NATIONAL ARCHIVES

OFFICE *of* INSPECTOR GENERAL

Date : January 30, 2012

Reply to Attn of : Office of Inspector General (OIG)

Subject : Advisory Report No. 12-04, Inadequate Contingency Planning Continues to be a Significant Risk for the Electronic Records Archives System

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

The purpose of this Advisory Report is to inform you of a situation that could adversely impact the National Archives and Records Administration's (NARA's) ability to meet its mission should the Electronic Records Archives (ERA) System's primary site be unavailable for an extended time period. As part of our effort, to provide audit coverage to NARA's ERA program, we followed up on the status of two issues: 1) system backups and 2) an alternative backup site, which we previously reported on in Advisory Report No. 10-11 entitled, "Inadequate Contingency Planning for the Electronic Records Archives System" dated April 29, 2010. We found these issues have not been adequately addressed: (1) it is still unknown if the ERA System (in its entirety) can be successfully restored from backup tapes and (2) there is not an alternative backup site.

The ERA System represents the largest information technology project ever undertaken by NARA. The ERA System is being developed to fulfill NARA's mission in the digital age: to safeguard and preserve the records of our government, ensure that the people can discover, use, and learn from this documentary heritage, and ensure continuing access to the essential documentation of the rights of American citizens and the actions of their government. In addition, the use of ERA will be mandatory for all Federal agencies in 2012. Without adequate contingency planning, ERA officials continue to lack assurance the ERA System can be successfully restored at an alternative location should its primary site be unavailable. Such a significant risk severely limits the reliability of the system.

Information technology (IT) systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire) from a variety of sources such as natural disasters to terrorists actions. Contingency planning refers to interim measures to recover IT services following an emergency or system

disruption. Interim measures may include the relocation of IT systems and operations to an alternative site, the recovery of IT functions using alternative equipment, or the performance of IT functions using manual methods.

The National Institute of Standards and Technology Special Publication 800-34 entitled "Contingency Planning Guide for Federal Information Systems" Revision 1 dated May 2010 states that backup and recovery methods and strategies are a means to restore system operations quickly and effectively following a service disruption. Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. The Federal Information Processing Standards Publication (FIPS PUB) 199, "Standards for Security Categorization of Federal Information and Information Systems" is used to rank as High, Moderate, or Low a system's: Confidentiality, Integrity, and Availability. FIPS Categorization is determined by the adverse effect that a security event could have on the system, and how it impacts the confidentiality, integrity, and availability, of the system. The ERA System's FIPS Categorization for Availability is Moderate which means that a prolonged discontinuance of service would result in an impact to mission requirements. The FIPS 199 Recovery Strategy for a system with an impact level of Moderate for Availability is to have a Cold or Warm Backup site.[1] Thus, the contingency plan for all FIPS 199 moderate or high impact systems should include a strategy to recover and perform system operations at an alternate facility for an extended period.

Backups

The current method of protecting the ERA System from a disaster is done by the storage of backup tapes at Archives II in College Park, MD. Incremental backups of data are done daily at the ERA System's primary location, the Allegany Ballistics Lab (ABL) in Rocket Center, West Virginia. Our concern, has been, and continues to be the ERA System, in its entirety, has still not been restored from backup tapes. Without adequate testing, it is still unknown if the ERA System can be restored in a timely manner from backup tapes. An ERA official acknowledged that although restoration from tape for the ERA System has not been demonstrated in its entirety, restoration of selected subsets of ERA business objects and records has been successfully accomplished. However, restoration of selected subsets of the ERA System does not provide us with an adequate level of confidence that the system, in its entirety, could be successfully restored in a timely manner should a disaster occur.

Additionally, in our April 2010 report we noted that of particular concern to ERA officials was the restoration of the Executive Office of the President (EOP) data archive from tape. The EOP data archive is mirrored to an onsite replicated archive. Program officials felt the EOP data could be recovered from the replica, but had serious concerns about the ability to restore the EOP

[1] Cold sites are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities. Warm sites are partially equipped office spaces that contain some or all of the systems hardware, software, telecommunications and power sources.

data archive from tape if the replica was not available. An ERA official indicated to us that it still has not been demonstrated the EOP data archive can be successfully restored from tape. Further, due to a software upgrade, the EOP production system and the replica were out of sync for about six months. A project has been initiated to upgrade EOP's Hitachi Content Platform infrastructure which introduces fail over capabilities between the production and replica archives. ERA management feels this will eventually allow them to position the EOP replica at an alternative operations site. We suggest the ERA Program Office conduct adequate testing to determine if the ERA System (in its entirety) can successfully be restored from backup tapes in a timely manner.

Alternative Backup Site

Currently, there is no alternative ERA backup site or an official Disaster Recovery Plan for the ERA System. In the event of a disaster that renders the current ERA production data center (i.e., ABL) unusable, NARA does not have an alternative processing site to continue ERA operations. NARA would need to acquire the funding to purchase replacement hardware, obtain data center space to house the new equipment and have the offsite tapes sent to the new location to begin restoration of the system. The ERA Contingency Plan dated August 9, 2011 states under a major system failure; an alternative processing site is utilized. The plan also states detailed information on the roles and responsibilities, support structure, line of succession, and procedures for a major system failure are documented in Contract Data Requirements List (CDRL) number 88 (Disaster Recovery Plan). However, CDRL number 88 was removed as a deliverable from the development contract in June 2011. A senior ERA Program Official stated that instead of a backup site, we are storing backup disks at Archives II. Although we agree that backing the system up and storing the tapes offsite is an important and necessary control for disaster recovery, we do not think it should be in lieu of an alternative backup site. The ERA System's FIPS Categorization for Availability is Moderate which means that a prolonged discontinuance of service would result in an impact to mission requirements. The FIPS 199 Recovery Strategy for a system with an impact level of Moderate for Availability is to have a Cold or Warm Backup site.

The Memorandum of Understanding (MOU) between NARA and Naval Sea Systems Command for space at the ABL states that either party may terminate the MOU by providing written notice, and the disposition of property and transition of personnel must be completed within 365 days. When an ERA official was asked if the Navy decided to terminate the MOU, could the ERA System be relocated to a new location and brought up within a year, she responded it has been estimated that the project to locate and acquire alternative space, provision the new space, fit-up and validate the new environment, and decommission the existing environment could be successfully completed within 365 days. However, she noted this timeline would be contingent upon several external factors including the acquisition lifecycle and the availability of funding for the work. Without adequate planning, and under the current budget environment, it may be very difficult to accomplish this type of move within the time constraints of the MOU, should the Navy decide to terminate this agreement.

The ERA System Security Plan states no alternative processing site has been implemented. The current ERA BIA and ERA Contingency Plan both address a primary site unavailability scenario by utilizing the existing NARA legacy applications: Archival Preservation System (APS), Accessions Management Information System (AMIS), and the Archival Electronic Records Inspection and Control System (AERIC). In the event of unavailability of the ERA System at Rocket Center, these plans call for customers to continue their business functions by using these legacy systems which are currently in place at Archives II, and which are running parallel operations. However, ERA's Business Case Analysis identified these three legacy systems, as well as the Access to Archival Databases System, as four systems that will be replaced by ERA because, individually and collectively, they are not adequate to NARA's mission needs, their designs cannot be accommodated into the NARA Target Architecture, and/or they automate certain processes that will no longer be necessary.

The Security Plan also states there is no alternative processing site in place and NARA accepts the risk. When asked what the basis for making this statement was, a senior ERA official stated this weakness has been identified in a Plan of Action and Milestones (POA&M). The planned corrective action in the POA&M is for NARA to designate and procure alternative operating facilities as part of their Continuity of Operations Plan (COOP) in support of the ERA System. However, this POA&M has been closed without implementing the corrective action. A comment field in the POA&M states to record (this weakness) as a risk within the System Security Plan without implementation. An ERA Official commented the risk is not "Accepted" by NARA and that it is an active risk documented in the Systems Security Plan. This official went on to say the ERA Program is not building a duplicate ERA site, so the only alternative for security is to document how ERA would operate if the ABL site was lost. In our opinion, the reliance on legacy systems is not an adequate control and does not comply with FIPS for a system that is critical to NARA's mission and that will be mandatory for use by all Federal agencies next year. We suggest the ERA Program Office conduct an analysis of risks and alternatives to determine the level of risk management is willing to accept and the most cost effective alternative to meeting NARA's mission if the ABL was unavailable for an extended time period.

Our review effort consisted primarily of reviewing applicable ERA documentation such as the ERA Core Infrastructure System Security Plan, ERA Contingency Plan, ERA Continuity of Operations Plan, ERA Business Case Analysis, and the ERA Business Impact Analysis; and interviews with responsible ERA Program Office officials.

As with all OIG products, we will determine what information is publically posted on our website from this report. Should you or management have any redaction suggestions based on FOIA exemptions, please submit them to my counsel within one week from the date of this letter. Should we receive no response from you or management by this timeframe, we will interpret that as confirmation NARA does not desire any redactions to the posted report.

Should you have any questions concerning the information presented in this Advisory Report, or there are other areas of the ERA Program that you would like for us to review, please do not hesitate to contact me or James Springs, Assistant Inspector General for Audits at (301) 837-3000.

Paul Brachfeld
INSPECTOR GENERAL

cc: Michael Wash, Chief Information Officer