Audit of NARA's Data Backup Operations

OIG Audit Report No. 13-09

July 9, 2013

Table of Contents

Executive Summary

Organizations should routinely duplicate or back up data files, computer programs, and critical documents. This assists in the organization's ability to ensure uninterrupted operations by providing reasonable and timely data recovery capabilities. Our objective was to determine whether NARA had a systematic, accountable, and documented process for restoring original data after a data loss event. Specifically, our review focused on whether NARA had documented plans and procedures for backing up data, whether backups were occurring on a regular basis, whether backups were tested to verify media reliability and information integrity, and whether the backup copies of the operating system and other critical information system software were stored in a separate facility from the operational software.

Overall, with the exception of the ERA, successful backups were accomplished on a regular basis for the systems reviewed. A full backup for one instance of the ERA system has not been accomplished since May 2011. In addition, security control weaknesses existed within NARA's data backup operations which jeopardize NARA's ability to sufficiently protect the confidentiality, integrity, and availability of data backups. For example, backup tapes containing Personally Identifiable Information (PII) were not encrypted to protect the information while stored offsite; backups were not regularly tested to ensure data could be restored in usable form; and backup media was not rotated offsite each week as prescribed. Without information system backup controls to protect data backups, there is an increased risk recovery operations could be delayed or information could be lost.

The audit also identified an opportunity for cost savings related to excess Iron Mountain storage containers in NARA's possession. Over the last seven years, NARA has spent about $31,900 that could have been put to better use. NARA decreased the number of tapes and other storage media stored offsite but did not return the excess containers to Iron Mountain. By reviewing and reducing the number of containers kept in the rotation for offsite storage, NARA could significantly reduce the cost of this service.

Payments made for offsite storage of backup tapes need further review to determine whether NARA's procurement process as well as Federal laws and regulations were violated. In addition, the payment for offsite storage costs may have been improper, and if so, NARA has paid approximately $48,712 over the last four years that could have been put to better use.

This report makes 11 recommendations to strengthen the management, accountability, and oversight of the data backup and recovery processes at NARA.

Background

Information systems are vital elements in most mission/business processes. Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures enabling a system to be recovered as quickly and effectively as possible following a service disruption. Contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level.

Organizations are required to adequately mitigate the risk arising from the use of information and information systems in the execution of mission and business processes. Contingency strategies are created to mitigate the risks for the contingency planning family of controls and cover the full range of backup, recovery, contingency planning, testing, and ongoing maintenance. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, contains the baseline set of controls that protect the confidentiality, integrity, and availability of a system and its information. Within SP 800-53, Contingency Planning Control 9 (CP-9) requires organizations to conduct backups of user-level and system-level data and to protect the confidentiality, integrity, and availability of backup information at the storage location.

Information system backups at NARA are managed by contractors. The NARA IT and Telecommunications Support Services (NITTSS) contractor is responsible for multiple systems running Novell SUSE Linux Enterprise Server (SLES), Microsoft Windows, UNIX, and Novell Netware. NARA Network (NARANet) systems data are backed up on a varied rotation of full and incremental backups which is not identical for all systems. The backup method, retention and destination of data backups are also different for each system. For example, Novell file and print servers are backed up at NARA's College Park, MD facility (AII) and replicated to NARA's facility at the Allegany Ballistic Laboratory (ABL), then transferred to tape. Novell Groupwise backups are replicated to ABL then to tape. Windows and UNIX servers are backed up using an Enterprise backup system at AII or locally attached media drives.

This audit also included a review of two systems, the Electronic Records Archives (ERA) and the Case Management and Reporting System (CMRS). The purpose of ERA is to preserve and manage NARA's electronic records and manage the lifecycle of paper

records and other holdings, including supporting records retention schedules and the accessioning process for all Federal records. In September 2011, NARA awarded an Operations and Maintenance contract for continued support of ERA. According to the contract Performance Work Statement (PWS), the contractor is required to perform backup of ERA systems and devices with the intent of having recoverable systems, data and services. Server backups were to include daily server file system backups, and the contractor is required to verify successful completion of all backups.

CMRS automates the end-to-end case processing for military records. CMRS assists in locating the record, assigning requests to staff, preparing the response to the customers, electronically referring requests to other offices, and advising the customer of the status of their request. The users of CMRS are entirely dependent upon the system to do their work. In September 2012, NARA issued a one year contract for the operations and maintenance of the NARA Integrated Siebel Platform (NISP) which covers several NARA systems, including CMRS. According to the contract, the contractor was to perform daily incremental backups and weekly full backups of the NISP database and system servers.

NITTSS, ERA, and CMRS contractors used NetBackup software to manage the system backups. NetBackup allows periodic or calendar-based schedules to perform automatic, unattended backups for clients across a network. The backups can be full or incremental. Full backups back up all client files. Incremental backups back up only the files that have changed since the last backup.

Objectives, Scope, Methodology

The purpose of this audit was to determine whether NARA had a systematic, accountable, and documented process for restoring original data after a data loss event. Specifically, we reviewed whether NARA had documented plans and procedures for backing up data; whether successful backups were accomplished on a regular basis; whether backups were tested to verify media reliability and information integrity; and whether backup copies of the operating system and other critical information system software were stored in a separate facility or in a fire-rated container which was not collocated with the operational software.

To accomplish our objective, we reviewed NARA's IT Security Policies and IT Security Requirements as well as National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53, Revision 3 "Recommended Security Controls for Federal Information Systems and Organizations," May 2010, 800-53, Revision 4 "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, and 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems," May 2010. We obtained and reviewed backup and recovery procedures from NITTSS and the ERA contractors. We were unable to review any backup procedures for CMRS because at the time of our audit, procedures did not exist.

We interviewed NARA IT Operations personnel as well as the contractors responsible for conducting data backups for selected NARA systems, including NARA's NITTSS contractor which included backups of email servers, Novell file servers, and other application and support servers residing on NARANet. We also reviewed backups for two systems: the Electronic Records Archives (ERA) and the Case Management and Reporting System (CMRS).

We reviewed backup schedules for selected servers and compared the schedule with the backup system job history log files for incremental and full backups. For backup media stored offsite, we reviewed whether backup files were created and rotated offsite as prescribed. We reviewed the security controls in place to protect backups at the storage locations. For backups stored on tapes, we reviewed the inventory and tape log information at the storage locations and reviewed the process to destroy backup tapes when no longer needed. We conducted a site visit at the Iron Mountain offsite storage location for backup tapes and compared the contents of each NARA container stored in the vault to NARA's records.

Our audit work was performed at Archives II in College Park, Maryland, Allegany Ballistics Laboratory in Rocket Center, West Virginia, and the Iron Mountain storage facility in Columbia, Maryland between October 2012[1] and May 2013. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[1] This audit was originally announced in May 2011 but was put on hold due to staffing constraints and competing priorities. In October 2012, the audit was re-announced with the same audit objective.

Audit Results

1. Controls Over Data Backups.

Overall, with the exception of the ERA, successful backups were accomplished on a regular basis for the systems reviewed. A full backup for one instance of the ERA system has not been accomplished since May 2011. In addition, security control weaknesses existed within NARA's data backup operations which jeopardize NARA's ability to sufficiently protect the confidentiality, integrity, and availability of data backups. For example:

- backup tapes containing sensitive PII were not encrypted to protect the confidentiality of the information while stored offsite;
- a method or process to verify the integrity of the backups was not in place;
- backups were not regularly tested to ensure data could be recovered in usable form;
- backup media was not rotated offsite as prescribed; and
- one offsite storage location for backup tapes was not geographically removed from the primary site which may create accessibility problems in the event of an area-wide disaster.

This occurred because NARA did not fully implement the contingency planning control related to information system backup, which is designed to provide a means to recover data needed to restore system operations quickly and effectively following a service disruption. In addition, plans and procedures for data backup and recovery operations did not exist for one system we reviewed. Without information system backup controls to protect data backups, there is an increased risk recovery operations could be delayed or information could be lost.

According to NIST SP 800-34, data backups are done primarily for recovery purposes, and should be conducted on all systems on a regular basis. At NARA, support contractors manage system backups. We reviewed the backup operations performed by NARA's Operations Support contractor, NITTSS, which includes NARANet Novell, Windows, and UNIX servers. In addition, we also reviewed backup operations performed for ERA and CMRS, which are maintained by different support contractors.

We reviewed a sample of backups conducted by the three different support contractors and found that overall, system backups were accomplished on a regular basis. Two exceptions occurred for backups of ERA. Backups for the Executive Office of the

President (EOP) instance[2] of ERA are scheduled to be run once every eight weeks. However, the last successful backup for the EOP ERA instance occurred in May 2011.[3] Although data is static within the system, there have been several data spillage[4] incidents since the last backup was run which would delay restoration efforts. In addition, the EOP operating system has been upgraded twice since the last set of backups which would further delay restoration efforts. Although an exact amount of time is not known, one official estimated it could take six months to restore the EOP system from the May 2011 set of backup tapes. This amount of time to restore a backup may not be acceptable to respond to all special access requests, subpoenas made pursuant to the Presidential Records Act by investigative bodies or other requesting parties for documents or information.

According to one ERA official, the decision was made not to create a backup of the system until equipment upgrades and data migration were completed. Specifically, new equipment was installed and data in the current EOP instance will be migrated to the new equipment. Transfer of the data will most likely take several months. Once the transfer is complete, the old equipment will be decommissioned. The ERA official stated a backup was not made before starting the transfer because backup tapes made with the current system would not be readable on the new equipment.

We identified another exception for backups of the ERA Base instance, which contains permanent electronic Federal records. ERA backups take point-in-time images (snapshots) of the data being backed up at scheduled intervals throughout the day. The snapshot image of the data at midnight is written to tape and transferred offsite the next day. However, for approximately two weeks, the ERA Base instance did not have a successful backup. System administrators were alerted to problems with backups of the ERA Base system in November 2012 and a work around was used to continue to generate offsite tapes. In January 2013, the tape library was upgraded and backups would not run properly. After two weeks of trouble shooting different hardware and backup software configurations, backups resumed but ERA officials are continuing to experience problems related to the encryption of the backups. As of May 2013, ERA officials have not been able to encrypt backups and therefore, backup tapes are not being rotated offsite each day. Instead, according to an ERA official, ERA backups are sent by secure courier about once a month. Until sent offsite, the backup tapes are stored in the data center and

[2] ERA is composed of several "instances" which each focus on a set of records or ERA function. The EOP instance contains the electronic records from the George W. Bush Administration.
[3] According to the ERA Operations manager, EOP backups were not completed because the system was in the process of being upgraded.
[4] A data spill is a security incident that results in the transfer of classified or sensitive information to unaccredited and unauthorized information systems, applications or media. In order to restore the entire EOP instance from backup, each of the files containing classified information would have to be identified, and deleted, from the May 2011 set of backup tapes.

although there are fire-rated containers onsite, the containers are not large enough to hold the backup tapes for the Base instance.

Confidentiality of Backup Data

Data confidentiality involves protecting data both onsite and offsite from unauthorized access or use. Maintaining the security of system data and software is a key component in contingency planning. Encryption is a common method for securing stored system data. Encryption is most effective when applied to both the primary data storage device and on backup media going to an offsite location.

CMRS is a web based application which enables the request and fulfillment of military service information, such as personnel records and medical case files pertaining to 20th-century military veterans. Information stored within CMRS includes the veteran's name, social security number, and date of birth; therefore it is identified as having a high confidentiality level. Unencrypted backup tapes containing this sensitive information were routinely sent to NARA's offsite storage vendor, Iron Mountain. The tapes were stored in locked containers and the offsite facility had physical security controls in place to restrict access to the vault where the tapes are stored. However, during the site visit to Iron Mountain, it was discovered Iron Mountain personnel had copies of the keys to unlock NARA's containers.

Office of Management and Budget Memorandum 06-16, "Protection of Sensitive Agency Information," June 23, 2006, included specific actions agencies were to take to properly safeguard PII when physically transported outside the agency's secured, physical perimeter. For example, in those instances where PII is transported to a remote site or stored at a remote site, agencies were to implement NIST SP 800-53 security controls ensuring information is transported or stored only in encrypted form. NARA 1608, "Protection of Personally Identifiable Information," August 6, 2009, also requires PII data transported on removable media to be encrypted unless encryption will impact the integrity of the data. In those instances, appropriate access controls, strong authentication procedures, or other security controls commensurate with the sensitivity of the PII data must be used.

In February 2013, NARA officials responded to a potential PII concern regarding backup media at one of NARA's St. Louis facilities. Three boxes of backup tapes, CDs, floppy discs, a Compact Flash card, and related material were abandoned for about a month on the loading dock at the St. Louis facility[5]. The backup media included CMRS backups

[5] According to NARA officials, the date of this incident closely corresponds to the period during which St. Louis NITTSS staff were completing their final pack up of IT and communication hardware at the old Page Ave facility.

which contain sensitive PII about veterans. Even though data stored on the backup media is not manually readable, compatible tape backup hardware and software are still generally available and could be attached to a server or workstation if an individual was intent on reading the tape cartridges. NARA officials determined information was not compromised in this instance since the loading dock is a secure area. However, if NARA encrypted the backup tapes, the probability of unauthorized disclosure of PII would be reduced in the event tapes were lost or stolen.

The Terms and Conditions listed in the Performance Work Statement for the CMRS support contract state removable media, such as hard drives, flash drives, devices with flash memory, CDs and floppy disks containing sensitive PII shall not be removed from a Government facility unless they are encrypted using a NIST FIPS 140-2 or successor approved product. According to the CMRS contractor responsible for backups, it would not be possible to encrypt the backups because encryption would significantly increase the processing times needed to run backups. The CIO should determine whether hardware or software encryption can be used to protect CMRS backup tapes that are currently transported and stored offsite or devise another method of protecting the data that provides a similar level or security.

Integrity of Backup Data

It is important to ensure the data backup copies have the same content as the original data file. One way to check the integrity of the backup data is to calculate a checksum[6] for both the original and the backup copy and then compare. Another way to check the integrity of the backup file is to periodically retrieve the backup file, open it on a separate system, and compare the backup copy to the original file.

According to NIST SP 800-34, backup tapes should be tested regularly to ensure data is being stored correctly and files may be retrieved without errors or lost data. Also, backup tapes should be tested at the alternate site, if applicable, to ensure the site supports the same backup configuration the organization has implemented. NARA does not regularly perform tests to restore files stored on backup tapes. None of the three contractors supporting NARA systems regularly tested backup tapes by trying to restore data. Two contractors provided examples of file restores they had performed however, it was not done on a regular basis and did not involve restoring data from backup tapes.

The NITTSS contract requires the contractor ensure, and demonstrate at NARA's request, that NARA IT systems are recoverable from backup tapes. NITTSS periodically

[6] A checksum is a small-size datum computed from an arbitrary block of digital data for the purpose of detecting errors that may have been introduced during its transmission or storage. The integrity of the data can be checked at any later time by recomputing the checksum and comparing it with the stored one. If the checksums match, the data was likely not accidentally altered.

performed file restores based on user requests. However, NARA cannot rely on this process to ensure all system are recoverable from backup tapes since there is no guarantee all systems would be tested. According to the IT Operations manager, she is confident with the backup operations for Novell Groupwise because of all the restores they have performed at user's requests. However, for minor application systems she did not have the same confidence level since those system backups may not be tested or validated to ensure the backup was successful.

The ERA contract requires the contractor, on a scheduled basis, to have tested processes and procedures for the recovery and reconstitution of ERA systems and services to the state prior to the disruption or failure. According to an ERA System Administrator, he was able to restore files using the Backup, Archives, and Restore functionality within the backup software. The System Administrator stated there was not a process in place to periodically test backups on a regular basis. He estimated the last data restore he performed was for an audit last year.

The CMRS contract does not include a requirement for periodic testing of backup data. According to the contractor, he performed file restores for two other systems he maintains at NARA but has not had to perform any real-time data restores for CMRS. According to the CMRS contractor, he tested the recovery of files every three months. Documentation from the last restore in December 2012 consisted of an email from the backup software stating the restore of a file onto a client directory had succeeded. The contractor noted this testing was not required, but he would perform the tests to ensure the backups were able to be restored.

For high impact systems[7] such as CMRS[8] and ERA, the annual contingency plan test should include the use of a sample of backup information in the restoration of selected information systems. Annual contingency plan testing at NARA did not include a test to restore files from backups. A test of the contingency plan was not conducted for CMRS during FY 2012 and the ERA contingency plan test involved only tabletop exercises.

The results of the ERA contingency plan test identified areas for improvement in ERA's ability to respond to an incident. For example, the summary of the test results identified the lack of formalized Backup and Recovery testing and that currently there is no process or method to verify NetApp snapshot backups are working. One recommendation made

[7] FIPS Publication 199 defines three levels of potential impact (low, medium, and high) on organizations or individuals should there be a loss of confidentiality, integrity, or availability. The potential impact is considered High if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

[8] The CMRS Contingency Plan dated December 27, 2012 categorizes the system as a High impact for confidentiality, integrity, and availability but the CMRS System Security Plan, dated July 23, 2012, categorizes the system as Moderate impact.

in the test results was for subsequent exercises to focus on the restoration of systems. NARA should regularly test data backups to ensure the information being backed up is stored correctly and can be retrieved if needed.

Availability of Backup Data

Maintaining the availability of backup data is important to ensure access to the backup information if needed. One way to protect the availability of backup data is to store the backup copy offsite to prevent a disaster from destroying the original file and the backup file. As shown in Table 1. below, NARA maintains three offsite storage locations.

Table 1. Offsite Storage Locations for Data Backups

Offsite Storage Locations	Backup Media	Systems/Servers
Iron Mountain, Columbia, MD	LTO Tapes, DLT Tapes, Compact Flash Cards	NITTSS Enterprise backups, CMRS backups, and other systems with locally attached tape drives
Allegany Ballistics Laboratory, Rocket Center, WV	Mirrored/Replicated to NetApp and then to tape	Novell file and print, Novell Groupwise
Archives II, College Park, MD	LTO Tapes	ERA

The NITTSS Tape Administrator was responsible for rotating backup media offsite to Iron Mountain each week. The schedule with Iron Mountain was for pickup and delivery of tapes to occur on Wednesdays. The NITTSS procedure specifies full backups are stored onsite for one week and then sent offsite for eight weeks. The Tape Administrator maintained a tape log documenting the backup tapes sent offsite, the date they were sent offsite, and their return date. However, when we compared the NITTSS tape logs to the Iron Mountain records; we found that while media was consistently returned by Iron Mountain each Wednesday, media was not actually being sent to Iron Mountain each week. Instead, during calendar year 2012, media was rotated offsite about once a month. Therefore, NARA systems were at risk of losing up to four weeks of data if a disaster had impacted the AII datacenter destroying the original system data and the backup tapes. For some systems, such as CMRS, losing four weeks of data would be extremely disruptive to the operations at the National Personnel Records Center and to military veterans who had submitted record requests during that time. Table 2. shows the dates backups were transferred to Iron Mountain during 2012.

Table 2. Number of Containers Sent to Iron Mountain Each Week in 2012

Date	Number of Containers	Date	Number of Containers
1/4/12	None	7/4/12	None
1/11/12	None	7/11/12	None
1/18/12	5	7/18/12	None
1/25/12	None	7/25/12	None
2/1/12	None	8/1/12	5
2/8/12	None	8/8/12	None
2/15/12	4	8/15/12	None
2/22/12	None	8/22/12	None
2/29/12	None	8/29/12	2
3/7/12	None	9/5/12	2
3/14/12	5	9/12/12	None
3/21/12	None	9/19/12	None
3/28/12	None	9/26/12	None
4/4/12	None	10/3/12	4
4/11/12	4	10/10/12	None
4/18/12	None	10/17/12	5
4/25/12	None	10/24/12	None
5/2/12	None	10/31/12	None
5/9/12	4	11/7/12	None
5/16/12	None	11/14/12	None
5/23/12	None	11/21/12	4
5/30/12	None	11/28/12	None
6/6/12	4	12/5/12	None
6/13/12	None	12/12/12	4
6/20/12	None	12/19/12	None
6/27/12	4	12/26/12	None

According to the Tape Administrator, tapes did not always get to him in time to be included in the weekly shipment so he would delay sending that week's container offsite until he received the backup tapes scheduled to be in the shipment. However, we noted that even when containers were not sent offsite for several weeks, those containers did not include backup tapes for every system. The NARA Technical Monitor responsible for overseeing this area of the NITTSS contract was not aware backup tapes were not being sent offsite each week. Additional oversight processes should be implemented to ensure backups are sent offsite each week as scheduled.

The OIG and the NITTSS Technical Monitor visited the Iron Mountain offsite storage location in January 2013 to review the contents of each container currently stored there and compare the contents of the containers with the Tape Administrator's tape log. Of

the seven containers[9] we reviewed, four of the containers matched the Tape Administrator's log. The remaining three containers either had tapes included in the container not recorded on the log or the container did not include all the tapes shown on the log. As shown in Table 3 below, none of the seven containers included a complete set of backup tapes.

Table 3. Inventory of Offsite Storage Containers at Iron Mountain

System:	28-Nov	5-Dec	12-Dec	19-Dec	26-Dec	2-Jan	9-Jan
OFAS	2	2	2	-	-	-	-
CMTS	-	-	-	-	1	-	-
VISTA	-	-	-	-	1	-	-
RCPBS	2	4	-	-	-	2	2
APS	1	1	1	-	1	-	-
AERIC	1	-	-	-	1	-	1
A1-PBX	1	1	1	1	-	1	1
A2-PBX	1	1	1	1	-	-	1
VAULT	-	5	4	6	4	-	-
NISP	6	7	6	8	6	3	5
Total Sent Offsite:	**14**	**21**	**15**	**16**	**14**	**6**	**10**

We contacted the Order Fulfillment and Accounting System (OFAS) Project Manager to ask why backup tapes were not included in the offsite containers between December 19, 2012 and January 9, 2013. According to the Project Manager, the system is managed by their own contractor who backs up the tapes locally. The Project Manager stated backup tapes were not sent offsite during that time period because the system had exceeded the storage limit for the backup tapes and more backup tapes had to be ordered. The system was being backed up onto two backup tapes. However, the system exceeded the storage limit on those two tapes and a third tape was needed for each backup. Additional tapes were ordered but backups could not resume until those tapes were received and placed into the rotation.

The process of providing tapes to the Tape Administrator should be improved to prevent lost or misplaced tapes. We found inconsistencies between the CMRS contractors tape log used to record backup tapes given to the Tape Administrator each week for offsite storage and the Tape Administrator's log. According to the CMRS contractor, the process for transferring tapes offsite was to place the backup tapes on the Tape Administrator's desk. During this process, the contractor stated that many times when dropping off the weekly tapes, the tapes from the previous week's backup were still on

[9] There were only seven containers at Iron Mountain the date of the site visit because our visit occurred on a Wednesday therefore one of NARA's containers was already out for delivery back to NARA.

the Tape Administrator's desk. Because the containers were not rotated offsite each week, tapes may have been mixed up or placed into the wrong containers. The NITTSS Technical Monitor agreed additional oversight was needed over the process of sending tapes offsite. NARA should ensure an accurate log or record of tapes going offsite is maintained so the correct container can be recalled if needed.

Offsite Storage Location

According to NIST SP 800-34, it is good business practice to store backup data offsite. Commercial data storage facilities are specially designed to archive media and protect data from threatening elements. When selecting an offsite storage facility and vendor, one of the criteria to be considered is the distance from the organization and the probability of the storage site being affected by the same disaster as the organization's primary site.

One of NARA's offsite locations for backup tapes is in Columbia, Maryland. This is the offsite storage location for systems and servers located in the Archives II datacenter which is approximately 15 miles from Columbia. Due to its close proximity, the offsite facility could be affected by the same area-wide disasters such as hurricane, tornado, or other severe weather. Although the offsite facility has environmental controls in place to protect the backup tapes, access to the facility may not be possible to retrieve the backup tapes. We attempted to find out why the Columbia facility was chosen as the location for offsite backup tapes but the decision appears to have been made over 10 years ago and several individuals we asked did not know the rationale behind the decision. NARA should evaluate the risks involved with storing backup tapes in the same geographic area as NARA's main data center. One option for NARA to consider is whether backup tapes could be stored at ABL, which is the NARA Continuity of Operations (COOP) site, or at a storage facility closer to the COOP site.

Information System Backup Control

NARA did not fully implement the NIST SP 800-53 control for information system backups. Specifically, NARA did not have controls in place to protect the confidentiality, integrity, and availability of backup information and did not regularly test backup information to verify media reliability and information integrity. Although NARA's IT Security Requirements include this control, it was not being enforced. In addition, NARA did not have mechanisms in place to ensure this control was working.

Organizations are required to adequately mitigate the risk arising from the use of information and information systems in the execution of mission and business processes. Contingency strategies are created to mitigate the risks for the contingency planning family of controls and cover the full range of backup, recovery, contingency planning,

testing, and ongoing maintenance. NIST SP 800-53 Contingency Planning Control CP-9 Information System Backup requires organizations to conduct backups of user-level and system-level data and to protect the confidentiality, integrity, and availability[10] of backup information at the storage location.

The supplemental guidance for control CP-9 clarifies system-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures[11] and cryptographic hashes[12] are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organization assessment of risk guides the use of encryption for protecting backup information.

NIST SP 800-53 also includes control enhancements for moderate and high baseline systems. For example, those systems categorized as moderate and high-impact level are required to test backup information at an organization-defined frequency to verify media reliability and information integrity. Systems categorized as high-impact level also must:

- use a sample of backup information in the restoration of selected information system functions as part of contingency plan testing;
- store backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational system; and
- transfer information system backup information to the alternate storage site at organization-defined time period and transfer rate.[13]

Additional controls that can be implemented, but are not required, include: the organization accomplishes information system backup by maintaining a redundant secondary system, not collocated, that can be activated without loss of information or disruption to the operation; and the organization enforces dual authorization for the deletion or destruction of organization-defined backup information.

[10] NIST SP 800-53, Revision 4, issued April 2013, included a change to the CP-9.d control. Specifically, CP-9.d was revised to require that organizations protect the availability of backup information at storage locations in addition to the confidentiality and integrity.
[11] A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe the message was not altered in transit.
[12] A cryptographic hash function is an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value, such that any accidental or intentional change to the data will (with very high probability) change the hash value.
[13] This is a new requirement for high-impact systems based on NIST SP 800-53, Revision 4.

Data Backup and Recovery Procedures

According to GAO, there are a number of steps an entity should take to prevent or minimize the damage to automated operations occurring from unexpected events. Implementing thorough backup procedures is generally an inexpensive way to prevent relatively minor problems from becoming costly disasters. We reviewed the data backup and recovery procedures provided by NITTSS for the systems they manage, and by the ERA support contractor. These procedures included roles and responsibilities, the frequency and scope of the backups and where the backups will be stored.

We were unable to review backup and recovery procedures for CMRS because the contractor was in the process of drafting the data backup procedures based on the redesign of the system. The CMRS Technical Monitor provided a copy of the CMRS Contingency Plan which she believed gave an overview of the CMRS backup function. Although the Contingency Plan did have an overview, it did not specify responsibility for the backups or the minimum frequency and scope of the backups. Without thorough backup and recovery procedures, NARA does not have a documented process for restoring CMRS data after a data loss event.

Conclusion

Information systems are vital elements in most mission/business processes. Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency Planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. The adequate protection of the confidentiality, integrity, and availability of the backups is important to ensure NARA information is not at risk of unauthorized disclosure and data is able to be recovered in usable form if needed.

Recommendations

1. The CIO should create a full backup of the EOP instance of ERA as soon as the upgrade and data migration is complete.

2. The CIO should encrypt backup tapes containing sensitive PII or devise another method of protecting the data that provides a similar level of security.

3. The CIO should include the restoration of files from backups as part of the annual contingency plan testing for at least high impact systems such as ERA and CMRS.

4. The CIO should develop a process to regularly test data backups to verify information integrity.

5. The CIO should develop increased oversight procedures for the process of sending backup media offsite to ensure media is rotated offsite as prescribed.

6. The CIO should evaluate the risks associated with storing backup tapes within the same geographic area as AII and determine whether the current strategy is sufficient.

7. The CIO should create or update Backup and Recovery Plans and Procedures for the Case Management and Reporting System.

Management Response

Management concurred with the recommendations.

2. Opportunities Exist to Reduce the Cost of Offsite Storage.

The audit identified cost savings related to excess Iron Mountain storage containers in NARA's possession. NARA has 90 Iron Mountain containers but only 17 of the containers have been used in the last year, with some containers having not been used in over seven years. This occurred because NARA's requirements for offsite storage changed but excess containers were not returned. In addition, the monthly invoices were paid with the government credit card without a sufficient review. As a result, NARA has spent about $31,900 over the last seven years that could have been put to better use.

Iron Mountain monthly invoices include two types of charges, transportation charges for pickup and return of backup tapes and set fees for storage containers. According to the invoices, NARA paid monthly charges for 90 storage containers. The Iron Mountain monthly invoices are usually around $1,000 which includes on average $100 for transportation charges and a recurring charge of $867 for the 90 containers (see Table 4).

Table 4. Monthly Cost for Iron Mountain Containers

Container Type	Quantity	Unit Price	Monthly Amount
DLT Container (capacity = 20)	51	$8.48	$432.48
DLT Container (capacity=10)	2	8.48	16.96
Cartridge 3480 (capacity=40)	2	10.47	20.94
IM Multi Media	27	8.48	228.96
Pendaflex	8	20.95	167.60
Total			$866.94

We found that of the 90 containers assigned to NARA, only 17 containers had been used in the last year. Some of the remaining containers had not been used in several years, including one container NARA received in 2005 that had never been stored at Iron Mountain. According to NARA's Account Manager at Iron Mountain, the cost for the container is the same whether the container is stored at Iron Mountain or at NARA. The Account Manager stated if there are containers sitting at NARA not in use, Iron Mountain can take them back. The Tape Administrator counted 48 containers located in the Tape Storage Room at Archives II. These containers had old backup tapes stored in them that were waiting to be disposed of. The Tape Administrator and the NITTSS Technical Monitor were unsure of where the remaining storage containers were located. The NITTSS Technical Monitor stated additional containers may be stored out at NARA field offices.

We identified five containers stored at Iron Mountain with a permanent retention date. In reviewing the contents of three of the permanent hold containers it was unclear as to whether these containers continued to require storage at Iron Mountain indefinitely. For example, one container held only one backup tape labeled with the year 2003. Another container held old server backups that may have been from 2004.

NARA had excess Iron Mountain containers because NARA's requirements for offsite storage changed in the last couple of years, but containers were not returned to Iron Mountain. For example, in March 2010, NARA transferred 31 containers offsite, sending about six containers offsite each week. Currently, NARA sends only four or five containers a month to Iron Mountain.

The review and approval process for payment of the Iron Mountain invoice did not include a review of the containers assigned to NARA's account. Iron Mountain invoices were paid using the government credit card. The approval process for payment was to create a Form 5007 Requisition based on the invoice which was given to an IT Operations official to sign. According to the IT Operations official, as long as the monthly charge remained consistent, she would approve the invoice for payment. However, if there were additional transportation charges for an unscheduled delivery she would discuss the extra charge with the Tape Administrator to find out why it was needed before paying the invoice. This review was not sufficient to identify the unnecessary costs NARA continues to pay for extra storage containers not in use.

Using the monthly fee for each of the storage containers and the number of months since the container was last used, we calculated the approximate amount of funds put to better

use as $31,900. If NARA returns the excess containers to Iron Mountain it could save approximately $708 each month, or $8,500 annually.

Recommendations

8. The CIO should review the current list of Iron Mountain containers assigned to NARA and return those containers that are no longer needed.

9. The CIO should examine the contents of those containers marked as permanent and determine whether permanent storage is still required.

Management Response

Management concurred with the recommendations.

3. Payment of Offsite Storage Costs Needs Further Review

During FY 2012, NARA paid $12,178 for offsite storage of backup tapes. We identified three issues with the payment of offsite storage costs:

1) the payment appears to be a split purchase;

2) costs incurred for services in one fiscal year were paid for using funds from the following fiscal year; and

3) payment for offsite storage costs may have been improper.

These issues occurred because NARA paid for these services with a government credit card instead of going through the procurement process and awarding a contract for offsite storage. In addition, based on the language in the NITTSS Request for Quote (RFQ) it could be reasonably interpreted that NITTSS was responsible for offsite storage costs. As a result, NARA's procurement process as well as Federal laws and regulations may have been violated. In addition, NARA has paid approximately $48,712 over the last four years that could have been put to better use.

According to NARA's Purchase Card Guide, split purchasing is the acquisition of a requirement by dividing it into smaller components thereby avoiding the established FAR and NARA procurement procedures for the elevated dollar thresholds. The Purchase Card Guide defines two types of split purchases: breaking down a one-time requirement

with a value greater than the single purchase limit[14] so the acquisition can be made using the purchase card; and using the purchase card to purchase a recurring requirement with a fiscal year value greater than the single purchase limit. The cost for offsite storage appears to meet the definition of a split purchase since the aggregate amount of this recurring monthly requirement was $12,178 for FY 2012 which exceeded the single purchase limit.

Although there are exceptions where this would be allowable, we were unable to find documentation that a contract was in place and an exception had been granted to allow payment of the contract to occur using the government credit card.

According to 31 United States Code (USC) 1502(a), the balance of an appropriation or fund limited for obligation to a definite period is available only for payment of expenses properly incurred during the period of availability or to complete contracts properly made within that period of availability. Further, the appropriation or fund is not available for expenditure for a period beyond the period otherwise authorized by law.

Iron Mountain invoices bill for the current month's service and are due in full within 90 days of the invoice date. According to the credit card holder, she usually pays the bill in the month it is due. For example, NARA received two invoices dated August 31, 2012 for costs incurred during August 2012. Although these costs were incurred during FY 2012, the amount appeared on the December 3, 2012 credit card statement. According to data from NARA's financial system, part of the cost for services rendered in August 2012 was paid for using FY 2013 appropriated funds[15]. We identified six months in which services from one fiscal year were paid for with funds from a different fiscal year.

The RFQ for the NITTSS contract states that the contractor shall manage NARA's off-site media storage. In addition, the RFQ states "the contractor shall store all backup media off-site, track all backup media, create off-site storage records and logs, and provide the records and logs to the government." Based on this language, it could be reasonably interpreted that the NITTSS contractor was responsible for the cost of storing backup tapes offsite. In FY 2012, NARA paid $12,178 for offsite storage costs. The NITTSS contractor began their work at NARA on April 1, 2009, therefore, NITTSS may have been responsible for offsite storage costs for the last four years. Using the cost paid in FY 2012 as an estimate, we calculated the approximate amount of funds put to better use as $48,712 over the last four years.

[14] The single purchase limit (also known as the micro-purchase limit) is a dollar amount of the procurement authority delegated to the cardholder. The single purchase limit is $3,000.
[15] The costs for offsite storage are split between two different funds. For most of the months we reviewed, 67% of the cost was paid for with appropriated funds and 33% was paid for with revolving funds.

Recommendations

10. The CIO, the Director of Acquisition Services, and NARA's Office of General Counsel should review purchases made for offsite storage costs to determine whether NARA's procurement process and Federal appropriations laws were violated and if so, take appropriate corrective action.

11. The CIO, the Director of Acquisition Services, and NARA's Office of General Counsel should review language in the NITTSS contract and determine whether payments NARA made for offsite storage were proper, and what, if any, remedies are available.

Management Response

Management concurred with the recommendations.

Appendix A – Acronyms and Abbreviations

ABL	Allegany Ballistics Laboratory
AII	Archives II
CIO	Chief Information Officer
CMRS	Case Management and Reporting System
COOP	Continuity of Operations Plan
EOP	Executive Office of the President
ERA	Electronic Records Archives
GAO	Government Accountability Office
IT	Information Technology
LTO	Linear Tape-Open
NARA	National Archives and Records Administration
NARANet	NARA Network
NISP	NARA Integrated Siebel Platform
NIST SP	National Institute of Standards and Technology Special Publication
NITTSS	NARA Information Technology and Telephone Support Services
OFAS	Order Fulfillment and Accounting System
PII	Personally Identifiable Information
PWS	Performance Work Statement
RFQ	Request for Quote
SLES	SUSE Linux Enterprise Server
USC	United States Code

Appendix B - Management's Response to the Report

NATIONAL ARCHIVES

Date: JUN 27 2013

To: James Springs, Acting Inspector General

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

Subject: OIG Revised Draft Audit 13-09, Audit of NARA's Data Backup Operations

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

We concur with the eleven recommendations in this audit.

If you have any questions or need additional information on these comments, please contact Mary Drak by phone at 301-837-1668 or via email at mary.drak@nara.gov.

David S. Ferriero
Archivist of the United States

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

Appendix C - Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Chief Operating Officer
General Counsel
Executive for Business Support Services
Executive for Information Services/Chief Information Officer
Performance and Accountability