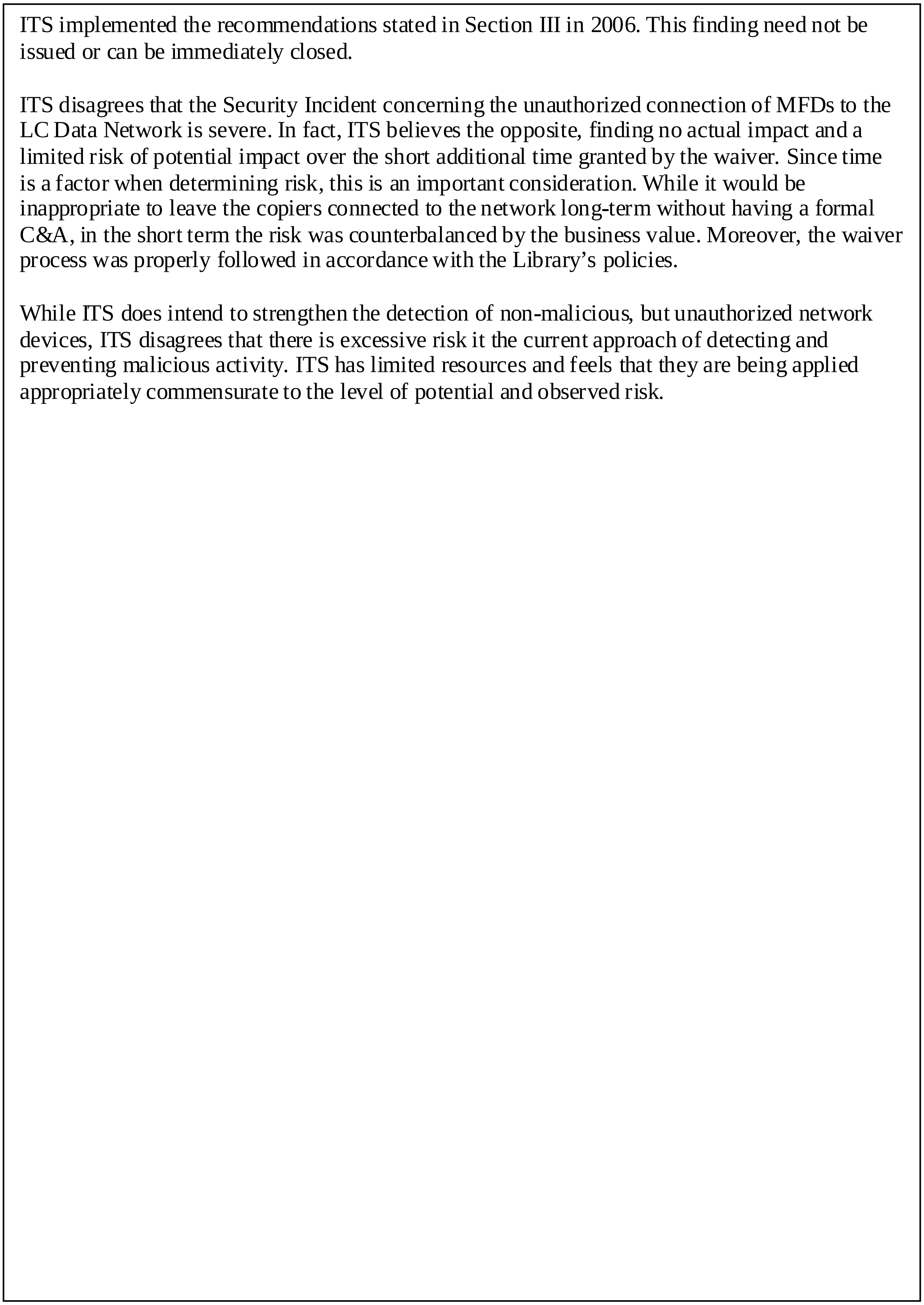
SUBJECT: Comments on Draft Report No. 2010-SP-101, Review of Underutilized Multifunction Devices dated March 23, 2010

We disagree with the findings on ITS support and ITS following the Library's IT Security Policy. We feel that ITS did follow LCR 1620 and provided adequate technical and IT security support to ISS. However, ITS does recognize that in early 2005, the personnel across the Library had very limited experience in IT Security and implemented a series of initiatives in 2006. Several key initiatives were implemented including requiring all Service Units to formally name Designated Approving Authorities and IT Security Program Managers and creating the Security Advisement Program to provide guidance to individual projects.

Since C&A was never attempted, ITS disagrees that either ITS or ISS failed to follow the Library's IT Security Policy, the IT Security Directives or the Federal best practices that the former are based upon. ITS disagrees that a vendor cannot perform C&A of a system that is purchased from or implemented by that vendor so long as the individuals performing the certification have adequate separation from those performing the design and implementation. This is documented in the IT Security Directives and is based upon NIST SP 800-37 and NIST SP 800-53.

ITS never required that the vendor perform C&A of the system, though ITS believed that the contract called for this. ITS always maintained it was ISS' responsibility per LCR 1620. C&A cannot come with a device. C&A is a review and authorization of a specific implementation of a system made up of devices. While Common Criteria evaluation is an indication of the potential of a device to be implemented in a secure fashion, unless the device is implemented in precisely the same configuration, the Common Criteria evaluation is not adequate on its face to accredit a system. ITS maintains that documents named in the report were never adequate or appropriate to integrate the copiers into the LC network in an acceptable manner. The documents were standard Xerox white papers and high-level diagrams.

We do agree that the contract language utilized in the Xerox contract was inadequate to require the contractor to perform C&A on the Xerox system. Therefore in 2006, ITS worked with OGCM and OGC to develop a set of mandatory contract inclusions for future contracts. These were issued in 2006 and updated in 2009.



ITS implemented the recommendations stated in Section III in 2006. This finding need not be issued or can be immediately closed.

ITS disagrees that the Security Incident concerning the unauthorized connection of MFDs to the LC Data Network is severe. In fact, ITS believes the opposite, finding no actual impact and a limited risk of potential impact over the short additional time granted by the waiver. Since time is a factor when determining risk, this is an important consideration. While it would be inappropriate to leave the copiers connected to the network long-term without having a formal C&A, in the short term the risk was counterbalanced by the business value. Moreover, the waiver process was properly followed in accordance with the Library's policies.

While ITS does intend to strengthen the detection of non-malicious, but unauthorized network devices, ITS disagrees that there is excessive risk it the current approach of detecting and preventing malicious activity. ITS has limited resources and feels that they are being applied appropriately commensurate to the level of potential and observed risk.