NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION

OFFICE *of* INSPECTOR GENERAL

Cotton & Company's Assessment of NARA's Cable Infrastructure

September 30, 2015

OIG Audit Report No. 15-15

Cotton&
Company

Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

James Springs
Inspector General
National Archives and Records Administration
8601 Adelphi Rd, Room 1300
College Park, MD 20740

Subject: Assessment of the Cable Infrastructure of the National Archives and Records Administration

Cotton & Company LLP is pleased to submit this independent audit report on its assessment of NARA's existing communication cabling infrastructure. We conducted a review of NARA's information security policies, procedures, and technical controls over its cabling infrastructure and information technology controls in accordance with Generally Accepted Government Auditing Standards (GAGAS), as established in the Government Accountability Office (GAO)'s *Government Auditing Standards*, December 2011 Revision. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We carried out testing during the period from October 1, 2014, through July 20, 2015. We discussed our observations and conclusions with management officials on August 17, 2015, and included their comments where appropriate. We did not audit NARA's responses, and accordingly, we express no opinion on them.

Sincerely,

COTTON & COMPANY LLP

George E Bills

George E. Bills, CPA, CISSP, CISA, CIPP
Partner, Information Assurance

September 30, 2015
Alexandria, Virginia

Table of Contents

Executive Summary

Cotton & Company LLP assisted the National Archives and Records Administration (NARA) Office of Inspector General (OIG) in assessing NARA's existing communications cabling infrastructure by evaluating and auditing NARA's computer rooms, network closets, and communications cabling at 39 NARA-owned or -leased locations to provide recommendations to better ensure that NARA's infrastructure will support current and emerging technologies. The purpose of this engagement was to:

1. Evaluate NARA's existing cabling infrastructure for each location against National Institute of Standards and Technology (NIST) standards and Telecommunications Industry Association (TIA)/Electronic Industries Alliance (EIA) 7-568 telecommunications standards, including:
    a. NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
    b. NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*
    c. ANSI/TIA-568-C.0, *Generic Telecommunications Cabling for Customer Premises*
    d. ANSI/TIA-568-C.1, *Commercial Building Telecommunications Cabling Standard*
    e. ANSI/TIA-568-C.2, *Balanced Twisted-Pair Telecommunication Cabling and Components Standard*
    f. ANSI/TIA-568-C.3*, Optical Fiber Cabling Components Standard*
    g. ANSI/TIA-568-C.4, *Broadband Coaxial Cabling and Components Standard*
2. Evaluate NARA's existing cabling infrastructure for each location compared to current and future technology needs, such as cloud computing, Video Teleconferencing (VTC), or Voice over Internet Protocol (VOIP).
3. Review bandwidth utilization reports at each location to ensure that adequate networking capabilities are in place.
4. Evaluate NARA's existing wired architecture and design documentation, including network diagrams and device configurations.
5. Identify security vulnerabilities in the cabling infrastructure.
6. Develop recommendations for improvement.

Overall, we determined that NARA is effectively managing its communications cabling infrastructure. Specifically, we noted that the NARA Security Management Division (BX) performs site reviews on a three-year rotational basis for all NARA locations to evaluate select physical, environmental, and infrastructure-related controls. Additionally, cables used at all locations were largely in line with industry best practice standards, including category 5e, category 6, and fiber, which support high-speed gigabit transfer rates. Finally, review of bandwidth reports for all NARA locations revealed that current bandwidth allotments appear adequate to support day-to-day networking activities and continued growth, as current utilization on average, was well below the established bandwidth thresholds.

While we found that NARA was generally managing cable infrastructure appropriately, we did identify weaknesses in the consistency of its implementation of specific physical, environmental, and infrastructure controls, and in how the specific site assessments are communicated to security management to ensure that an appropriate understanding of risk is identified, communicated to affected individuals, and accepted by individuals responsible for documenting and approving security controls. These weaknesses, if exploited, could limit the agency's ability to perform operations that support its mission; could adversely impact the confidentiality, integrity, and availability of NARA's data and information systems; and could ultimately have a negative impact on the agency's ability to protect the security of its information or information systems. These weaknesses include:

- NARA Physical and Environmental (PE) policies only addresses the National Archives at College Park (Archives II) and are not inclusive of all NARA locations. Similarly, NARA does not have a system security plan (SSP) that addresses the specific PE controls at any NARA locations outside Archives II.
- PE, infrastructure, and cabling controls are inconsistently implemented across locations.
- Several sites have patch panels that are near capacity, increasing the risk that the respective locations will run out of ports to add new users and support continued growth.

A key cause of the weaknesses identified in this report is that NARA has not implemented the security assessment and authorization (SA&A) process for all of its locations. Specifically, while all NARA locations are included within the security boundary of the NARANet SA&A, their specific site controls are not addressed. Because changes regularly occur within organizations and new security risks are constantly being identified, full implementation of the SA&A process (which is addressed at tier 3[1], the information system level, of the Risk Management Framework [RMF]) is essential to ensure that systems and data supporting NARA's mission are adequately protected. Diagram 1 shows the formal steps carried out within tier 3 of the RMF. This process helps ensure that important systems are identified and that appropriate security controls are selected, implemented, and regularly assessed to ensure that they are working as intended.

[1] NIST SP 800-37 illustrates a three-tiered approach to risk management that addresses risk-related concerns at: (tier 1) the *organizational* level; (tier 2) the *mission and business process* level; and (tier 3) the *information system* level.

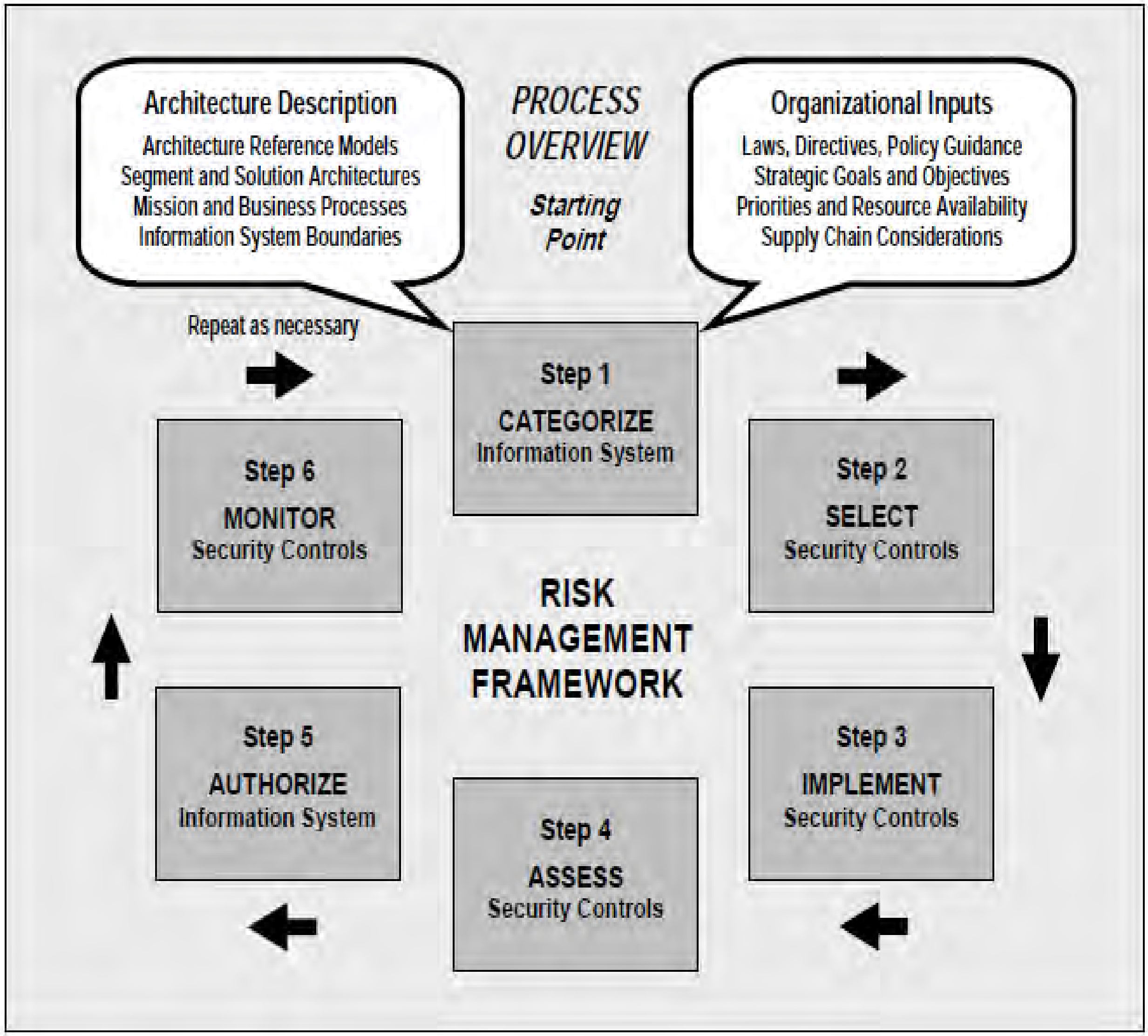

Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

Diagram 1

When implemented, the SA&A helps ensure that management is aware of the risks to their environment, and that the limited resources available are used to protect the systems and data most important to the organization's goals. Further, because this process is intended to be carried out continuously, an SA&A helps ensure that management continues to understand the risks present within their environment and the effectiveness of the controls as changes occur.

We are making three recommendations that we believe, once implemented, will address the weaknesses cited in this review.

Background

NARA's core network infrastructure is known as NARANet and is primarily administered from the Archives II location in College Park, Maryland, with local administration at field sites by Field Office System Administrators (FOSAs). Some sites have limited FOSA availability, with on-site visits limited to one to two days per month. If a significant issue arises that cannot be dealt with either remotely or by the FOSA, a member of the NARA IT team from Archives II can be dispatched to the site to resolve the issue.

Archives II monitors and maintains the health of NARANet primarily through the use of three monitoring and maintenance tools: SolarWinds, Riverbed, and Cisco LMS. All three tools have reporting capabilities. Through the use of these tools, Archives II can detect if a device is down, push out new Access Control Lists to routers and firewalls, implement new security policies and configurations to remote devices, and track bandwidth usage.

NARA has contracted with Century Link for Internet service. Based on the contract, data bandwidth to each site is throttled based on the purpose of the site and the number of users at the site that require access to NARANet. The bandwidth for each location is established as follows:

- 10.5 Mbps[2] for the National Archives and Federal Records Centers (FRCs) at Chicago, Dayton-Kingsridge, and Kansas City; the Office of the Federal Register in Washington, DC; and the Washington National Records Center in Suitland, MD;
- 100 Mbps for the National Archives and Natioanl Personnel Records Center (NPRC) in St. Louis, MO;
- 1 Gbps[3] for Rocket Center, WV;
- Dual 1 Gbps for Archives II in College Park, MD; and
- 45 Mbps for all other sites.

NARA locations include a variety of facility types, which impacts the cabling at those sites. These locations include NARA-controlled sites, General Services Administration (GSA)-controlled sites, and private leased facilities. Some of the sites are converted facilities, such as the Seattle Federal Records Center, which began as a military parts hanger for the United States Navy in 1944.

[2] Megabits per second

[3] Gigabits per second

Objectives, Scope, and Methodology

Cotton & Company's objective for this engagement was to assist the NARA OIG in assessing NARA's existing communications cabling infrastructure by evaluating and auditing NARA's computer rooms, network closets, and communications cabling at various NARA locations to provide recommendations to better ensure that NARA's infrastructure can support current and emerging technologies. Cotton & Company conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), as established in the Government Accountability Office (GAO)'s *Government Auditing Standards*, December 2011 Revision. To meet this objective, we:

1. Evaluated NARA's existing cabling infrastructure for each location compared to NIST standards and industry best practices.
2. Evaluated NARA's existing cabling infrastructure for each location compared to current and future technology needs, such as cloud computing, VTC, or VOIP.
3. Reviewed bandwidth utilization reports at each location to ensure that adequate networking capabilities are in place.
4. Evaluated NARA's existing wired architecture and design documentation, including network diagrams and device configurations.
5. Identified security vulnerabilities in the cabling infrastructure.
6. Developed recommendations for improvement.

We conducted our review in three distinct phases: planning, testing, and reporting. During the planning phase, we obtained a high-level understanding of NARA's information technology (IT) and infrastructure policies, procedures, and practices by reviewing available documentation and interviewing key individuals responsible for information security and facilities management. Based on our understanding of NARA's IT and security controls environment, we designed specific test procedures to assess the effectiveness of the cable infrastructure and information security controls. Cotton & Company's detailed test plan for assessing NARA's cable infrastructure was as follows:

1. Evaluate Policy and Procedures

Cotton & Company obtained NARA's PE control policies and procedures and reviewed them to ensure compliance with requirements outlined in NIST SP 800-53, Rev. 4, as well as to ensure that they appropriately address security considerations at each of NARA's physical locations. We also reviewed NARA policies and procedures to determine whether controls around the management of NARA's cable network infrastructure are appropriately developed and documented. Specifically, we reviewed NARA Directive 804, *Information Technology System Security*, and associated supplements, as well as select policy and procedures from the following NIST SP 800-53, Rev. 4 control areas:

- Configuration Management
- Contingency Planning
- Maintenance
- System and Communication

Key controls that we looked for during our review included:

- Detailed procedures regarding how wiring is to be performed at all NARA locations, including requirements related to location, length, color, and labeling of cables.
- Contingency planning policy and procedures that adequately address cable network infrastructure risks, constraints, and requirements.
- Up-to-date diagrams of the current network layout.
- Detailed policies and procedures describing when changes to the cable network infrastructure can be made, who can make the changes, and how the changes should be tested.

2. Test PE Controls

Cotton & Company conducted physical walkthroughs of selected NARA locations to determine whether PE controls were in place and operating as designed. Walkthroughs were focused on datacenters, wiring closets, and other key locations where cable network infrastructure is located and maintained. Testing covered each of the PE controls identified in NIST SP 800-53, Rev. 4. In addition to testing each of the PE controls, we also used our cable wiring checklist, which is based on industry best practices outlined in ANSI/TIA-568-C, to ensure that NARA's cable network is appropriately installed. This extensive checklist covers a wide range of best practices and includes assurances that:

- All horizontal cables are plenum-rated
- Cables are not lying directly on ceiling tiles or T-bars
- Cables are not wrapped or twisted around mounting collars
- Jackets remain up to the edge of connecting blocks
- There is no visible conductor insulation damage
- Pairs are terminated in the correct positions
- Bends in pairs are tight and conductors are not spread apart
- Visible sag is seen between hanging supports
- Conductors are seated according to the color chart on the outlet
- Cable runs are 300 feet or less

As part of our review, we also:

- Checked the types of cabling in use (e.g., Category 5e, Category 6, T568A, T568B, Fiber)
- Checked for bends, kinks, and crimps in the cable
- Checked that cables are away from any potential sources of EMI/RFI (e.g., power cables)
- If zip ties were used, checked for slack to prevent heavy pressure

- Checked that the category rating of the jack is appropriate for the category of the cable (e.g., Category-6-rated jacks with Category 6 cabling)
- Ensured that there is no splice or bridge between Category 5e and Category 6 cables
- Ensured that there is slack in cable runs, preferably at least 5 feet
- Ensured that standard staples are not used to secure Category 5 or Category 6 cabling
- Verified cables with a tester
- Checked for signs of cables being tugged or pulled
- Checked that copper wires are fully seated in the terminator
- Compared cables to diagrams
- Checked for "cable clutter"
- Ensured that labeling is complete and accurate in all work area outlets, telecommunication closets, and equipment rooms.

The above procedures were carried out at the following locations:

State	Name and Address of NARA Location
Arkansas	1. William J. Clinton Presidential Library and Museum 1200 President Clinton Avenue Little Rock, AR 72201
California	2. Laguna Niguel Records Management Chet Holifield Federal Building 24000 Avila Road 1st Floor, East Entrance Laguna Niguel, CA 92677-3497
	3. National Archives & FRC at Riverside 23123 Cajalco Road Perris, CA 92570
	4. National Archives & FRC at San Francisco Leo J. Ryan Building 1000 Commodore Drive San Bruno, CA 94066-2350
	5. Richard Nixon Presidential Library and Museum 18001 Yorba Linda Boulevard Yorba Linda, CA 92886-3903
	6. Ronald Reagan Presidential Library and Museum 40 Presidential Drive Simi Valley, CA 93065
Colorado	7. National Archives & FRC at Denver 17101 Huron Street Broomfield, CO 80023-8909
District of Columbia	8. National Archives Building 700 Pennsylvania Avenue, NW Washington, DC 20408
	9. Office of the Federal Register 800 North Capitol Street, NW Washington, DC 20002
Georgia	10. Atlanta Federal Records Center 4712 Southpark Boulevard Ellenwood, GA 30294

State	Name and Address of NARA Location
	11. Jimmy Carter Presidential Library and Museum 441 Freedom Parkway Atlanta, GA 33037
	12. National Archives at Atlanta 5780 Jonesboro Road Morrow, GA 30260
Illinois	13. National Archives & FRC at Chicago 7358 South Pulaski Road Chicago, IL 60629-5898
	14. National Personnel Records Center 1411 Boulder Boulevard Valmeyer, IL 62295
Iowa	15. Herbert Hoover Presidential Library and Museum 210 Parkside Drive West Branch, IA 52358
Kansas	16. Dwight D. Eisenhower Presidential Library and Museum 200 SE. Fourth Street Abilene, KS 67410-2900
	17. Lenexa FRC 17501 W. 98th Suites 3150 & 4748 Lenexa, KS 66219
Maryland	18. National Archives at College Park 8601 Adelphi Road College Park, MD 20740
	19. Washington National Records Center 4205 Suitland Road Suitland, MD 20746
Massachusetts	20. John F. Kennedy Presidential Library and Museum Columbia Point Boston, MA 02125
	21. National Archives & FRC at Boston Frederick C. Murphy Federal Center 380 Trapelo Road Waltham, MA 02452-6399
Michigan	22. Gerald R. Ford Presidential Library 1000 Beal Avenue Ann Arbor, MI 48109-2114
	23. Gerald R. Ford Presidential Museum 303 Pearl Street Grand Rapids, MI 49504-5353
Missouri	24. Kansas City FRC 8600 NE Underground Dr., Pillar 300-g Kansas City, MO 64161
	25. Harry S. Truman Presidential Library and Museum 500 W. U.S. Hwy 24 Independence, MO 64050
	26. Lee's Summit FRC 200 Space Center Drive Lee's Summit, MO 64064-1182
	27. National Archives at Kansas City 400 West Pershing Road Kansas City, MO 64108

State	Name and Address of NARA Location
	28. National Archives & NPRC at St. Louis 1 Archives Drive St. Louis, MO 63138
New York	29. Franklin D. Roosevelt Presidential Library and Museum 4079 Albany Post Road Hyde Park, NY 12538-1999
	30. National Archives at New York City Alexander Hamilton US Customs House 1 Bowling Green New York, NY 10004-1415
Ohio	31. Dayton FRC 3150 Springboro Road Moraine, OH 43439
	32. Dayton-Kingsridge FRC 8801 Kingsridge Drive Dayton, OH 45458
Pennsylvania	33. Philadelphia FRC 14700 Townsend Road Philadelphia, PA 19154-1096
Texas	34. Fort Worth FRC 1400 John Burgess Drive Fort Worth, TX 76140
	35. Lyndon B. Johnson Presidential Library and Museum 2313 Red River Street Austin, TX 78705
	36. George Bush Presidential Library and Museum 1000 George Bush Drive West College Station, TX 77845
	37. George W. Bush Presidential Library and Museum 2943 SMU Boulevard Dallas, TX 75205
Washington	38. National Archives & FRC at Seattle 6125 Sand Point Way, NE Seattle, WA 98115
West Virginia	39. National Archives and Records Administration Rocket Center 610 State Route 956, Building 494 Rocket Center, WV 26726

Where walkthroughs were not sufficient to test the effectiveness of a control, we performed additional testing. For example, PE-2, *Physical Access Authorizations*; PE-3, *Physical Access Controls*; PE-6, *Monitoring Physical Access*; and PE-8, *Visitor Access Records* all require action by NARA personnel to be effectively in place. For each of these controls, we reviewed supporting documentation to ensure that NARA personnel are performing required control activities.

3. Test Communications Cabling

For each NARA location identified above, we reviewed bandwidth reports generated by the Riverbed monitoring tool, accessed at Archives II. These reports provided information on daily bandwidth usage for each location over a one-month period. This enabled Cotton & Company to determine if the cable type found at the location would need to be upgraded if we found that the usage was at maximum capacity for the cable type identified, or if the Century Link Internet Service Provider (ISP) contract would need to be modified to provide a greater throughput.

Audit Results

1. NARA has not applied the SA&A process to all NARA locations.

Controls are not adequate to ensure that NARA has incorporated all locations into its SA&A process. Specifically, we found that NARA has not maintained an up-to-date and accurate SSP that describes the operating environment and the security controls in place at each NARA location. In reviewing the NARANet SSP (dated November 24, 2014), we noted that it states that the controls addressed within it apply to the General Support System (GSS) infrastructure and environments across all NARA locations, including each of the locations identified as in scope for the audit. The NARANet SA&A package does not address controls specific to the respective locations, however; rather, it only appears to address the Archives II location.

Through walkthroughs and interviews performed throughout the audit, we noted that security controls vary from site to site based on varying criteria determined by the Interagency Security Committee (ISC) of the Department of Homeland Security. Some of these varying controls were independently assessed by the NARA Security Management Division (BX), which performed risk assessments for each of the NARA sites. These reviews were primarily facility security reviews, that did not and were not designed to address all relevant NIST PE controls, specifically those intended to protect server rooms and network equipment. In those occasions when the physical security review identified concerns for NARANet equipment, BX stated they informed Information Security/Assurance Division (IT) and provided them with a copy of the report. However, the results of these reviews were not incorporated into the NARA SA&A process to ensure that the NARANet system owner performed documentation, testing, and subsequent risk acceptance of the controls.

The above conditions exist because NARA management did not incorporate all NARA locations into its existing SA&A process; rather, it included all sites outside of Archives II within the NARANet SA&A boundary without considering additional controls specific to the sites. In addition, NARA's BX and Information Services (I) division are not adequately communicating the results of current facility reviews and coordinating these efforts to ensure that in-place security controls and risks identified during facility risk assessments are also documented and tested as part of the NARANet SA&A process.

Without including all controls across all NARA-owned and -leased sites, NARA management may not have a clear understanding of risk related to each of its locations, is increasingly vulnerable to a variety of risks that may not be foreseen or mitigated, and is not able to self-identify and appropriately manage significant weaknesses. Additionally, NARA is not able to take advantage of the benefits that come with the establishment of a well-developed and defined program, such as (1) improved decision-making; (2) risk identification, management, and mitigation; (3) opportunities for process improvement; (4) effective use of budgeted resources; and (5) strategic planning.

The following guidance is relevant to this control activity:

NIST SP 800-37, Revision 1, *Guide to Applying the Risk Management Framework to Federal Information Systems,* section 2.1, *Integrated Organization-Wide Risk Management,* states:

> *The RMF steps include:*
>
> - ***Categorize*** *the information system and the information processed, stored, and transmitted by that system based on an impact analysis.*
> - ***Select*** *an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.*
> - ***Implement*** *the security controls and describe how the controls are employed within the information system and its environment of operation.*
> - ***Assess*** *the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.*
> - ***Authorize*** *information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.*
> - ***Monitor*** *the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.*

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* states:

> *PL-2*
> *Control: The organization:*
>
> *a. Develops a security plan for the information system that:*
>
> - *Is consistent with the organization's enterprise architecture;*
> - *Explicitly defines the authorization boundary for the system;*
> - *Describes the operational context of the information system in terms of missions and business processes;*
> - *Provides the security category and impact level of the information system including supporting rationale;*

> - *Describes the operational environment for the information system;*
> - *Describes relationships with or connections to other information systems;*
> - *Provides an overview of the security requirements for the system;*
> - *Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and*
> - *Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;*
>
> *b. Reviews the security plan for the information system [Assignment: organization-defined frequency]; and*
>
> *c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.*

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* states:

> *RA-3*
> *<u>Control:</u> The organization:*
>
> *a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;*
>
> *b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];*
>
> *c. Reviews risk assessment results [Assignment: organization-defined frequency]; and*
>
> *d. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.*

Recommendation 1

We recommend that NARA incorporate all locations into the NARANet SA&A package by documenting location-specific security controls and ensuring that they are appropriately tested and monitored.

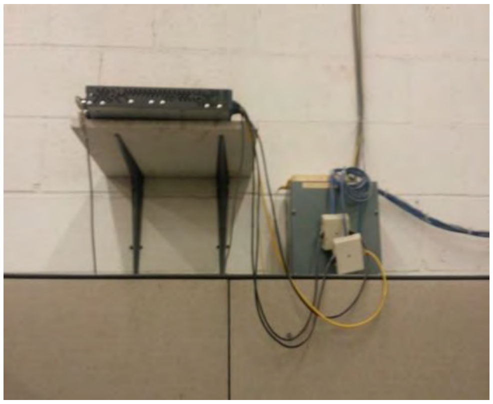
Management's Response

Management concurred with the recommendation.

2. NARA has not consistently implemented security controls across all NARA locations.

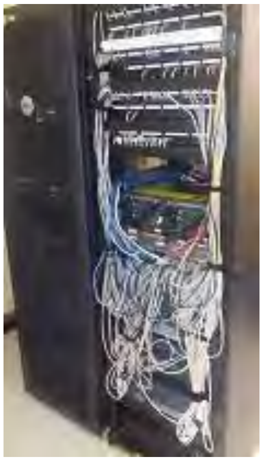
Controls are not adequate to ensure that NARA has consistently implemented physical and environmental security controls across all NARA locations. Specifically, we noted the following:

- **Lee's Summit FRC**
  - One of the networks switches is not located in a wiring closet; instead, the device is mounted on the cave wall on a stand about 14 feet in the air. There is no cage or other protection for the device. This is inconsistent with implementation at other NARA locations, where switches are protected via locked cages, and does not comply with Directive 804 requirements to "protect power equipment and power cabling for the information system from damage and destruction."

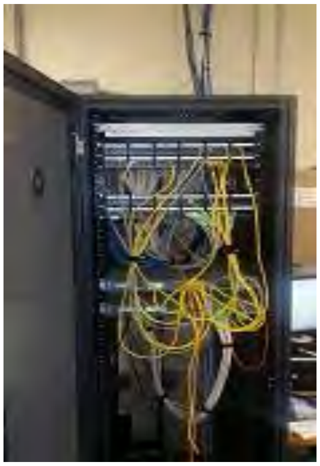


  - The server room is not equipped with a smoke detector, which is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "employ fire detection devices/systems for the information system that activate automatically and notify the NARA System Owner and emergency responders in the event of a fire."
  - Closed-circuit TV (CCTV) cameras are not currently recording activity at this location. This does not comply with Directive 804 requirements to monitor physical access.
- **Harry S. Truman Presidential Library and Museum**
  - Wiring in the server room rack is not secure and does not employ a cable management system. The Cisco 4506 core switch is exposed, as the rack does not have a lockable front cage door. Similarly, wiring in the closet rack does not employ a cable management system, which is inconsistent with implementation at other NARA locations and does not comply with

Directive 804 requirements to "protect power equipment and power cabling for the information system from damage and destruction."



Server Rack



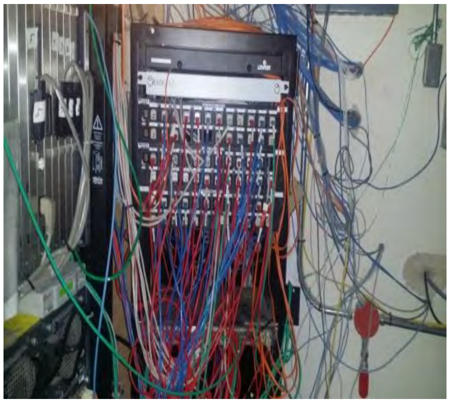
Closet Rack

- The server room is not equipped with a smoke detector, which is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "employ fire detection devices/systems for the information system that activate automatically and notify the NARA System Owner and emergency responders in the event of a fire."

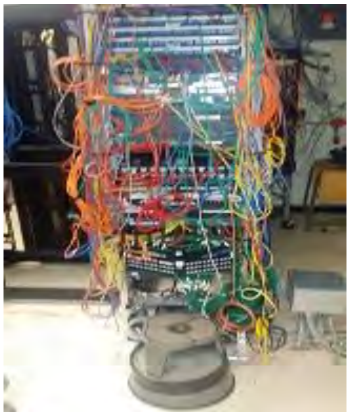
- This location does not employ temperature or humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."

- **Lyndon B. Johnson Presidential Library and Museum**

  - The patch panel in the server room is unsecured and cannot be moved due to the length of the cable runs from various access switches into the equipment room. Cable management is not possible due to the cable lengths, which is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "protect power equipment and power cabling for the information system from damage and destruction."



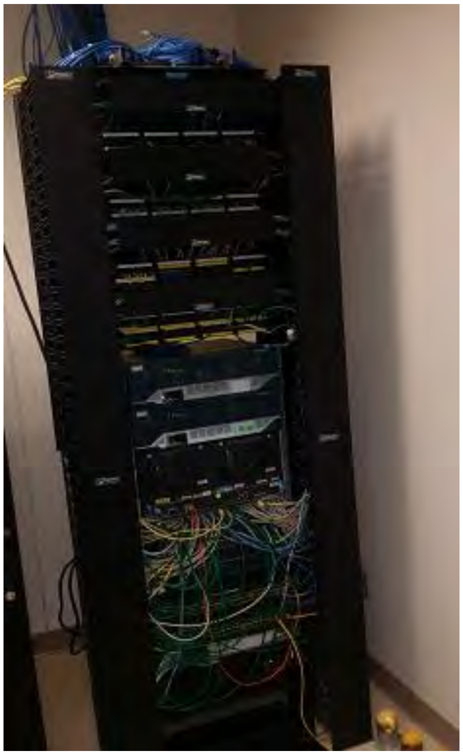
Similarly, the original wiring feed into the facility supports multiple networks (University of Texas, LBJ Foundation, and NARANet), and the library does not employ cable management for the core switches and patch panels.



- This location does not employ humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."

- **Fort Worth FRC**

    - Server racks at this location were not protected by a locked cage. This is inconsistent with most NARA sites and does not comply with Directive 804 requirements to "protect power equipment and power cabling for the information system from damage and destruction."

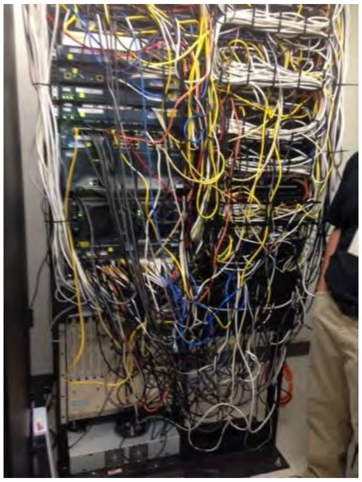


- This location does not employ humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to “maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels.”

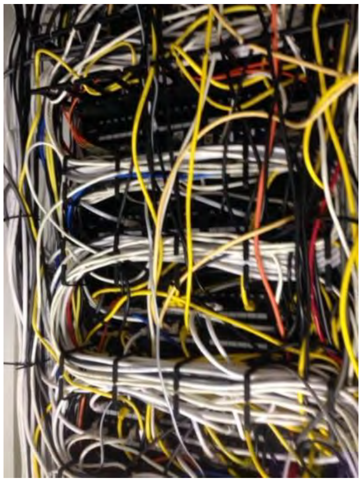
- **George W. Bush Presidential Library Library and Museum**

  - The patch panels at this location need to be replaced. Site panels were installed using “110 punch down” blocks on both sides and do not use industry-standard RJ45 jacks. This location also uses custom connectors that the FOSA created to connect panel cable runs to the site Cisco switches. This setup is inconsistent with implementation at all of the other NARA locations.

- **National Archives and FRC at San Francisco**
    - The server room is not equipped with a smoke detector, which is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "employ fire detection devices/systems for the information system that activate automatically and notify the NARA System Owner and emergency responders in the event of a fire."
    - This location also does not employ humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."
- **National Archives and FRC at Seattle**
    - We found that the server which CCTV camera recordings are stored on was located in an open office area where all employees could potentially access it. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 to "control physical access to information system output devices to prevent unauthorized individuals from obtaining the output."
- **Richard Nixon Presidential Library and Museum**
    - Cable management is not possible due to the cable lengths, which results in cables not being organized and labeled. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "protect power equipment and power cabling for the information system from damage and destruction."



Cable Runs



Patch Panel

- **Ronald Reagan Presidential Library and Museum**
  - This location does not employ humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."

- **Herbert Hoover Presidential Library and Museum**
  - Access to the server room is not secured, allowing full access to all employees. The server room is co-located with the facility copy and printer devices. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides."
  - This location does not employ temperature or humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."

- **National Archives at Kansas City**
  - The server room is not equipped with a smoke detector, which is inconsistent with implementation at most sites and does not comply with Directive 804 requirements to "employ fire detection devices/systems for

the information system that activate automatically and notify the NARA System Owner and emergency responders in the event of a fire."

  - The facility backup battery power is not adequate to support mission-essential devices until a portable generator is brought to site, as the server racks in rooms 10 and 110 do not have an uninterruptable power supply (UPS) installed. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss."

- **Dayton-Kingsridge FRC**

  - The site does not employ appropriate access controls to the server room, as we found the door propped open. It is also co-located with the facility mail/copy room. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides."

  - This location does not employ temperature or humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."

- **Dayton FRC**

  - The server room serves as a multipurpose supply and storage room. As a result, there is debris near the equipment (see below exhibit), and there is excessive access authorized for the room; only 3 of the 12 individuals authorized to access the server room have a need to access sensitive IT equipment. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides."

- This location does not employ temperature or humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."

- **Gerald R. Ford Presidential Library**

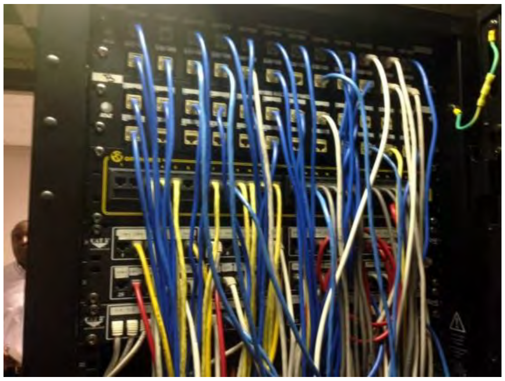
  - The server room is not equipped with a smoke detector. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "employ fire detection devices/systems for the information system that activate automatically and notify the NARA System Owner and emergency responders in the event of a fire."

  - This location does not employ temperature or humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."

  - All employees are issued a master key that provides access to the wiring closets. This is inconsistent with most sites and does not comply with

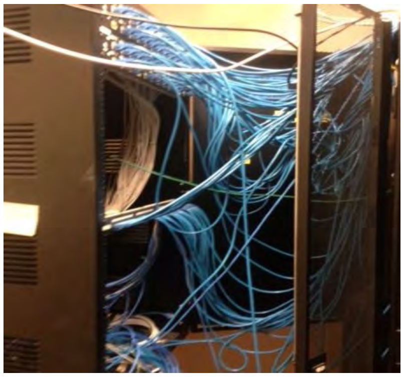
Directive 804 requirements to "enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides."

- **Gerald R. Ford Presidential Museum**
  - The server room is not equipped with a smoke detector. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "employ fire detection devices/systems for the information system that activate automatically and notify the NARA System Owner and emergency responders in the event of a fire."
  - This location does not employ temperature or humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."
- **National Archives and FRC at Riverside**
  - This location does not employ humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."
- **National Archives and FRC at Chicago**
  - Cable management is not possible due to the cable lengths, which results in cables not being organized and labeled. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "protect power equipment and power cabling for the information system from damage and destruction."



- Humidity levels are set for the building; however, they are not set specifically for the server room to ensure appropriate humidity levels to protect hardware from damage. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."

- **Jimmy Carter Presidential Library and Museum**
  - Cable management is not possible due to the cable lengths, which results in cables not being organized and labeled. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "protect power equipment and power cabling for the information system from damage and destruction."



  - This location does not employ humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."

- **National Archives at Atlanta**
    - This location does not employ humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."

- **Atlanta FRC**
    - This location does not employ humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."
    - There are no automated or manual fire-suppression mechanisms within the server room; specifically, we were unable to locate any sprinklers, gas, or fire extinguishers. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source."

- **National Archives and FRC at Boston**
    - This location does not employ humidity level monitors and controls within the server room to ensure that appropriate environmental controls are in place. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "maintain temperature and humidity levels within the facility where the information system resides at [SSP-defined acceptable levels]; and monitor temperature and humidity levels."
    - The site does not employ appropriate access controls to the switch room, as we found the door open. It is also co-located with the Archives file storage. This is inconsistent with implementation at other NARA locations and does not comply with Directive 804 requirements to "enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides."

The above weaknesses exist because NARA has not consistently implemented its PE, infrastructure, and cabling controls across all NARA facilities.

Without implementing consistent controls that are tracked by security management, there is an increased susceptibility to vulnerabilities and attacks from both inside and outside threats.

The following guidance is relevant to this control activity:

***NARA IT Security Requirements*, version 6.0, dated November 2014, states:**

> *The IT Security Requirements are derived from the controls identified in NIST Special Publication 800-53 for unclassified information systems and classified information systems. The requirements for classified information systems were formerly derived from Director of Central Intelligence Directive (DCID) 6/3, but have since been merged into the Rev. 4 version of NIST SP 800-53. NIST SP 800-53 represents the specific requirements that must be met to enable the control to the required level for confidentiality, integrity, and availability. These requirements are listed in Table 2-1 below. The* **Control** *column gives the name for the control, followed by its identifier in brackets. The* **Requirements** *column gives the requirement statements to achieve each control, with each being labeled with an identifier in brackets.*
>
> *Most of the requirements apply to all of NARA or to all information systems. These will be stated such that "NARA shall…" or "Each information system shall…" as appropriate. Other requirements only apply to information systems at a moderate or high level of confidentiality, integrity or availability. These requirements will be qualified as being "For high availability information systems" or "For moderate integrity information systems" or something similar. A few of the requirements are not mandated for any particular system, but can be implemented where data is "deemed by the NARA System Owner to require additional protection" to enhance a particular security control. While no information system is required to enhance security beyond the minimum required levels, if stronger security is desired, it must be enhanced using one of these approved methods. Additional requirements that apply to classified systems will noted as such.*

Recommendation 2

We recommend that, to the extent possible, NARA revisit all site locations and ensure that appropriate and consistent PE, infrastructure, and cabling controls are implemented. At a minimum, NARA should take the following appropriate steps to remediate the issues identified above, which represent the present risks and flaws applicable to NARA:

1. Ensure that neat cable management and labeling mechanisms are employed for all sites.
2. Ensure that all server rooms are equipped with appropriate fire detection and suppression capabilities.
3. Limit access to all server rooms to those individuals with an explicit need to access IT equipment.
4. Ensure that appropriate temperature and humidity monitoring and control mechanisms are employed for all server rooms.
5. Ensure that appropriate UPS devices are employed for hardware supporting the site’s network infrastructure.
6. Ensure that all server racks, switches, and network equipment are adequately secured from unauthorized access via locked racks.

Management’s Response

Management concurred with the recommendations.

3. NARA has not adequately implemented networking capabilities to support the continued growth of its user population at several of its locations.

Controls are not adequate to ensure that NARA management is actively aware of and implementing contingency plans or solutions to ensure that they do not supersede networking capabilities at all of their sites. While we noted that NARA has the technical infrastructure to support increasingly network-taxing technologies, we found several sites with patch panels that are near capacity, increasing the risk that these locations will run out of ports to add new users and support continued growth. These sites include:

- National Archives and FRC at San Francisco: This location has utilized 90 percent of the blade chassis and switch ports.

- National Archives and FRC at Seattle: This location has utilized 95 percent of the switch ports, and the patch panel is maximized.

- National Archives and NPRC at St. Louis: There are no available ports in communication room #2 on the closet access switch due to current staff requirements and the building floor plan.

The above weaknesses above exist because NARA management has not implemented contingent devices or procedures to mitigate these issues.

The following guidance is relevant to this control activity:

***NARA IT Security Requirements* states:**

> *CP-8. Telecommunications Services*
>
> *For data requiring moderate or high availability, the NARA NHT shall establish alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [SSP as per BIA for unclassified information systems or 24 hours for classified information systems] when the primary telecommunications capabilities are unavailable.*

Recommendation 3

We recommend that NARA develop and implement a plan to install additional networking capabilities at facilities that are near capacity, or develop and implement a contingency plan to support continued operations in the event that networking capabilities are maximized.

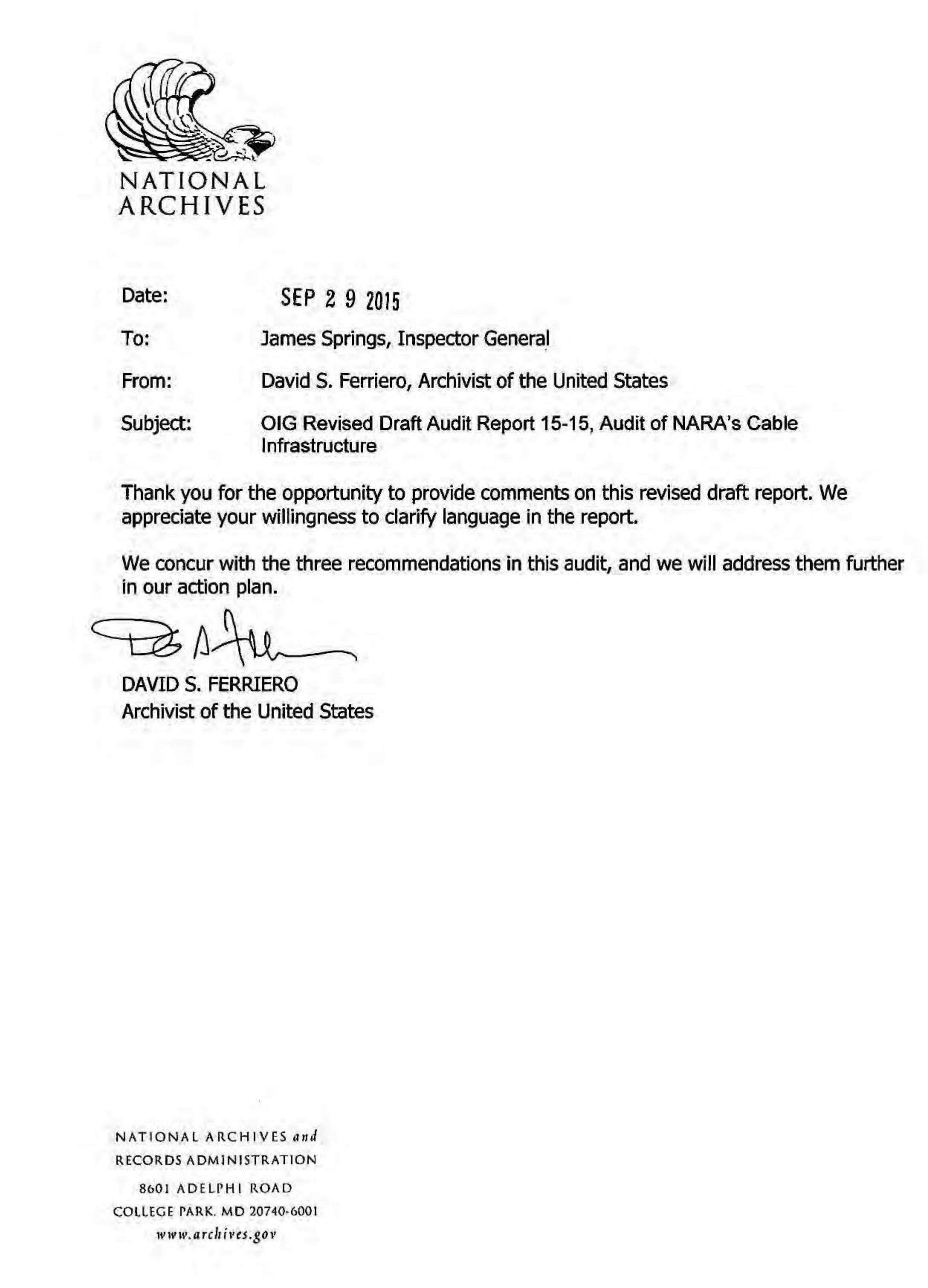
Management's Response

Management concurred with the recommendation.

Appendix A – Acronyms and Abbreviations

BX	NARA Security Management Division
CCTV	Closed Circuit Television
EIA	Electronic Industries Alliance
FIPS	Federal Information Processing Standards
FRC	Federal Records Center
GAO	Government Accountability Office
GAGAS	Generally Accepted Government Auditing Standards
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
PE	Physical and Environmental
RMF	Risk Management Framework
SA&A	Security Assessment and Authorization
SSP	System Security Plan
TIA	Telecommunications Industry Association
VOIP	Voice Over Internet Protocol
VTC	Video Teleconferencing
WAN	Wide Area Network

Appendix B - Management's Response to the Report



NATIONAL
ARCHIVES

Date: SEP 2 9 2015

To: James Springs, Inspector General

From: David S. Ferriero, Archivist of the United States

Subject: OIG Revised Draft Audit Report 15-15, Audit of NARA's Cable Infrastructure

Thank you for the opportunity to provide comments on this revised draft report. We appreciate your willingness to clarify language in the report.

We concur with the three recommendations in this audit, and we will address them further in our action plan.

DAVID S. FERRIERO
Archivist of the United States

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001
www.archives.gov

Appendix C - Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Chief Operating Officer
Chief Information Officer