

Checklist for Securing Electronic Records for Agencies Undergoing Reorganizations or Other Major Changes

Federal records are evidence of the decisions and actions of an organization. Records must be secured and preserved, and may only be disposed of in accordance with a NARA-approved records schedule, as required by the Federal Records Act ("FRA") ([44 U.S.C. Chapters 21, 29, 31, and 33](#)). Agencies' record keeping obligations continue, even as they discontinue some or most of their functions.

Agencies largely create and store electronic records using cloud, on-premises, or hybrid storage. To ensure that your records are maintained during reorganizations or other major changes, you need to gather information on where your records are stored. It is critical to make sure the records are fully captured. Below are a series of questions that will help you safeguard the records documenting decisions and protecting rights and interests.

Questions for Securing Electronic Records

Coordinate with your general counsel, procurement, and IT offices to answer the questions below for records in cloud and on-premise storage. This information will help you develop an action plan that ensures records are maintained until they can be exported to a secure system, deleted, or transferred to NARA.

Cloud Storage

- What cloud enterprise agreement(s) do you have in place for cloud storage? Which providers?
- When does your cloud service current fiscal year contract conclude? Where are you in the enterprise agreement cycle? For example in year 2 of 5.
- What options are available for you to extend your storage?
- Does your cloud contract include language concerning the closeout of the contract?
- How long does the provider retain your records if the agency interrupts the contract?
- What kind of contractor services are allowed under your cloud contract? For example, migration to a new provider or export of records.
- What are the costs associated with moving records from the cloud to another cloud or on premise? Are there limitations on how and when this can be done?
- Are you creating and maintaining records with other agencies with an interagency agreement? Is it clear who has responsibility if one of the other agencies isn't able to maintain the contact?

On-premise Storage

- What system documentation do you have in place?
- Where are the servers located? Do you have ongoing access to the facility?
- What contractors support your infrastructure?
- Do you need to maintain any contracts to keep up infrastructure?

Helpful: Backup or COOP Plans

It may be helpful to reference your agency's backup processes or continuity of operations plan (COOP). Documentation for backup processes often includes a list of systems that are being backed up. COOP material often includes information about IT systems and records required during an emergency. Your agency's point of contact for COOP will have information on operations for essential records.