OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES

August 20, 2018

TO: David S. Ferriero
Archivist of the United States

FROM: James Springs
Inspector General

SUBJECT: *Audit of NARA's Continuity of Operations (COOP) Readiness*

This memorandum transmits the results of our final report entitled, *Audit of NARA's Continuity of Operations (COOP) Readiness* (OIG Audit Report No. 18-AUD-14). We have incorporated the formal comments provided by your office.

The report contains thirty (30) recommendations, which are intended to strengthen NARA's COOP program. Your office concurred with all of the recommendations. Based on your August 17, 2018 response to the final draft report, we consider all the recommendations resolved and open. Once your office has fully implemented the recommendations, please submit evidence of completion of agreed upon corrective actions so that recommendations may be closed.

As with all OIG products, we determine what information is publically posted on our website from the attached report. Consistent with our responsibility under the *Inspector General Act, as amended,* we may provide copies of our report to congressional committees with oversight responsibility over the National Archives and Records Administration.

We appreciate the cooperation and assistance NARA extended to us during the audit. Please call me with any questions, or your staff may contact Jewel Butler, Assistant Inspector General for Audits, at (301) 837-3000.

OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES

Audit of NARA's Continuity of Operations (COOP) Readiness

August 20, 2018

OIG Audit Report No. 18-AUD-14

Table of Contents

Executive Summary

Audit of NARA's Continuity of Operations (COOP) Readiness

OIG Report No. 18-AUD-14 August 20, 2018

Why Did We Conduct This Audit?

It is the policy of the United States to have in place a comprehensive and effective program to ensure continuity of essential Federal functions under all circumstances. As a baseline of preparedness for the full range of potential emergencies, all Federal agencies shall have in place a viable COOP capability which ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations.

This audit was conducted to determine whether NARA has appropriate processes and controls in place to continue its mission-essential functions with minimal disruption in case of an emergency or a disaster, in accordance with federal laws and guidance.

What Did We Recommend?

We made a total of 30 recommendations relating to COOP planning and preparation, ISCP, management of essential COOP documents, COOP training, and the submission process for required COOP documentation.

These recommendations, if implemented will strengthen NARA's COOP program and provide additional assurance that NARA can continue its essential functions with minimal disruptions in the event of an emergency or disaster.

What Did We Find?

The National Archives and Records Administration (NARA) is continuously progressing toward a more mature, agency-wide continuity of operations (COOP) program. However, opportunities for improvement exist in COOP planning and preparation, Information Systems Contingency Planning (ISCP), management of essential documents, training, and the submission process for required documentation. Specifically, we found not all of NARA's COOP personnel are telework-ready or telework-capable; NARA was operating without a valid Memorandum of Understanding (MOU) for its alternate facility; the Information Technology (IT) inventory and network diagrams at the alternate facility were inaccurate or outdated; and Staff Accountability and Personnel Readiness Data submissions during continuity exercises were not always completed and accurately tracked.

We also found contingency planning for information systems supporting essential functions remains a challenge. Weaknesses continue to exist in NARA's identification of mission-critical systems, management of information system inventory and system security categorization, and maintenance of ISCP documents in accordance with NARA policy and federal guidance. Although COOP Plans for the Headquarters (HQ) and field sites were generally maintained up-to-date, other Emergency Response Plans, including the Occupant Emergency Plans (OEPs), Pandemic Influenza Plans (PIP), and Records Emergency Plans (REPs), were not always maintained in accordance with federal guidance and NARA policies and procedures.

While NARA tracks the overall number of employees who take annual COOP training, it does not track the training status based on the designated role of the employee (senior leadership, staff with assigned COOP roles, and all other staff). We also found there is a lack of mission-specific training tailored to each NARA organization supporting the essential functions. Finally, NARA does not ensure the Standard Form 2050 (SF-2050), *Reconstitution Questionnaire*, is reviewed and submitted to the General Services Administration (GSA) for NARA's headquarters on an annual basis as required. These weaknesses are attributed to inconsistently developed or implemented policies and procedures, previously discovered weaknesses not being mitigated in a timely manner, and a lack of coordination and communication. Without improvements, NARA may not be able to ensure its full compliance with federal and internal continuity requirements, and may not develop and sustain a mature COOP program.

Background

In May 2007, the President signed National Security Presidential Directive (NSPD)-51/Homeland Security Presidential Directive (HSPD)-20, *National Continuity Policy* (the Policy), to establish a comprehensive national policy for the continuity of Federal Government structures and operations. It also established a single National Continuity Coordinator (NCC) responsible for coordinating the development and implementation of federal continuity policies and the National Essential Functions (NEFs). In conjunction with NSPD-51/HSPD-20, the White House published *the National Continuity Policy Implementation Plan* (NCPIP) in August 2007. The purpose of NCPIP was to be the means by which the Policy is translated into action and is intended to be a comprehensive and integrated list of directives for the Federal Executive branch in order to ensure the effectiveness and survivability of our national continuity capability. In 2008, the Department of Homeland Security (DHS) published *Federal Continuity Directive 1* (FCD-1) to establish continuity planning requirements for executive departments and agencies (D/As) as directed by the Policy.

In July 2016, the President signed PPD-40, *National Continuity Policy*, which replaced NSPD-51/HSPD-20 and the NCPIP, addressing lessons learned, best practices, and the integration of new technologies and processes since 2007. Some relevant material in the NCPIP was added to PPD-40, and certain portions were adopted in the update to FCD-1 dated January 2017.[1] This version of FCD-1 establishes the framework, requirements, and processes to support the development of D/As continuity programs by specifying and defining elements of a continuity plan. These required elements include delineation of essential functions; succession to office and delegations of authority; safekeeping of and access to essential records; continuity locations; continuity communications; human resources planning; devolution of essential functions; reconstitution; and program validation through testing, training, and exercises (TT&E).

In an effort to be in compliance with the Policy, NARA maintains, among others, NARA's HQ COOP Plan (the Plan), that provides a structure for incorporating continuity requirements into the daily operations of the agency. This Plan was developed to ensure agency Mission Essential Functions (MEFs) continue to be performed under all conditions during a wide range of emergencies. While the Plan is the overarching continuity plan for all non-headquarters facilities across the nation, NARA also maintains local facility-level COOP plans to be in compliance with the Policy.

[1] This was the second update to FCD-1 since initially published in 2008; the first update was made in October 2012 to provide new policies and clarifications to existing policies and to give direction to further development of continuity plans and programs to D/A's.

NARA has one Primary Mission Essential Function (PMEF), validated by the NCC, which is to publish presidential and federal government documents in the daily Federal Register, or publish and broadly disseminate an Emergency Federal Register during national security emergencies when necessary. PMEFs are required to be continuous or resumed within 12 hours after an event in order to support or implement the performance of one or more National Essential Functions (NEFs) before, during, and after an emergency.

In addition to the PMEF, NARA has eight MEFs, the functions that enable NARA to provide vital services, exercise civil authority, maintain the safety of the public and the industrial and economic base, during a disruption of normal operations but do not support one or more of the NEFs. The Policy also defines 11 Essential Supporting Activities (ESAs), which must be performed by every department and agency in order to achieve and sustain a viable continuity capability. NARA's HQ COOP Plan delineates the PMEF, MEFs, and ESAs applicable to the agency, and the offices and teams responsible for carrying out those functions and activities.

NARA's Executive for Business Support Services (B) serves as the Agency Continuity Coordinator. Security Management Division (BX), under Business Support Services, takes charge of directing the development and administration of plans for the performance of the essential functions at all NARA facilities during agency or national emergencies. Included within these responsibilities are maintaining an up-to-date NARA HQ COOP Plan, conducting regularly scheduled continuity TT&E, and participating with DHS and other entities concerning NARA continuity policies and performance. NARA conducts two types of continuity exercises (Eagle Horizon and Operation Activate), to fulfill the annual continuity exercise and training requirements under FCD-1. Eagle Horizon focuses on the agency's capability to perform PMEFs and MEFs from alternate facilities, as well as plan for reconstitution. Operation Activate assesses field capabilities in the areas including communications, teleworking, alert and notification, NARANet[2] connectivity, accountability of all NARA staff, and remote access to essential records.

The total Fiscal Year (FY) 2016 and FY 2017 obligated resource requirements for NARA's COOP program were $1,048,364 and $944,605, respectively. The total FY 2018 estimated resource requirements for the program is $653,744.

[2] A computer network system providing access to NARA's intranet, email, and to the Internet.

Objectives, Scope, Methodology

The objective of the audit was to determine whether NARA has appropriate processes and controls in place to continue its mission-essential functions with minimal disruption in case of an emergency or disaster. Specifically, we determined whether proper controls were in place to meet the following requirements:

- Develop and maintain up-to-date COOP policies and procedures.
- Train and educate employees to ensure they are fully cognizant of their roles and responsibilities during an emergency.
- Develop, maintain, and test up-to-date NARA-wide and system-specific Contingency Plans (CPs).
- Follow up on findings and recommendations from previous NARA-wide or system-specific COOP exercises, audits, and other internal or external evaluations and assessments.
- Ensure the failover and redundancy technology and location are properly prepared for a contingency.

To meet the audit objectives, we:

- reviewed NARA's policies and procedures for COOP, in conjunction with the requirements found in Federal Continuity Directives 1 and 2;
- visited NARA's alternate facility in Rocket Center, West Virginia, to conduct a walkthrough of the facility, observe the monthly telecommunications testing, and observe the annual Eagle Horizon Exercise for FY 2017;
- conducted sample testing of 10 NARA's PMEF, MEFs, and ESAs to determine if the function is adequately prepared to achieve COOP in accordance with the policies and procedures;
- interviewed representatives from NARA offices responsible for carrying out COOP functions; and requested and reviewed relevant documentation (e.g., policies, procedures, training, and ISCPs);
- conducted sample testing of Emergency Response Plans for 15 NARA facilities consisting of three HQ locations, eight Federal Records Centers, and four Presidential Libraries; and
- conducted sample testing of 45 mission-critical personnel[3] for their telework agreements available in NARA's Vital Records folder.

[3] Emergency employees who may be assigned to one or more of the pre-designated teams or groups of employees that are called on to perform duties during a continuity event.

Samples were judgmentally selected based on various factors including, but not limited to, the type of mission and its criticality (PMEF, MEF, and ESA); the need to revisit previously identified issues in the functional area(s); and the location and type of facility, as well as the number of employees at the facility. These samples were non-statistical and cannot be projected to the intended population.

To assess internal controls relative to our objectives, we reviewed Business Support Services' internal control reports for FYs 2016 and 2017. In the end-of-the-year reports, management reported there was reasonable assurance the management controls in effect were adequate and effective in ensuring:

(1) programs achieved their intended results;
(2) resources were used consistent with NARA's mission;
(3) programs and resources were protected from waste, fraud, and mismanagement;
(4) laws and regulations were followed; and
(5) reliable and timely information was obtained, maintained, reported and used for decision making.

BX, the office in charge of NARA's overall COOP program, stated in the Internal Controls Program (ICP) Detailed Reports for FYs 2016 and 2017 that there were 30 and 14 open observations or deficiencies, respectively, included in the Continuity Corrective Action and Implementation Plan (CCAP). However, BX believed none of the observations or deficiencies were for critical tasks or indicative of significant compliance or implementation concerns. BX reported for both years that NARA received the "Green[4]" rating in all 13 elements that comprise a viable continuity capability from the DHS Continuity Readiness Reporting System (RRS) assessments. These assessments are the primary method of monitoring continuity capability readiness status at NARA.

This performance audit was conducted in accordance with generally accepted government auditing standards between February 2017 and April 2018 in College Park, Maryland, and Rocket Center, West Virginia. The generally accepted government auditing standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit was conducted by Jina Lee, Senior IT Auditor.

[4] A Green rating indicates all critical tasks are "Yes", and at least 80% of all tasks within the respective continuity elements are "Yes", signifying there are no significant deficiencies within the respective continuity element.

Audit Results

Finding 1. COOP Planning and Preparation Could Be Improved.

NARA is continuously progressing toward a more mature, agency-wide COOP program in accordance with federal laws and guidance. However, opportunities for improvement exist in COOP planning and preparation, ISCP, management of essential documents, training, and the submission process for required documentation. Specifically, we found not all of NARA's COOP players are telework-ready or telework-capable, NARA was operating without a valid MOU for its alternate facility, the IT inventory and network diagrams at the alternate facility were inaccurate or outdated, and Staff Accountability and Personnel Readiness Data submission during continuity exercises were not always completed and accurately tracked.

These conditions existed because NARA has not always ensured policies and procedures for COOP were consistently developed and implemented across the agency; and has not adequately addressed previously identified weaknesses around COOP or the weaknesses discovered in other program areas that have relevance to COOP. FCD-1, issued in January 2017, states organizations must fully integrate continuity planning and procedures into all aspects of daily operations to create a "culture of continuity." By not ensuring preexisting weaknesses are adequately addressed, NARA may not be able to ensure full compliance with federal requirements for COOP or carry out essential functions in the most effective and efficient manner that maximizes the use of available resources, in case of an emergency or a disaster.

Telework Agreements & Telework Capabilities for Mission-Critical Personnel

There is a risk that not all of NARA's COOP players are telework-ready or telework-capable. In June 2017, we conducted sample testing of NARA's mission-critical personnel and found 29 of 45 employees sampled, or 64%, had current telework agreements. Telework agreements for the remaining COOP participants were either not found in the folder or were outdated. In the FY 2015 and 2016 Eagle Horizon exercises, approximately 80% of participants responded they participated remotely via telework during part or all of the exercise. According to the FY 2017 Eagle Horizon Player Handbook, 105 individuals participated in the exercise as telework players, representing approximately 60% of all unexcused exercise participants. The FY 17 Eagle Horizon Player Handbook required mission-critical employees maintain current telework agreements before they participated in the annual exercise that began in June 2017. NARA

Directive 332 further states agency-designated Emergency Relocation Group (ERG) members[5] must have an approved telework agreement with their supervisors to properly exercise their ERG responsibilities.

We also found among 226 exercise participants (including excused exercise participants) for FY 2017 Eagle Horizon, only 64 individuals, or 28%, appeared to have a NARA-issued laptop computer. Twenty-one individuals were not found in the device list provided by Information Services.[6] NARA's Telework Agreement form, NA Form 3040, includes the employee's agreement to use the government-provided computer equipment for official duties only. The form does not include any reference to what is expected of an employee when a personally owned computer is used for telework and to address potential confidentiality and security concerns for the information accessed through or processed on the personally owned computer.

Additionally, the After-Action-Report (AAR) for FY 2016 Eagle Horizon exercise revealed individuals who participated in the exercise remotely had issues connecting to the backup Citrix Virtual Private Network (VPN), which supports COOP in the event the primary Citrix application is disrupted. According to the AAR, only those individuals using NARA-issued laptop computers could access the VPN. The remote connectivity issue has been consistently identified in past AARs, and management acknowledged it is a significant obstacle to effectively deploying telework as a continuity option.

Finally, the results of the FY 2017 Eagle Horizon revealed Federal Register personnel with U.S. Government Publishing Office (GPO)-issued laptop computers could not access NARANet because GPO does not allow permission to upload Citrix.[7] During the 2017 exercise, concerns were raised by the participants of the reconstitution team that not all participants had a NARA-issued laptop computer. It was stated that although they could use their personally owned computers to access NARANet remotely, they may have to share the computer with other members of their household, thus allowing a potential compromise of confidentiality and integrity of the information accessed. According to the AAR for Operation Activate 2017, many ERG members do not telework on a regular basis and are unfamiliar with remote access requirements and capabilities.

[5] According to NARA's Continuity Manager, in many cases the term ERG is used to include all mission-critical personnel in various task organizations, including the Transition Team, Devolution Emergency Response Group (DERG), and Reconstitution Planning and Reconstitution Implementation Team (RPT/RIT).

[6] OIG performed a manual reconciliation of employee names between the Eagle Horizon exercise participant roster and device list, because for many devices only the employee's NARANet login ID, instead of the employee's name, was available or employee names were inaccurately documented. Therefore, OIG cannot attest to the completeness or accuracy of the analysis conducted.

[7] FY 2017 Eagle Horizon was a tabletop exercise and did not utilize the backup Citrix VPN.

Memorandum of Understanding between NARA and Naval Sea Systems Command

We found NARA had been operating at its alternate facility without a current MOU with the facility owner for over one year from July 1, 2016, through July 23, 2017. FCD-1 requires organizations and components performing MEFs that directly support PMEFs to continue essential functions from an alternate location. In 2006, NARA established a working relationship with the Commander, Naval Sea Systems Command (COMNAVSEA) by signing an MOU that delineated responsibilities, authorized use, and the financial and administrative responsibilities of both parties with the primary goal being the establishment and maintenance of Allegheny Ballistics Laboratory (ABL), Rocket Center, West Virginia as an alternate operating facility for the NARA headquarters. This MOU became effective upon signatures from both parties on August 31, 2006, and expired on June 30, 2016.

NARA initiated planning for a renewal of the MOU (internally) in May 2016, one month prior to the MOU expiring. In early July (after the MOU expired) a draft MOU was still being circulated internally within NARA. Subsequently, multiple versions of an updated draft MOU were created between May 2016 and January 2017. Additionally, the most recent version reviewed during the audit (dated January 23, 2017), did not include key information such as ERA operations and the alternate network operations center still operating at ABL. NARA's Continuity Manager indicated the initial version of the updated draft MOU included this information however those functions were removed after being circulated to various NARA organizations for a review. Upon OIG's notification, management conducted another review of the updated draft MOU and concluded it should continue to list the operations of ERA and alternate network operations center. Subsequently, an updated MOU was prepared to re-list these functions and was signed by both parties by July 24, 2017.

IT Inventory Management at the Alternate Facility

The IT inventory and network diagrams at the alternate facility were inaccurate or outdated. The IT inventory at the alternate facility did not consistently include ERA equipment. The Field Officer Systems Administrator (FOSA) for the facility stated the IT inventory at the alternate facility is taken annually, in addition to a quarterly inventory conducted by the Operation and Maintenance (O&M) contractor for the facility. In reviewing November 2016 and April 2017 inventory listings, we found the November 2016 list included many of the ERA components as "COOP Equipment" and listed only one asset item under "ERA equipment", whereas the April 2017 list did not include ERA equipment. The ERA system is composed of separate "instances"

or programs, many of which operate at this facility without having an alternate site. ERA supports at least two MEFs at NARA.[8]

The network diagram for the alternate facility found in the latest version of the NARA COOP Infrastructure Specification and Rocket Center Network Design, maintained by NARA's IT Operations and dated November 2015, reflected an outdated network infrastructure. The Electronic Editing and Publishing Document System (eDOCS)[9] was previously moved to the Amazon Web Services (AWS) cloud-hosting environment, yet the network diagram still reflected the local area network components for the system. In May 2017, during and subsequent to our site visits, Information Services representatives agreed the diagram was outdated. However, we were not provided with an updated document reflecting the current network infrastructure.

According to the National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Rev. 4*, Security and Privacy Controls for Federal Information Systems and Organizations*, organizations should develop and document an inventory of information system components that accurately reflects the current information system and review and update the information system component inventory at a frequency defined by the organization. NARA's security architecture requires the component inventory to be reviewed and updated at least annually.

Staff Accountability and Personnel Readiness

Staff Accountability and Personnel Readiness Data submission during continuity exercises were not always completed and accurately tracked. The staff accountability tool allowed the supervisor to efficiently identify and account for direct reports using the pre-populated lists of employees in each NARA organization. However, controls needed to be strengthened in the following areas. [10]

- User Accountability – The username and password transmitted to managers and supervisors via email communications, were shared among all users, which could lead to compromise of data integrity.

[8] OIG Advisory Report No. 10-16, No Alternate Back-up Site for the Electronic Records Archives System, was issued in October 2010 to notify management of the lack of a back-up site for the system, which still remains unresolved to date.

[9] eDOCS is the NARA Office of the Federal Register (OFR)'s electronic content management system for managing, editing, and making publicly available the legal documents required to be published within the Federal Register system.

[10] Management indicated it intentionally allowed the use of a global username and password for all supervisors and also to account for staff outside their organizations for maximum flexibility of accountability, and the use of a global username and password was discussed and reviewed by NARA IT Security and leadership.

- Submitter Organization – The non-supervisory OIG employee selected an inaccurate NARA organization, and the tool allowed her to account for the employees within that organization who had not yet been accounted for by other submitters.
- Supervisor and Direct Reports - Within the NARA organization a submitter was allowed to account for other employees in that organization, including the submitter's supervisor.

According to the AAR for FY 2017 Eagle Horizon, there were a number of comments about the staff accountability tool database not reflecting current/accurate information. In addition, our follow-up testing of the accountability tool during the Operation Activate exercise in October 2017 revealed the issues still existed. NARA OIG reported in a previous audit (*Report No. 15-13, Audit of NARA's Human Resources Systems and Data Accuracy)*, that inaccurate supervisory information was found in NARA's Learning Management System (LMS) and Federal Personnel and Payroll System (FPPS). This was attributable to a manual process used to update supervisory information in FPPS, and a lack of a process to request NARA organizations verify supervisory information on a periodic basis.[11] We were informed during the audit in FY 15 that the Office of Human Capital was in the process of implementing a new supervisory information update process which would help eliminate formatting issues arising from the manual update process. In the aforementioned report, we recommended management fully implement the new supervisory information update process and conduct a periodic review of the data in the system. The estimated implementation date for the recommendation was July 2016. To date, the recommendation remains open.

As part of annual continuity exercises, NARA requires all exercise participants to submit their individually completed Personnel Readiness Data Sheets after receiving the continuity event alert notification. NARA uses OpsPlanner, the emergency planning and alert notification tool, as a means to collect the readiness data submitted by the participants. Although the process for collecting personnel readiness data is in place, and the content of the Data Sheet appears be helpful for NARA to identify and contact key COOP employees in case of an emergency, we determined the quality of the information needs improvements. For example, the link to the tool was not personalized, i.e., employees could input a name other than their own without being detected by the tool. We also noted the tool did not detect inaccurately entered names of the users. According to the Continuity Manager, the data sheet is blank, and all data entered comes directly from the submitter, and it does not feed or receive information from Employee Locator or any other HR-related databases.

We also noted management did not exclude multiple submissions by one user or incomplete submissions when counting the number of employees that completed the data sheets. In FY 2017 Eagle Horizon, management reported a total of 185 employees completed the data sheets. However, we found, after removing multiple and/or incomplete submissions, the total decreased to 149, representing approximately 86% of the total unexcused exercise players. For Operation Activate, management reported 242 employees, or 81% of total participants, completed the

[11] OIG Audit Report No. 15-13, pgs. 9 – 11.

submission. Again, after removing multiple and/or incomplete submissions, we found only 217 employees, or 76% of total participants, completed the submission. FEMA requires at least 80% of critical tasks are "Yes" in order to achieve a "Green" rating for a continuity element in the Continuity RRS Assessment. Had the multiple and/or incomplete entries been excluded from computing the completion rate, NARA would have fallen under the 80% completion requirement to achieve the "Green" rating.

Employee Contact Information for Emergency Alert Notification

In March 2016, concerns were raised by NARA senior executives about the consistency and completeness of NARA's emergency alert notification practices. For example, personnel from outside of the affected area for the alert notification test received an automated phone notification from OpsPlanner, while over 50% of the personnel who were supposed to receive the automated phone notification did not receive them. According to the Continuity Manager, this issue was caused by inaccurate or incomplete duty station entries in OpsPlanner and unpopulated contact information for employees.

NARA's data quality in OpsPlanner has improved, and less than 1% of approximately 2,900 employees found in the OpsPlanner database were missing their duty locations in the database as of April 2018. However, a significant number of employees were still missing business or personal phone numbers in the database. We found approximately 630 employees did not have a phone number at all, business, cellular, home, or other, in the OpsPlanner database, indicating they may not receive a phone notification in case of an emergency. According to the Continuity Manager, incomplete contact information in OpsPlanner is caused by the incomplete data entries on the Employee Locator that feeds OpsPlanner on a biweekly basis. A recommendation to include the Employee Locator review and update process in the new hire orientation was also made in *Audit Report No. 15-13, Audit of NARA's Human Resources Systems and Data Accuracy*, which remains open as of April 2018.[12] If data integrity and completeness of employee contact information is not assured, NARA may not be able to contact employees in an emergency.

Recommendations

In order to improve COOP readiness in the areas discussed above, we recommend:

> **Recommendation 1:** The Human Capital Officer, in collaboration with Business Support Services, develop and implement a process to ensure all designated ERG/DERG/RPT members maintain a copy of current telework agreements.

[12] This recommendation has recently been closed on April 27, 2018, after the end of the fieldwork for this audit.

Management Response

Human Capital will update telework policy (NARA 332) and COOP documentation (Player Handbook) to no longer explicitly require a telework agreement specifically from designated ERG/DERG/RPT players. COOP participants will still require a telework agreement, but under the general requirement that all NARA employees must have an agreement in order to telework. NARA will further update the telework policy to clarify that any employee may be required to telework in the event of an actual emergency, regardless of whether he or she has a telework agreement. In addition, NARA will no longer require that extra copies of telework agreements be stored on the vital records drive.

Target Completion Date: December 31, 2018

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 2: The Chief Information Officer:

(a) determine the laptop computer needs for all current ERG, DERG, and RIT/RPT member employees, in consultation with Executives responsible for executing the PMEFs, MEFs, and ESAs for NARA;
(b) conduct a cost-benefit analysis for providing a government-furnished laptop computer to those employees identified from (a); and
(c) provide a government-furnished laptop computer to the ERG, DERG, and RPT/RIT member employees, based on the analyses conducted from (a) and (b) above.

Management Response

Information Services will work with each Executive responsible for executing the PMEFs, MEFs, and ESAs, to develop a needs assessment for remote productivity and to conduct a cost-benefit analysis for all current ERG, DERG, and RIT/RPT member employees. Based on the results of the needs assessment and the cost-benefit analyses, laptops will be provided to ERG, DERG, and RPT/RIT members.

Target Completion Date: March 29, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 3: The Chief Human Capital Officer, in collaboration with the Chief Information Officer:

(a) update the telework policy to include the employee's responsibility to test the connectivity to NARANet when the employee uses a personally owned computer for teleworking; and

(b) provide a reference in the policy reminding teleworkers of NARA policies and procedures for using a personally owned computing resources to conduct official NARA duties.

Management Response

Human Capital will update the NARA telework policy to require employees to test the connectivity to NARANet when using personally owned computers for teleworking. The updated policy will also include a reference to NARA policies regarding use of personally owned resources for conducting official NARA duties.

Target Completion Date: December 31, 2018

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 4: The Executive for Business Support Services develop and implement a process to ensure proper planning for updating and renewing all interagency agreements pertinent to NARA's continuity of operations is performed in a timely manner.

Management Response

Business Support Services will add the MOU with NAVSEA to NARA's Continuity Multi-Year Strategy Program Management Plan (MYSPMP) to ensure proper planning for updating and renewal prior to its September 2021 expiration.

Target Completion Date: January 31, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 5: The Chief Information Officer ensure the inventory is reviewed and updated for all NARA IT assets at the alternate site, including ERA equipment, at least on an annual basis.

Management Response

The Network Services Branch (IOO) will provide a copy of the complete and updated ERA inventory.

Target Completion Date: October 31, 2018

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 6: The Chief Information Officer ensure the NARA COOP Infrastructure Specification and Rocket Center Network Diagram document is reviewed on an annual basis and updated as necessary, consistent with any other IT policies, procedures, methodologies, and supplements to the policies.

Management Response

The Network Services Branch (IOO) will provide an updated copy of the NARAnet Disaster Recovery and Contingency Plan and a corrected network diagram.

Target Completion Date: October 31, 2018

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

In order to improve user accountability and data integrity for the staff accountability tool utilized during continuity exercises, we recommend:

Recommendation 7: The Chief Human Capital Officer, in coordination with Business Support Services, establish controls to ensure the accurate supervisor-employee relationship is reflected on the staff accountability tool.

Management Response

The Interior Business Center has added a new field to the employee record for the supervisor name in FPPS. This new field will be available to NARA in August 2018. We have requested that it be configured as a required field for NARA. In addition, we are

developing a job aid to remind supervisors of the requirement to put through an action in FPPS when supervisors change.

Target Completion Date: December 31, 2018

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 8: The Chief Human Capital Officer, in coordination with Business Support Services, consider implementing controls to ensure the submitter only has access to the organization to which he/she belongs.

Management Response

Human Capital, in coordination with Business Support Services, will evaluate the risks and benefits of restricting access as recommended and will take appropriate actions, including documenting Management's acceptance of the risk, if that is the appropriate result.

Target Completion Date: December 31, 2018

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 9: The Chief Human Capital Officer, in coordination with Business Support Services, consider implementing a unique username and password to each authorized submitter of the form for user accountability and data integrity.

Management Response

Human Capital, in coordination with Business Support Services, will evaluate the risks and benefits of restricting access as recommended and will take appropriate actions, including documenting Management's acceptance of the risk, if that is the appropriate result.

Target Completion Date: December 31, 2018

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

In order to improve the completeness and accuracy of the personnel readiness data collected from COOP exercise participants, we recommend:

Recommendation 10: The Executive of Business Support Services, in collaboration with the Offices of Human Capital and Information Services as applicable, strengthen the process to manage personnel readiness data submission to more accurately count completed submissions and verify the accuracy of the data submitted.

Management Response

Business Support Services will evaluate the costs and benefits of applying more active management of personnel readiness data and will take appropriate actions, including documenting Management's acceptance of the risk, if that is the appropriate result.

Target Completion Date: November 30, 2018

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 11: The Executive of Business Support Services, develop and implement a process to remind the participants who have not completed the submission to complete it.

Management Response

Business Support Services will incorporate this recommendation into the cost-benefit analysis in recommendation 10.

Target Completion Date: November 30, 2018

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 12: The Executive of Business Support Services, in collaboration with the Offices of Human Capital and Information Services as applicable, consider providing exercise participants with personalized link to the data sheet, with pre-populated basic personnel information, where participants could review, verify, and add required information, for data integrity and efficient use of exercise time.

Management Response

Business Support Services will evaluate the costs and benefits of increasing personnel data collection efforts as recommended and will take appropriate actions, including documenting Management's acceptance of the risk, if that is the appropriate result.

Target Completion Date: November 30, 2018

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 2. Information System Contingency Planning Needs Improvement.

Contingency planning for information systems supporting essential functions remain challenged. Weaknesses continue to exist in NARA's identification of mission-critical systems; management of information system inventory and system security categorization; and maintenance of ISCP documents in accordance with NARA policy and NIST guidance. Specifically, NARA did not maintain up-to-date ISCPs, ISCP tests, or Business Impact Analyses (BIAs) for many of the systems that perform or support NARA's MEFs or ESAs in the sample. This occurred because of a lack of coordination between NARA organizations for determining and maintaining a list of mission-critical systems; and policies and procedures for maintaining up-to-date ISCPs were not adequately followed. FCD-1 requires organizations to identify, prioritize, and document essential functions in the continuity plan, which should include plans and procedures to ensure access to critical communications and information systems necessary to support sustainment of essential functions. In addition, NARA's IT Security Methodology for Contingency Planning, consistent with NIST SP 800-53 Rev. 4 states NARA System Owners are responsible for developing and testing contingency plans for the information system at least annually to determine the effectiveness of the plan and the NARA System Owner (SO) or Information System Security Officer (ISSO)'s readiness to execute the plan. Failure to maintain up-to-date contingency plans and ensure the plans are tested on a periodic basis may result in the inability to provide interim measures to recover information system services after a disruption.

Lack of Coordination between NARA Organizations for Mission-Critical Systems

NARA's HQ COOP Plan, maintained by Business Support Services, includes a list of mission-critical systems, applications, and services necessary for the first thirty days of a continuity event that are not otherwise mandated or required by the National Continuity Policy and related Executive Orders and Directives. As of June 2017, we found the Plan included at least 15 systems, applications, or services supporting one or more essential functions at NARA. However, NARA's Information Services only designated access to the internet and e-mail capability as mission-critical functions in the IT Security Architecture. During the course of the audit, we notified Information Services of the discrepancy, and subsequently, the IT Security Architecture document was updated twice (March and August 2017); however, neither of the revisions included an updated list of NARA's mission-critical systems or a reference to the mission-critical systems already designated in the NARA HQ COOP Plan.

Additionally, there were at least 10 systems that support one or more essential functions sampled. Of the 10 systems, Emergency Federal Register (EFR) was not in NARA's information system inventory, and therefore not assigned a security categorization. We also found 3 systems with a security categorization of "Low", and one system included in the inventory but not assigned security categorization. Assigning a security categorization is the first step in the risk management process whereby organizations must select an appropriate set of security controls for their information systems that satisfy the minimum security requirements for the security category determined.[13] Without ensuring all NARA systems are included in the system inventory and proper security categories are assigned to the systems in the inventory, NARA cannot ensure appropriate security controls are selected and implemented to maintain confidentiality, integrity, and availability of the information and information systems that support NARA's essential functions.

Further, we found there are information systems that were not listed as mission-critical systems in NARA's HQ COOP Plan but support essential functions. For example, ERA[14] and Description and Authority Service (DAS)[15] support at least two essential functions, MEFs 41 and 43, and LMS supports the TT&E for NARA's COOP program. Based on the definition of mission-critical systems found in the NARA HQ COOP Plan, if any of these systems are necessary for the continued operation of essential functions and mission-critical supporting activities for the first thirty days of a continuity event, they should be included in the list. However, these systems have not been designated as mission-critical.

[13] FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.
[14] ERA is a system designed to preserve and manage NARA's electronic records and to manage the lifecycle of records and other holdings; ERA allows federal agencies to perform critical record transactions with NARA online.
[15] DAS includes standardized descriptions of both non-electronic and born-digital holdings and provides secure access to them.

Our review of the Business Process Analysis (BPA) status for the essential functions at NARA found BPAs were completed for majority of the essential functions. However, due to the discrepancies we identified above, the accuracy and completeness of the resource requirements are not assured and may lead to a lack of emergency preparedness of the systems. This could result in a delayed resumption of the essential functions during or after a continuity event affecting NARA. According to Federal Continuity Directive 2 (FCD-2), July 2013, federal agencies perform a BPA to ensure correct resources, including information technology requirements are identified and available where needed during a disruption so that essential functions can be resumed quickly and performed as required.

Management of Information Systems Contingency Plans

We found 4 of the 10 systems in our sample did not have an ISCP, 5 did not have an ISCP test, and 3 did not have a BIA. In addition, ISCPs and BIAs for 3 of the systems in the sample were severely outdated. NARA has not made contingency planning for systems a priority.

NARA OIG has consistently reported NARA's deficiency in developing, maintaining, and testing up-to-date ISCPs and BIAs for its information systems as part of the annual Federal Information Security Modernization Act (FISMA) assessments and audits. The FY 2017 OIG (FISMA) assessment, conducted between July and October 2017, also found approximately 50% of the systems sampled were not compliant with the annual ISCP review, update, and testing requirements, many of which were also missing BIAs. In response to similar findings from a FY 2015 FISMA audit[16], NARA's Office of Information Services agreed to develop and annually review and update ISCPs for the systems with an impact level of moderate or high with planned completion dates of March through August 2017. However, as of April 2018, these action plans still remain open.

Lack of Insight into the Emergency Federal Register (EFR)

Although we found the documentation for eDOCS, including the ISCP, ISCP test, and BIA, was generally maintained effectively and contained up-to-date information on the security posture of the system, NARA lacked insight into EFR because it was not included in the Office of Information Services' system inventory. EFR must be utilized in national security emergency situations where eDOCS becomes inoperable. Information Services, who is responsible for maintaining an accurate and complete information system inventory, was misinformed that EFR was either a GPO-owned system; or not a system, but an output automatically created by eDOCS.

[16] OIG Audit Report No. 16-02, NARA's Compliance with FISMA, as Amended, Recommendations 16, 17, and 18.

Our interviews with the Office of the Federal Register (OFR) representatives and review of the documentation for the system revealed EFR is a NARA-owned system[17], and it does not share any connections or IT architecture with eDOCS. The lack of insight into EFR not only resulted in the system being excluded from the system inventory, but also led to missing a security categorization and an absence of an ISSO for the system. As a result, no security authorization package[18] or ISCP documentation was available for the system, indicating that NARA may not be fully cognizant about or be able to effectively manage the security state of this mission-critical system in the event of an emergency or disaster.

In addition, we found the documentation describing the roles and responsibilities for maintaining and testing the system had not been accurately maintained. Although there was a switch in the vendors for the system in 2011, as of July 2017, the document still included the outdated vendor information. The document also did not define who the NARA technical contact should be or how the daily monitoring of the server should be conducted as required. This occurred because acquisition of the hosting service was not considered a contract[19], and little oversight controls were put in place to ensure the system was effectively maintained and tested for security and availability. According to NARA's HQ COOP Plan, documents, including emergency documents, cannot become effective until they have been processed and disseminated in either the Federal Register or the Emergency Federal Register. Without oversight controls for EFR, NARA may not be able to maintain the operational capability to conduct PMEFs 5 and 6, jeopardizing the government's ability to effectively issue, disseminate, and enforce Presidential documents and executive branch regulatory actions in case of a national security emergency.

Recommendations

In order to improve the effectiveness of NARA's Information System Contingency Planning, we recommend:

> **Recommendation 13:** The Chief Information Officer, in collaboration with Business Support Services as applicable, conduct a review and reconciliation of the lists of mission-critical systems identified by the Office of Information Services and Business Support Services.

[17] NARA OFR makes annual payments to the vendor hosting the system in the cloud environment.

[18] A set of documentation (i.e., security plans, security assessment reports, and plans of action and milestones) that provide the authorizing officials and information system owners with an up-to-date status of the security state of the information system and its operating environment. (NIST SP 800-53, Rev. 4)

[19] The annual cost of hosting the system was under the micro-purchase threshold defined by the Federal Acquisition Regulation (FAR), and there is no contract documentation available for the service.

Management Response

Information Services will review and reconcile Information Services' and Business Support Services' lists of mission-critical systems. Information Services will

maintain the consolidated list.

Target Completion Date: March 29, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 14: The Chief Information Officer, in collaboration with Business Support Services as applicable, conduct a detailed re-evaluation of mission-criticality of the systems that are not currently listed as mission-critical, and reflect the results on the reconciled list of mission-critical systems identified from Recommendation 13.

Management Response

Information Services will conduct a detailed re-evaluation of mission-criticality of the systems that are not currently listed as mission-critical. Systems determined to be mission-critical will be included in the consolidated list identified in Recommendation 13.

Target Completion Date: March 29, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 15: The Chief Information Officer, in collaboration with Business Support Services as applicable, conduct a detailed review of the FIPS PUB 199 security categorization of all mission-critical systems identified from Recommendations 13 and 14 to ensure all of such systems are subject to appropriate contingency planning requirements documented in the NARA IT Security Methodology for Contingency Planning.

Management Response

Information Services, in collaboration with Business Support Services as applicable, will conduct a detailed review of the FIPS PUB 199 security categorizations of all mission-critical systems identified from Recommendations 13 and 14 to determine whether these systems are following appropriate contingency planning requirements documented in the NARA IT Security Methodology for Contingency Planning.

Target Completion Date: March 31, 2020

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 16: The Chief Information Officer, in collaboration with Business Support Services as applicable, develop a procedure to review the reconciled list of mission-critical systems identified from Recommendations 13 and 14 above at least on an annual basis to re-evaluate the systems' mission-criticality, identify newly commissioned, mission-critical systems, and remove systems that have been decommissioned.

Management Response

Information Services, in collaboration with Business Support Services, will develop a procedure to review the reconciled list of mission-critical systems identified from Recommendations 13 and 14, at least on an annual basis. Information Services will re-evaluate the systems' mission-criticality, identify newly commissioned, mission-critical systems, and remove systems that have been decommissioned.

Target Completion Date: March 29, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

In order to improve the oversight controls for the security and availability of EFR, we recommend:

Recommendation 17: The Chief Information Officer, in coordination with the Office of the Federal Register, include EFR in NARA's information system inventory.

Management Response

Information Services and the Office of the Federal Register will ensure that the EFR is included on NARA's information system inventory either as a standalone system or documented as a sub-system within another system's boundary.

Target Completion Date: March 29, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 18: The Chief Information Officer, in coordination with the Office of the Federal Register designate a SO, ISSO, and COR (if applicable) to EFR, to effectively maintain security and availability of the system.

Management Response

Information Services will assign a SO, ISSO, and COR (if applicable) to the EFR. If the EFR is documented as a sub-system within another system's boundary, that system's SO, ISSO, and COR will maintain security and availability of the system.

Target Completion Date: March 29, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 19: The Chief Information Officer, in coordination with the Office of the Federal Register, develop and implement a process to maintain an up-to-date security authorization package for the EFR system, including a system security plan, security assessment report, risk assessment report, plan of action and milestones (POA&M), contingency plan, contingency plan test, and business impact analysis.

Management Response

Information Services will follow the existing RMF process to maintain an up-to-date security authorization package for the EFR system, including a system security plan, security assessment report, risk assessment report, plan of action and milestones

(PO&M), contingency plan, contingency plan test, and business impact analysis; either as a standalone system or subsystem.

Target Completion Date: March 31, 2020

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 20: The Chief Information Officer develop and implement a process to update the contingency plan, contingency plan test results, and business impact analysis on an annual basis for all information systems with a FIPS PUB 199 security categorization of moderate or high.

Management Response

Information Services will follow the existing RMF process to update the contingency plan, contingency plan test results, and business impact analysis on an annual basis for all information systems with a FIPS PUB 199 security categorization of moderate or high. The CIO will award an ISSO contract to perform this work.

Target Completion Date: March 31, 2020

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 21: The Director of the Federal Register develop and maintain an up-to-date Standard Operating Procedures (SOP) for maintaining and testing the EFR system.

Management Response

The Director of the Federal Register will create standard operating procedures for maintaining and testing the EFR system.

Target Completion Date: December 31, 2018

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 22: The Director of the Federal Register develop and implement a process to review, update, and test the SOP created from Recommendation 21 at least on an annual basis, including as part of the annual Eagle Horizon exercises, and document and submit to NARA's Continuity Coordinator the test results.

Management Response

The Director of the Federal Register will add processes to the standard operating procedures referenced in Recommendation 21 to address and implement reviewing, updating and testing our EFR SOP on an annual basis.

Target Completion Date: December 31, 2018

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 23: The Executive for Business Support Services include the activation of EFR as part of the annual Eagle Horizon exercise plan, regardless of the continuity scenarios applicable to the year, and develop and implement a process to review the test results from OFR.

Management Response

Business Support Services, in collaboration with the Office of the Federal Register, will ensure the activation and publication of the EFR is one of the objectives of the 2019 Eagle Horizon exercise plan and include as a part of that plan, Office of the Federal Register standard operating procedure to publish the EFR electronically as a test result.

Target Completion Date: May 31, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 3. Management of Essential COOP Documents Needs Improvement.

Although COOP Plans for the HQ and field sites were generally maintained up-to-date in designated electronic locations, other Emergency Response Plans, including the Occupant Emergency Plans (OEPs), Pandemic Influenza Plans (PIP), and Records Emergency Plans (REPs), were not always maintained in accordance with federal guidance and NARA policies and procedures. This occurred because policies and procedures for maintaining up-to-date Emergency Response Plans were not always followed by designated officials at NARA sites. Numerous federal policy documents and publications, including FCD-1, as well as NARA Directives, emphasize the importance of maintaining up-to-date essential COOP documents. As a result of NARA's actions, NARA may not be able to ensure each location is prepared to:

(1) provide a set of procedures to address specific emergency conditions;
(2) provide continuity strategy to prepare for, and begin responding to, an influenza pandemic, and;
(3) provide an understandable and accessible reference for use in emergency situations where any records in NARA control or custody are affected or threatened.

Additionally, NARA is not in full compliance with the essential document management requirements outlined in FCD-1, and may not be able to provide a set of complete and up-to-date procedures to address specific emergency conditions.

FCD-1 defines essential records as those an organization needs to meet operational responsibilities under national security emergencies or other emergency conditions, or to protect the legal and financial rights of the government. It states essential records must include a copy of the organization's continuity plans, which must be reviewed and updated (if necessary) to ensure the latest versions are available. FEMA's *Continuity Planning for Pandemic Influenza* encourages organizations to develop a PIP to ensure additional considerations are addressed during a pandemic. Further, the *Occupant Emergency Programs: An Interagency Security Committee Guide* requires the Designated Official of the facility to develop, implement, maintain, review, and sign the OEP. The OEP should be written with input from and be signed by each tenant agency representative for a multi-tenant facility. Additionally, NARA Directive 1561 states the facility director or administrator and the Records Emergency Management Team

(REMT)[20] must annually review the records emergency preparedness plan and the records emergency response and recovery plan[21], and update the plans as needed, to prevent or minimize damage to records in case there is a threat of damage or loss of records.

These plans, among others, are contained in NARA's continuity program and are considered vital components of NARA's continuity and emergency management. NARA utilizes a network folder hosted in NARA's alternate facility in Rocket Center, WV to copy and store the agency's vital records in electronic formats. In addition to the Vital Records folder, NARA requires Designated Officials for each facility to certify that they maintain the current version of the Continuity Plan and associated procedures in OpsPlanner, a cloud-based emergency planning and alert notification tool.

The following observations were made during audit fieldwork as of August 2017.[22]

- An OEP for the Federal Register was not maintained in accordance with the Interagency Security Committee Guidance, where the Designated Officials for each tenant agency are required to provide input to and sign in receipt of the OEP for the facility.
- OEPs for 6 facilities, PIPs for 3 facilities, and REPs for all HQ facilities and FRCs in the sample were not found on the Vital Records drive.
- OEPs PIPs for the HQ facilities were not found in OpsPlanner, and many of the REPs found in OpsPlanner were either not found or outdated.
- Records of changes for REPs were not consistently completed by NARA sites in the sample, and conflicting guidance existed as to where REPs should be stored.
- Many folders in OpsPlanner were poorly organized, and subfolders and documents no longer utilized or applicable, dating back to 2008, were stored with current documents in the same folders.
- Although the COOP & Essential Records Inventory and Tracking Report (CERIT) included a document inventory by NARA organization, it did not include a document inventory by site.
- The Essential Records Certification Statements for each NARA organization did not include a requirement to confirm essential documents are also present in OpsPlanner, which also conflicts with the requirements followed by many NARA facilities that essential documents should be present in both electronic locations.

[20] The group appointed for each NARA facility responsible for planning, coordinating, and overseeing the development and implementation of the records emergency preparedness plan and the response and recovery plan.
[21] These plans are currently called Records Emergency Plans.
[22] Some of these documents were added to one or both of the electronic repository locations subsequent to auditor inquiry.

Recommendations

In order to manage NARA's COOP documents more effectively and efficiently, we recommend:

Recommendation 24: The Executive for Business Support Services, in coordination with Corporate Records Management, ensure NARA's essential COOP documents, including COOP Plans, OEPs, PIPs, and REPs, are reviewed on an annual basis, updated as needed, and stored in designated electronic locations.

Management Response

Business Support Services, in collaboration with Corporate Records Management, will develop a set of requirements and instructions and communicate them to Designated Officials and Local Continuity Managers for an annual review update, certification, and proper filing location for the COOP, OEP, and PIPs. REPs are not essential COOP documents. Annual updates will be conducted in accordance with NARA 1561 and Interim Guidance 1561-1.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 25: The Executive for Business Support Services ensure Occupant Emergency Plans for all NARA sites, where NARA is a tenant agency, are provided to NARA's Designated Official for the site on an annual basis for review, update if necessary, and a signature.

Management Response

In conjunction with the planned action to address Recommendation 24, Business Support Services will incorporate instructions for the annual review, update and concurrence signature of OEP's by the NARA Designated Officials at the facilities where NARA is a tenant agency.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 26: The Executive for Business Support Services, in coordination with Corporate Records Management, develop and implement a file structure to more effectively organize and manage current and non-current COOP documents for each MEF, ESA, and facility.

Management Response

Business Support Services, in coordination with Corporate Records Management, will update the Vital (Essential) Records of the NARA HQ COOP Plan and the corresponding file structure of the Vital (Essential) Records drive to correspond with current requirements, organizational structure, and the Essential Records Inventory and Tracking Program (CERIT).

Target Completion Date: January 31, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 27: The Executive for Business Support Services, in coordination with Corporate Records Management, Develop and implement a process to maintain version control and record of changes for revisions made to essential COOP documents and Emergency Response Plans.

Management Response

Per NARA Records Schedule DAA-0064-2011-0002, Emergency plans and documentation that explain or amplify them are temporary in nature and the Disposition instructions are "Destroy when superseded." Business Support Services, in collaboration with Corporate Records Management, and in conjunction with the planned action for Recommendation 24, will add a table to create a record of changes for revisions and include instructions for the purging and destruction of all superseded documentation at the front of key documents.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 28: The Executive for Business Support Services, in coordination with Corporate Records Management, ensure all essential COOP documentation and their locations are reflected in CERIT.

Management Response

Business Support Services, in collaboration with Corporate Records Management will develop procedures to include a document inventory by site (field location) in the CERIT and to confirm that the limited set of duplicate essential records that should be included in OpsPlanner are verified and documented on the CERIT inventory.

Target Completion Date: April 30, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 4. Improvement is Needed in Providing and Tracking COOP Training.

While NARA tracks the overall number of employees who take the annual COOP training provided via LMS, it does not track the training status based on the designated role of the employee (senior leadership, staff with assigned COOP roles, and all other staff). NARA also lacks mission-specific training, tailored to each NARA organization supporting essential functions. NARA relies heavily on the annual Eagle Horizon exercise as its best TT&E opportunity and has not developed a process to provide other in-depth, mission-specific training opportunities. According to NARA HQ COOP Plan, the objectives for NARA's TT&E includes: (a) ensuring agency personnel are sufficiently trained to carry out minimum essential operations and functions when deployed at a COOP site or working in a COOP environment; and (b) conducting individual and team training of agency personnel to ensure currency of knowledge and integration of skills necessary to implement COOP plans and carry out essential functions. Failure to ensure employees are knowledgeable of and adequately trained on their roles and responsibilities may result in a substantial delay in carrying out minimum essential operations and functions in a COOP environment.

The AARs for FY 2016 and FY 2017 Operation Activate exercises consistently reported many exercise players expressed their concern that they were unfamiliar with their ERG responsibilities and COOP processes. According to the FY 2016 AAR, between 15% and 20% of participating ERG members stated lack of familiarity with COOP initiatives and their respective roles and responsibilities, despite the training available in LMS. In addition, a similar percentage of the participants stated they did not feel their field site was prepared to execute the COOP plan.

Our inquiries with the representatives for essential functions in the sample revealed most NARA organizations supporting such functions solely relied on the annual NARA-wide COOP training in LMS and Eagle Horizon exercises as their COOP training opportunities. NARA offices with significant COOP responsibilities have not developed SOPs or similar documentation containing detailed instructions on how the essential functions or supporting activities will be carried out during or after a continuity event. In addition, according to the FY 2017 Eagle Horizon Players Handbook, 52 of 226 employees with assigned COOP roles, or 23%, did not participate in the exercise.

Although NARA has reported consistently reaching over 90% completion rate of the annual All Staff COOP training provided in LMS, NARA does not track the completion of training based on each employee's assigned role. For example, if an ERG employee completes the "All Other Staff" module instead of the "Staff with Assigned COOP Roles" module, the selection and completion of an incorrect training module is not reflected on the employee's training status. The AAR from FY 2016 Eagle Horizon exercise showed, although there are 266 staff with assigned COOP roles NARA-wide, 324 employees completed the "Staff with Assigned COOP Roles" module, indicating that at least 58 employees selected the wrong training module. The AAR also showed the training completion rate of the actual staff with assigned COOP roles was approximately 63%. However, there was no way to determine what modules these individuals completed.

According to NARA's TT&E Lead for COOP, several NARA offices have recently requested COOP training specific to their offices during the fieldwork of the audit. None of NARA offices had requested COOP training in prior years. During our interview with the TT&E Lead, the employee stated NARA offices are encouraged to request COOP training specific to the essential functions supported by the office. However, there is no formalized process to provide COOP training to offices supporting essential functions.

Recommendations

In order to more effectively provide and track COOP training for employees with COOP responsibilities, we recommend:

> **Recommendation 29:** The Executive for Business Support Services review the training needs of staff in light of their comments in exercise AARs and either:

(a) develop and implement the content and schedule of mission-specific COOP training to be provided to each NARA office on a periodic basis; or,
(b) develop and implement a systematic process to ensure and all NARA employees take the correct, annual COOP training module commensurate with their roles and responsibilities, and accurately track the status based on the assigned roles.

Management Response

Business Support Services will develop and implement a systematic process to ensure all NARA employees take the correct, annual COOP training module commensurate with their roles and responsibilities, and accurately track the status based on the assigned roles.

Target Completion Date: March 29, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Finding 5. Review and Submission of SF-2050 Lacked Formalized Process.

We found NARA does not ensure the SF-2050, *Reconstitution Questionnaire*, is reviewed and submitted to GSA for NARA's headquarters on an annual basis. NARA used the data for available resources for its headquarter locations (gathered in 2014), to populate the SF-2050s for subsequent years without conducting an annual review of the currency of the data. This occurred because NARA has not developed or implemented a systematic process to review and submit the SF-2050, as mandated by FCD-1. According to FCD-1, to assist in scoping of the Federal Government's reconstitution plans and programs, organizations should internally identify and document anticipated reconstitution needs for headquarter facilities located within the National Capital Region (NCR) by completing and submitting SF-2050. In addition, organizations are required to annually review and submit their SF-2050 to GSA. Without a formalized process to review, update, and submit accurate and complete SF-2050s on an annual basis, NARA may not be providing GSA information it needs to adequately scope the Federal Government's reconstitution plans and programs.

Recommendations

In order to complete and submit SF-2050 as intended by FCD-1, we recommend:

Recommendation 30: The Executive for Business Support Services develop and implement a systematic process to: (a) conduct a review of the source data for the SF-2050 for NARA's facility in College Park, MD (Archives II), which is the primary operating

facility on an annual basis for accuracy, update the data if necessary, and maintain documentation of the review for future reference; and (b) submit the completed form to GSA on an annual basis.

Management Response

Business Support Services will develop and implement a process to review, update, and submit accurate and complete SF-2050s to GSA on annual basis.

Target Completion Date: March 29, 2019

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Appendix A – Acronyms

Acronyms	Definition
AAR	After-Action Report
ABL	Allegheny Ballistics Laboratory
AWS	Amazon Web Services
BIA	Business Impact Analysis
BPA	Business Process Analysis
CCAP	Continuity Corrective Action and Implementation Plan
CIO	Chief Information Officer
COMNAVSEA	Naval Sea Systems Command
COOP	Continuity of Operations
COR	Contracting Officer's Representative
CP	Contingency Plan
DAS	Description and Authority Service
DERG	Devolution Emergency Response Group
DHS	United States Department of Homeland Security
eDOCS	Electronic Editing and Publishing Document System
EFR	Emergency Federal Register
ERA	Electronic Records Archives
ERG	Emergency Relocation Group
ESA	Essential Supporting Activity
FAR	Federal Acquisition Regulation
FCD	Federal Continuity Directive
FEMA	Federal Emergency Management Agency
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act of 2014
FOSA	Field Office Systems Administrator
FPPS	Federal Personnel and Payroll System
FY	Fiscal Year
FRC	Federal Records Center
GSA	United States General Services Administration
GPO	United States Government Publishing Office
HR	Human Resources
HSPD	Homeland Security Presidential Directive
HQ	Headquarters
ICP	Internal Controls Program
ID	Identifier
ISCP	Information Systems Contingency Planning
ISSO	Information System Security Officer
IT	Information Technology
LMS	Learning Management System

Acronyms	Definition
MEF	Mission Essential Function
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NCC	National Continuity Coordinator
NCPIP	National Continuity Policy Implementation Plan
NEF	National Essential Function
NPRC	National Personnel Records Center
NSPD	National Security Presidential Directive
OEP	Occupant Emergency Plan
OIG	Office of Inspector General
O&M	Operation and Maintenance
PAO	Property Accountability Officer
PIP	Pandemic Influenza Plan
PMEF	Primary Mission Essential Function
REP	Records Emergency Plan
RPT/RIT	Reconstitution Planning and Reconstitution Implementation Team
RRS	Readiness Reporting System
SO	System Owner
SOP	Standard Operating Procedures
TMO	Telework Managing Officer
TT&E	Test, Training, and Exercise
VPN	Virtual Private Network

Appendix B – Management Response

NATIONAL ARCHIVES

Date: 17 August 2018

To: James Springs, Inspector General

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

Subject: Management's Response to OIG Report 18-AUD-14, *Audit of NARA's Continuity of Operations (COOP) Readiness*

Thank you for the opportunity to provide comments on this final report. We appreciate your willingness to meet and clarify language in the report.

As you know, the Federal Emergency Management Agency (FEMA) concluded their Biennial Continuity Assessment of this Agency in February 2018. FEMA determined that NARA has a comprehensive continuity program and the operational capability to sustain our essential functions during an emergency. Their assessment along with your audit will allow NARA to achieve a fully mature continuity of operations program.

We concur with the 30 recommendations in this audit, and in response, the attachment provides a summary of our proposed actions. As each recommendation is satisfied, we will provide documentation to your office. If you have questions about this action plan, please contact Kimm Richards at kimm.richards@nara.gov or by phone at 301-837-1668.

DAVID S. FERRIERO
Archivist of the United States

Attachment

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20408-0001
www.archives.gov

Action Plan Response to OIG Report 18-AUD-14,
Audit of NARA's Continuity of Operations (COOP) Readiness

Recommendation 1: We recommend the Human Capital Officer, in collaboration with Business Support Services, develop and implement a process to ensure all designated ERG/DERG/RPT members maintain a copy of current telework agreements.

Planned Action: Human Capital will update telework policy (NARA 332) and COOP documentation (Player Handbook) to no longer explicitly require a telework agreement specifically from designated ERG/DERG/RPT players. COOP participants will still require a telework agreement, but under the general requirement that all NARA employees must have an agreement in order to telework. NARA will further update the telework policy to clarify that any employee may be required to telework in the event of an actual emergency, regardless of whether he or she has a telework agreement. In addition, NARA will no longer require that extra copies of telework agreements be stored on the vital records drive.

Target Completion Date: December 31, 2018

Recommendation 2: We recommend the Chief Information Officer:
(a) determine the laptop computer needs for all current ERG, DERG, and RIT/RPT member employees, in consultation with Executives responsible for executing the PMEFs, MEFs, and ESAs for NARA;
(b) conduct a cost-benefit analysis for providing a government-furnished laptop computer to those employees identified from (a); and
(c) provide a government-furnished laptop computer to the ERG, DERG, and RPT/RIT member employees, based on the analyses conducted from (a) and (b) above.

Planned Action: Information Services will work with each Executive responsible for executing the PMEFs, MEFs, and ESAs, to develop a needs assessment for remote productivity and to conduct a cost-benefit analysis for all current ERG, DERG, and RIT/RPT member employees. Based on the results of the needs assessment and the cost-benefit analyses, laptops will be provided to ERG, DERG, and RPT/RIT members.

Target Completion Date: March 29, 2019

Recommendation 3: We recommend Chief Human Capital Officer, in collaboration with the Chief Information Officer:
(a) update the telework policy to include the employee's responsibility to test the connectivity to NARANet when the employee uses a personally owned computer for teleworking; and

(b) provide a reference in the policy reminding teleworkers of NARA policies and procedures for using a personally owned computing resources to conduct official NARA duties.

Planned Action: Human Capital will update the NARA telework policy to require employees to test the connectivity to NARANet when using personally owned computers for teleworking. The updated policy will also include a reference to NARA policies regarding use of personally owned resources for conducting official NARA duties.

Target Completion Date: December 31, 2018

Recommendation 4: We recommend the Executive for Business Support Services develop and implement a process to ensure proper planning for updating and renewing all interagency agreements pertinent to NARA's continuity of operations is performed in a timely manner.

Planned Action: Business Support Services will add the MOU with NAVSEA to NARA's Continuity Multi-Year Strategy Program Management Plan (MYSPMP) to ensure proper planning for updating and renewal prior to its September 2021 expiration.

Target Completion Date: January 31, 2019

Recommendation 5: We recommend the Chief Information Officer ensure the inventory is reviewed and updated for all NARA IT assets at the alternate site, including ERA equipment, at least on an annual basis.

Planned Action: The Network Services Branch (IOO) will provide a copy of the complete and updated ERA inventory.

Target Completion Date: October 31, 2018

Recommendation 6: We recommend the Chief Information Officer ensure the NARA COOP Infrastructure Specification and Rocket Center Network Diagram document is reviewed on an annual basis and updated as necessary, consistent with any other IT policies, procedures, methodologies, and supplements to the policies.

Planned Action: The Network Services Branch (IOO) will provide an updated copy of the NARAnet Disaster Recovery and Contingency Plan and a corrected network diagram.

Target Completion Date: October 31, 2018

Recommendation 7: We recommend the Chief Human Capital Officer, in coordination with Business Support Services, establish controls to ensure the accurate supervisor-employee relationship is reflected on the staff accountability tool.

Planned Action: The Interior Business Center has added a new field to the employee record for the supervisor name in FPPS. This new field will be available to NARA in August 2018. We have requested that it be configured as a required field for NARA. In addition, we are developing a job aid to remind supervisors of the requirement to put through an action in FPPS when supervisors change.

Target Completion Date: December 31, 2018

Recommendation 8: We recommend the Chief Human Capital Officer, in coordination with Business Support Services, consider implementing controls to ensure the submitter only has access to the organization to which he/she belongs.

Planned Action: Human Capital, in coordination with Business Support Services, will evaluate the risks and benefits of restricting access as recommended and will take appropriate actions, including documenting Management's acceptance of the risk, if that is the appropriate result.

Target Completion Date: December 31, 2018

Recommendation 9: We recommend the Chief Human Capital Officer, in coordination with Business Support Services, consider implementing a unique username and password to each authorized submitter of the form for user accountability and data integrity.

Planned Action: Human Capital, in coordination with Business Support Services, will evaluate the risks and benefits of restricting access as recommended and will take appropriate actions, including documenting Management's acceptance of the risk, if that is the appropriate result.

Target Completion Date: December 31, 2018

Recommendation 10: We recommend the Executive of Business Support Services, in collaboration with the Offices of Human Capital and Information Services as applicable, strengthen the process to manage personnel readiness data submission to more accurately count completed submissions and verify the accuracy of the data submitted.

Planned Action: Business Support Services will evaluate the costs and benefits of applying more active management of personnel readiness data and will take

appropriate actions, including documenting Management's acceptance of the risk, if that is the appropriate result.

Target Completion Date: November 30, 2018

Recommendation 11: We recommend the Executive of Business Support Services, develop and implement a process to remind the participants who have not completed the submission to complete it.

Planned Action: Business Support Services will incorporate this recommendation into the cost-benefit analysis in recommendation 10.

Target Completion Date: November 30, 2018

Recommendation 12: We recommend the Executive of Business Support Services, in collaboration with the Offices of Human Capital and Information Services as applicable, consider providing exercise participants with personalized link to the data sheet, with pre-populated basic personnel information, where participants could review, verify, and add required information, for data integrity and efficient use of exercise time.

Planned Action: Business Support Services will evaluate the costs and benefits of increasing personnel data collection efforts as recommended and will take appropriate actions, including documenting Management's acceptance of the risk, if that is the appropriate result.

Target Completion Date: November 30, 2018

Recommendation 13: We recommend the Chief Information Officer, in collaboration with Business Support Services as applicable, conduct a review and reconciliation of the lists of mission-critical systems identified by the Office of Information Services and Business Support Services.

Planned Action: Information Services will review and reconcile Information Services' and Business Support Services' lists of mission-critical systems. Information Services will maintain the consolidated list.

Target Completion Date: March 29, 2019

Recommendation 14: We recommend the Chief Information Officer, in collaboration with Business Support Services as applicable, conduct a detailed re-evaluation of mission-criticality of the systems that are not currently listed as mission-critical, and

reflect the results on the reconciled list of mission-critical systems identified from Recommendation 13.

Planned Action: Information Services will conduct a detailed re-evaluation of mission-criticality of the systems that are not currently listed as mission-critical. Systems determined to be mission-critical will be included in the consolidated list identified in Recommendation 13.

Target Completion Date: March 29, 2019

Recommendation 15: We recommend the Chief Information Officer, in collaboration with Business Support Services as applicable, conduct a detailed review of the FIPS PUB 199 security categorization of all mission-critical systems identified from Recommendations 13 and 14 to ensure all of such systems are subject to appropriate contingency planning requirements documented in the NARA IT Security Methodology for Contingency Planning.

Planned Action: Information Services, in collaboration with Business Support Services as applicable, will conduct a detailed review of the FIPS PUB 199 security categorizations of all mission-critical systems identified from Recommendations 13 and 14 to determine whether these systems are following appropriate contingency planning requirements documented in the NARA IT Security Methodology for Contingency Planning.

Target Completion Date: March 31, 2020

Recommendation 16: We recommend the Chief Information Officer, in collaboration with Business Support Services as applicable, develop a procedure to review the reconciled list of mission-critical systems identified from Recommendations 13 and 14 above at least on an annual basis to re-evaluate the systems' mission-criticality, identify newly commissioned, mission-critical systems, and remove systems that have been decommissioned.

Planned Action: Information Services, in collaboration with Business Support Services, will develop a procedure to review the reconciled list of mission-critical systems identified from Recommendations 13 and 14, at least on an annual basis. Information Services will re-evaluate the systems' mission-criticality, identify newly commissioned, mission-critical systems, and remove systems that have been decommissioned.

Target Completion Date: March 29, 2019

Recommendation 17: We recommend the Chief Information Officer, in coordination with the Office of the Federal Register, include EFR in NARA's information system inventory.

Planned Action: Information Services and the Office of the Federal Register will ensure that the EFR is included on NARA's information system inventory either as a standalone system or documented as a sub-system within another system's boundary.

Target Completion Date: March 29, 2019

Recommendation 18: We recommend the Chief Information Officer, in coordination with the Office of the Federal Register designate a SO, ISSO, and COR (if applicable) to EFR, to effectively maintain security and availability of the system.

Planned Action: Information Services will assign a SO, ISSO, and COR (if applicable) to the EFR. If the EFR is documented as a sub-system within another system's boundary, that system's SO, ISSO, and COR will maintain security and availability of the system.

Target Completion Date: March 29, 2019

Recommendation 19: We recommend the Chief Information Officer, in coordination with the Office of the Federal Register, develop and implement a process to maintain an up-to-date security authorization package for the EFR system, including a system security plan, security assessment report, risk assessment report, plan of action and milestones (PO&M), contingency plan, contingency plan test, and business impact analysis.

Planned Action: Information Services will follow the existing RMF process to maintain an up-to-date security authorization package for the EFR system, including a system security plan, security assessment report, risk assessment report, plan of action and milestones (PO&M), contingency plan, contingency plan test, and business impact analysis; either as a standalone system or subsystem.

Target Completion Date: March 31, 2020

Recommendation 20: We recommend the Chief Information Officer develop and implement a process to update the contingency plan, contingency plan test results, and business impact analysis on an annual basis for all information systems with a FIPS PUB 199 security categorization of moderate or high.

Planned Action: Information Services will follow the existing RMF process to update the contingency plan, contingency plan test results, and business impact analysis on an annual basis for all information systems with a FIPS PUB 199 security categorization of moderate or high. The CIO will award an ISSO contract to perform this work.

Target Completion Date: March 31, 2020

Recommendation 21: We recommend the Director of the Federal Register develop and maintain an up-to-date Standard Operating Procedures (SOP) for maintaining and testing the EFR system.

Planned Action: The Director of the Federal Register will create standard operating procedures for maintaining and testing the EFR system.

Target Completion Date: December 31, 2018

Recommendation 22: We recommend the Director of the Federal Register develop and implement a process to review, update, and test the SOP created from Recommendation 21 at least on an annual basis, including as part of the annual Eagle Horizon exercises, and document and submit to NARA's Continuity Coordinator the test results.

Planned Action: The Director of the Federal Register will add processes to the standard operating procedures referenced in Recommendation 21 to address and implement reviewing, updating and testing our EFR SOP on an annual basis.

Target Completion Date: December 31, 2018

Recommendation 23: We recommend the Executive for Business Support Services include the activation of EFR as part of the annual Eagle Horizon exercise plan, regardless of the continuity scenarios applicable to the year, and develop and implement a process to review the test results from OFR.

Planned Action: Business Support Services, in collaboration with the Office of the Federal Register, will ensure the activation and publication of the EFR is one of the objectives of the 2019 Eagle Horizon exercise plan and include as a part of that plan, Office of the Federal Register standard operating procedure to publish the EFR electronically as a test result.

Target Completion Date: May 31, 2019

Recommendation 24: We recommend the Executive for Business Support Services, in coordination with Corporate Records Management, ensure NARA's essential COOP documents, including COOP Plans, OEPs, and PIPs, and REPs, are reviewed on an annual basis, updated as needed, and stored in designated electronic locations.

Planned Action: Business Support Services, in collaboration with Corporate Records Management, will develop a set of requirements and instructions and communicate them to Designated Officials and Local Continuity Managers for an annual review, update, certification, and proper filing location for the COOP, OEP, and PIPs. REPs are not essential COOP documents. Annual updates will be conducted in accordance with NARA 1561 and Interim Guidance 1561-1.

Target Completion Date: September 30, 2019

Recommendation 25: We recommend the Executive for Business Support Services ensure Occupant Emergency Plans for all NARA sites, where NARA is a tenant agency, are provided to NARA's Designated Official for the site on an annual basis for review, update if necessary, and a signature.

Planned Action: In conjunction with the planned action to address Recommendation 24, Business Support Services will incorporate instructions for the annual review, update and concurrence signature of OEP's by the NARA Designated Officials at the facilities where NARA is a tenant agency.

Target Completion Date: September 30, 2019

Recommendation 26: We recommend the Executive for Business Support Services, in coordination with Corporate Records Management, develop and implement a file structure to more effectively organize and manage current and non-current COOP documents for each MEF, ESA, and facility.

Planned Action: Business Support Services, in coordination with Corporate Records Management, will update the Vital (Essential) Records of the NARA HQ COOP Plan and the corresponding file structure of the Vital (Essential) Records drive to correspond with current requirements, organizational structure, and the Essential Records Inventory and Tracking Program (CERIT).

Target Completion Date: January 31, 2019

Recommendation 27: We recommend the Executive for Business Support Services, in coordination with Corporate Records Management, develop and implement a process

to maintain version control and record of changes for revisions made to essential COOP documents and Emergency Response Plans.

Planned Action: Per NARA Records Schedule DAA-0064-2011-0002, Emergency plans and documentation that explain or amplify them are temporary in nature and the Disposition instructions are "Destroy when superseded." Business Support Services, in collaboration with Corporate Records Management, and in conjunction with the planned action for Recommendation 24, will add a table to create a record of changes for revisions and include instructions for the purging and destruction of all superseded documentation at the front of key documents.

Target Completion Date: September 30, 2019

Recommendation 28: We recommend the Executive for Business Support Services, in coordination with Corporate Records Management, ensure all essential COOP documentation and their locations are reflected in CERIT.

Planned Action: Business Support Services, in collaboration with Corporate Records Management will develop procedures to include a document inventory by site (field location) in the CERIT and to confirm that the limited set of duplicate essential records that should be included in OpsPlanner are verified and documented on the CERIT inventory.

Target Completion Date: April 30, 2019

Recommendation 29: We recommend the Executive for Business Support Services review the training needs of staff in light of their comments in exercise AARs and either:
(a) develop and implement the content and schedule of mission-specific COOP training to be provided to each NARA office on a periodic basis; or,
(b) develop and implement a systematic process to ensure and all NARA employees take the correct, annual COOP training module commensurate with their roles and responsibilities, and accurately track the status based on the assigned roles.

Planned Action: Business Support Services will develop and implement a systematic process to ensure all NARA employees take the correct, annual COOP training module commensurate with their roles and responsibilities, and accurately track the status based on the assigned roles.

Target Completion Date: March 29, 2019

Recommendation 30: We recommend the Executive for Business Support Services develop and implement a systematic process to:

(a) conduct a review of the source data for the SF-2050 for NARA's facility in College Park, MD (Archives II), which is the primary operating facility on an annual basis for accuracy, update the data if necessary, and maintain documentation of the review for future reference; and
(b) submit the completed form to GSA on an annual basis.

Planned Action: Business Support Services will develop and implement a process to review, update, and submit accurate and complete SF-2050s to GSA on annual basis.

Target Completion Date: March 29, 2019

Appendix C – Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Chief Operating Officer
Deputy Chief Operating Officer
Chief of Management and Administration
Executive for Business Support Services
Chief Information Officer
Chief Innovation Officer
Chief Human Capital Officer
Director of Office of the Federal Register
Director of Corporate Records Management
Accountability
United States House Committee on Oversight and Government Reform
Senate Homeland Security and Governmental Affairs Committee

OIG Hotline

To report fraud, waste, or abuse, please contact us:

Electronically:
OIG Hotline Referral Form

Telephone:
301-837-3500 (Washington, D.C. Metro Area)
1-800-786-2551 (toll-free and outside the Washington, D.C. metro area)

Mail:
IG Hotline
NARA
P.O. Box 1821
Hyattsville, MD 20788-0821