

Abridged Checklist for Securing Federal Entity Records in Draw-Down

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. Chapter 31](#) and [36 CFR § 1231](#)).

- **Agencies’ record keeping obligations continue, even as they discontinue some or most of their functions.** As long as any portion of your federal entity is still in operation, that entity is legally responsible for its records.
- **Agencies must assign responsibility for ongoing records management and access** (including FOIA, legal, and Congressional), maintenance, and safeguarding of their records to a person who can perform these functions.

NARA has prepared this checklist to help federal entities prepare for large-scale changes.

Identify Where Your Records are Stored

Coordinate with your general counsel, procurement, and IT offices to answer the below questions.

Cloud Storage

Identify the cloud enterprise agreement(s) you have in place for cloud storage.

- Which provider and cloud are your records in?
- When does your cloud service current fiscal year contract conclude? What options are available for you to extend your storage?
- How long does the provider retain your records if the agency interrupts the contract?
- 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?

Paper Records Transferred to Inactive Storage

- For temporary scheduled records, ensure proper documentation of transfer as outlined in [36 CFR §1232.16](#).
- For unscheduled and permanent records, request authority from NARA to transfer to a records storage facility by contacting NARA at rm.communications@nara.gov. ([36 CFR §1232.14](#) and [§1232.16](#) describes what the request must include.)

On-premise Electronic 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?

Triage Actions

Determine if records can securely remain where they are:

- If so, maintain and monitor. If not:
 - Move digital records to sustainable and accessible electronic storage.
 - Pack physical records in FRC boxes and move to a secure location.
- Determine if records for scaled back, devolved, or ceased functions should be transferred to another federal entity.
- Determine if records can be destroyed or transferred to NARA.

Classified, Legal, and Access Considerations:

There are considerations in addition to disposition timeframes in the records schedules that must also be addressed:

- Legal holds must continue - records may not be destroyed and must remain accessible.
- Proper handling and control of classified and sensitive information must continue.