



NATIONAL
ARCHIVES

OFFICE *of the*
CHIEF RECORDS
OFFICER

Unauthorized Disposition Safeguards

Records Management Assessment Report

National Archives and Records Administration
April 4, 2024

UNAUTHORIZED DISPOSITION SAFEGUARDS ASSESSMENT

INTRODUCTION

The National Archives and Records Administration (NARA), based on authority granted by [44 United States Code \(USC\) 2904\(c\)](#) is responsible for conducting inspections, surveys, studies, or assessments of records and record management (RM) programs across the federal government to ensure the proper management of records in all media to protect rights, assure government accountability, and preserve and make available records of enduring value.

A records management assessment is a multi-agency evaluation of a specific topic, issue, or activity that can impact records and RM processes, procedures, or policies. The purpose of conducting an assessment is to determine the efficacy of business practices and policies. Additionally, NARA seeks to identify and understand agency successes and challenges related to RM and share findings, recommendations, and best practices throughout the federal RM community.

In the fourth quarter of fiscal year (FY) 2023, NARA conducted an assessment of seven agencies' policies, practices, and procedures associated with incidents of unauthorized disposition (UD) of agency records and the development and implementation of safeguards for certain closed UD cases. This report synthesizes NARA's analysis of the information gathered during the assessment. See **Appendix A** for a list of participating agencies.

Assessment Scope

This assessment primarily focused on agency policies, procedures, and practices related to reported safeguards associated with UD incidents and the requirements outlined in [36 Code of Federal Regulations Chapter XII Subchapter B Part 1230](#) (36 CFR 1230).

Assessment Methodology

NARA utilized internal data from closed UD cases and developed specific selection criteria to identify a small subset of cases for deeper analysis during the assessment. Agencies associated with the selected subset of UD cases were invited to participate in this assessment.

NARA reviewed formal correspondence, UD reports, and any supporting documentation agencies provided for the selected UD cases. Additionally, participating agencies were asked to provide relevant policies, procedures, tools, and training materials associated with the UD reporting process and reported safeguards for each case.

Finally, NARA conducted interviews with agency representatives to understand how each agency investigates, reports, and establishes safeguards in response to UD occurrences.

UD Cases Data Analysis

NARA analyzed data for 316 closed UD cases from FY 2017-2023. The criteria below were used to identify which cases and agencies should receive closer evaluation during the assessment.

UD Case Selection Criteria

NARA focused on UD cases that were:

1. Annotated as closed and founded;
2. Related to destruction, removal, or alienation (i.e., record losses by unknown means or records lost during shipment);
3. Illustrating similar UD incidents reported by a department/agency more than once; and
4. Categorizable by having at least two or more similar characteristics such as record format, subject, annotated UD type, or UD circumstance.

Table 1. The number of UD cases considered during preliminary evaluation.

Total closed cases (founded & unfounded)	316
Total founded destruction cases	184
Total founded removal cases	44
Total founded alienation cases	9
Total cases considered based on selection criteria	237

Table 2. The number of selected cases by category and agency.

UD Categories	Total no. of UD cases	Agency A	Agency B	Agency C	Agency D	Agency E	Agency F	Agency G
Unauthorized destruction related to FOIA	5	5						
Unauthorized removal by departing agency personnel	2	2						
Accidental disposal/deletion by agency personnel	7	1	3				3	
Missing - unknown causation	10			2		7		1
Lost in transit during shipment to offsite storage from agency	4		4					
Lost in transit during shipment to agency from offsite storage	5		1		4			
Accidental destruction at offsite storage	3		3					
Inadvertent deletion of cellular data	2			2				
Total UD cases	38	8	11	4	4	7	3	1

NB: This report provides anonymity for participating agencies by concealing specific identifiers that may reveal which agency reported what information.

36 CFR 1230–Unlawful or Accidental Removal, Defacing, Alteration, or Destruction of Records

[36 CFR 1230](#) mandates that the heads of federal agencies must prevent the unlawful or accidental removal, defacing, alteration, or destruction of federal records based on the mandatory disposition instructions defined by a NARA-approved records schedule, also known as a UD incident or occurrence. This regulation identifies applicable penalties, [18 USC 641](#) and [207](#), and outlines what actions agencies and NARA must take when allegations of or actual UDs occur.

According to 36 CFR 1230 (b), *alteration* means the unauthorized annotation, addition, or deletion of information to a record; *defacement* refers to the obliteration, marring, or spoiling of the appearance or surface of a record to the extent that it impairs the usefulness or value of the record; and *removal* indicates selling, donating, loaning, transferring, stealing, or otherwise allowing a record to leave the custody of a federal agency without the permission of the Archivist of the United States.

Unlawful or accidental destruction speaks to the disposal of an unscheduled, temporary or permanent record prior to the end of a NARA-approved retention period, other than court-ordered disposal described in [36 CFR 1226.14\(e\)](#), and destruction of a record subject to a Freedom of Information Act (FOIA) request or litigation hold.

Reporting UD Incidents

When an actual UD incident occurs, agencies must promptly send a report to the Office of the Chief Records Officer, RM Oversight and Reporting Program via email to UnauthorizedDisposition@nara.gov. The report must be submitted or approved by the individual authorized to sign records schedules or persons assigned operational responsibility for the agency's RM program. For example, the department or agency records officer (DRO/ARO), a Senior Agency Official for RM (SAORM), or other RM program personnel appointed by the DRO/ARO.

When an agency reports a UD incident to NARA, the agency must include the reporting requirements described below. UD cases remain open until an agency has satisfactorily met each requirement.

UD Reporting Requirements

- 1. A complete description of the records with volume and dates if known:** A “complete description” is a description of the content or types of information the record documents, a record series, or a NARA-approved disposition authority number.

A record series is a collection of records or documented information arranged according to a classification system or because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship associated with its creation, receipt, or use ([36 CFR 1220.18](#)).

A disposition authority is legal authorization granted by the Archivist of the United States to retain or dispose of federal records (36 CFR 1220.18). Volume quantifies the number of records lost based on the record medium type or record content, for example, five cubic feet, two manilla folders, five two-inch binders, one TB of data, 34 email accounts, 103 emails, or four 75mm film reels.

Finally, dates should represent when the records were created or the date range covering the records in question (e.g., emails from calendar year (CY) 2000 - 2007, FY 2012 budget files, or litigation case files from January - April 2021).

- 2. The office maintaining the records:** This requirement refers to which agency program office, division, branch, or component has custodial responsibility for managing the records at the time of the loss.

3. **A statement of the exact circumstances surrounding the removal, defacing, alteration, or destruction of records:** Agencies must provide as much detailed information as possible regarding the circumstances surrounding the UD incident. This should include what precipitated the loss of records, the timeframe when the incident occurred, who was involved, and why this incident occurred.
4. **A statement of the safeguards established to prevent further loss of documentation:** Reported safeguards should describe any controls, processes, and procedures an agency implements to ensure the circumstances surrounding the removal, defacing, alteration, or destruction of records do not reoccur.

When establishing UD safeguards, agencies should carefully evaluate current RM practices, policies, and procedures, as well as relevant systems and agency personnel behaviors, to identify contributing factors that led to the UD incident and determine what immediate or eventual actions are necessary to prevent further loss of agency records in this manner.

For example, if an agency reported an employee lost paper receipts while teleworking, a potential safeguard could entail creating new procedures and supplying the necessary equipment that would facilitate the digitization of paper receipts and uploading the digitized files to an agency's Electronic Records Management System (ERMS) from the employee's telework location.

5. **When appropriate, details of the actions taken to salvage, retrieve, or reconstruct the records:** Agencies should describe any attempts to recover or rebuild records from other sources. For example, if backup files exist, another program office maintains records containing information that could re-establish the lost record partially or entirely, or copies of lost records can be obtained from a third party outside the agency.

NARA Treatment of UD Allegations

NARA receives UD allegations from a variety of sources including private citizens, publications from news media outlets, agency personnel, Congress, agency Offices of Inspector General (OIG), NARA's Federal Records Center Program (FRCPP), as well as other program offices.

Upon receiving sufficient plausible information regarding a potential or actual loss of federal records, the Chief Records Officer (CRO) of the federal government sends formal correspondence (UD case letters) to the DRO/ARO of the agency associated with the allegation requesting an investigation and a formal response of agency findings within 30 days.

A listing of open and closed UD cases, including related NARA correspondence, is posted on [NARA's Unauthorized Disposition of Federal Records](#) webpage.

FINDINGS AND RECOMMENDATIONS

UD Policies and Procedures

Most agencies covered mandated UD reporting requirements in their overarching RM policy or mandatory annual RM training. Some agencies developed standard operating procedures (SOPs) and a standard reporting form that agency staff must complete to report UD incidents to its RM program.

One agency had a section on its RM intranet website dedicated to UD. This internal website identified agency RM program points of contact, UD reporting instructions, and the agency's standard reporting form. This agency also held training on investigating UD incidents and completing its internal reporting form during quarterly meetings with its RM network staff. NARA considers this agency's policies and procedures a best practice.

Agencies that used a standard reporting form, covering UD in its annual RM training and regularly informing their RM network staff on UD reporting requirements, often received sufficient and more meaningful information to meet the reporting requirements of 36 CFR 1230.

Recommendation 1: Agencies should create multiple RM resources that support UD reporting requirements. NARA recommends resources like SOPs, an internal agency reporting form, and how-to training materials that give examples and guide agency personnel with information and specific actions required when UD incidents occur.

Recommendation 2: Agencies should ensure that all RM resources related to UD are easy to find and are periodically and intentionally promoted throughout the agency. Strategic and regular announcements can ensure all personnel are informed on the agency's responsibilities to prevent UD incidents and how UD incidents must be handled to meet reporting requirements.

Agency UD Investigations

Some agencies indicated that when UD incidents occurred, the agency personnel involved in the incident were responsible for investigating and developing the UD report submitted to NARA. Other agencies asserted that personnel engaged in a UD incident would complete the agency's internal reporting form, submit the form to its RM program, and the ARO or other RM network staff would collaborate with the individual who submitted the form to thoroughly investigate the incident and create the report sent to NARA.

When RM program staff are consistently involved with investigating UD incidents, it is more likely for agencies to not only quickly and more accurately satisfy all UD reporting requirements, but also tend to develop more comprehensive and adequate UD safeguards that prevent UD reoccurrences.

Recommendation 3: When UD incidents occur, agencies' RM programs should lead standardized investigatory actions to ensure sufficient information is gathered in a timely fashion and documented to satisfy all UD reporting requirements.

UD Safeguards

NARA reviewed each UD case report to identify safeguards and correlated that information with each agency's documentation provided for the assessment data call. Finally, during interviews, NARA validated how agencies implemented and assessed the efficacy of their safeguards. See Appendix B for a table that briefly describes the reported safeguard for each UD case evaluated in this assessment.

NARA found that agencies successfully implemented reported safeguards for most UD cases. One agency had a few components of its safeguard still in development, and another agency was awaiting senior management approval to deploy its reported safeguard.

NARA observed that safeguard implementation could be an iterative process where what agencies reported to NARA could evolve over several months or even years after being reported as agencies become more engaged with the myriad of factors leading to UD occurrences or receive the necessary resources to implement safeguards.

Some agencies exhibited poor follow-through with ensuring that reported safeguards were substantially implemented or consistently executed after implementation. One agency's RM program was never involved in the UD safeguard development or implementation. Other agencies had safeguards that failed to comprehensively address vulnerabilities, thus leading to the recurrence of similar UD incidents.

Additionally, NARA noted that other contributing factors that may lead to an agency having ineffective safeguards or UD recurrences could be traced to insufficient communication of established safeguards across different agency components or the elements that led to the UD incident being outside the agency's control.

One of the participating agencies utilizes its OIG, and another agency relies on its Office of Quality Assurance to promote timely implementation and compliance with UD safeguards. One other agency described involving its SAORM in developing UD safeguards to augment the RM program's ability to gain senior management buy-in and acquire the needed resources to implement the developed safeguards fully.

Recommendation 4: Agencies should leverage their RM program and network of RM staff's specialized perspectives and RM expertise whenever a UD incident occurs. It is imperative that RM programs lead and collaborate with agency program offices/components to develop UD safeguards to ensure that any policies, procedures, processes, or systems created as interventions are comprehensive solutions that appropriately remediate circumstances that led to UD incidents.

Recommendation 5: Agency RM programs should monitor how agency components implement established safeguards to confirm whether safeguards have been completed correctly and

validate that the safeguard sufficiently addresses those factors that contributed to the UD incident.

Recommendation 6: Agency RM programs should consider which program offices or senior-level personnel could enhance their ability to deploy and enforce compliance with developed UD safeguards and involve these offices or individuals in UD safeguard development, implementation, and monitoring.

Recommendation 7: When an agency experiences a UD incident that involves business practices, systems, or record types that are common to multiple program offices/components, agencies should create a mechanism for sharing these UD incidents and their implemented safeguards agency-wide or to all relevant program offices. Doing so enhances agency personnel's awareness of potential RM vulnerabilities and the safeguards established to redress these vulnerabilities.

Recommendation 8: When agencies develop UD safeguards that potentially require several months or years to implement thoroughly, and the UD incident involves permanent or mission-critical records, agency RM programs should consider developing immediate temporary solutions to prevent future loss of records in the interim.

Recommendation 9: When a UD incident involves permanent or mission-critical functions or records, agencies should consider developing a process that regularly monitors and evaluates the efficacy of implemented safeguards. Having an established monitoring strategy enables agencies to respond to inefficiencies or areas of noncompliance more expeditiously, preventing future potential losses.

CONCLUSION

In conclusion, this comprehensive review of 38 UD cases, the reporting, investigation, and the development of safeguards across the participating agencies highlights the critical role that robust RM policies, procedures, and training play in mitigating the risk of UD incidents. Best practices identified, such as the use of SOPs, standard reporting forms, dedicated RM resources, and regular training, significantly enhance an agency's ability to meet reporting requirements, investigate incidents effectively, and implement effective safeguards.

NARA's recommendations emphasize the importance of creating accessible RM resources, leading standardized investigatory actions, developing comprehensive UD safeguards, and ensuring the thorough implementation and monitoring of these safeguards. Agencies are encouraged to adopt a proactive and collaborative approach to RM when UD incidents occur, leveraging the expertise within their RM programs and involving senior management to secure the necessary resources and buy-in for implementing and sustaining effective safeguards. By doing so, agencies can better protect their records from unauthorized dispositions, thereby preserving crucial information that supports the mission, operations, and record-keeping responsibilities of the federal government.

APPENDIX A

Table 4. List of Participating Agencies

#	Department and Agency
1.	Department of Agriculture – Agriculture Research Services
2.	Department of Defense – Air Force
3.	Department of Defense – Defense Logistics Agency
4.	Department of Defense – Office of the Secretary of Defense
5.	Department of Homeland Security – US Coast Guard
6.	Department of Justice – Federal Bureau of Investigations
7.	Department of Treasury – Internal Revenue Service

APPENDIX B

Table 3. Summary of Reported Safeguard per UD Case.

#	UD Case Category	UD Safeguard Summary
1	Accidental destruction at offsite storage	Reviewed and modified operational and quality control processes in collaboration with the custodial agency's personnel. Appropriate offsite storage personnel were evaluated and retrained.
2	Accidental destruction at offsite storage	Offsite storage vendor reviewed and modified operational and quality control (QC) processes in collaboration with the custodial agency's personnel. Appropriate offsite storage personnel were evaluated and retrained.
3	Accidental destruction at offsite storage	Agency collaborated with custodial agency personnel to evaluate and update QC procedures.
4	Accidental disposal/deletion by agency personnel	Agency developed and implemented new RM storage, transfer and destruction procedures, and reiterated agency RM policies and procedures with relevant personnel.
5	Accidental disposal/deletion by agency personnel	Agency developed and implemented new RM destruction procedures and guidance.
6	Accidental disposal/deletion by agency personnel	Agency retrained agency personnel on shipping procedures and systems.
7	Accidental disposal/deletion by agency personnel	Agency established and implemented a digitization initiative to eliminate hardcopy records and developed new controls to safeguard hardcopy records awaiting digitization. Agency retrained relevant personnel on basic RM, staging, tracking, and shipping procedures for records being digitized.
8	Accidental disposal/deletion by agency personnel	Agency established and implemented a digitization initiative to eliminate hardcopy records and developed new controls to safeguard hardcopy records awaiting digitization. Agency retrained relevant personnel on basic RM, staging, tracking, and shipping procedures for records being digitized.
9	Accidental disposal/deletion by agency personnel	Agency reported reviewing and updating current RM procedures to implement stricter ERMS controls, executing disposition instructions/applicable records schedule, and additional administrator user roles to improve quality assurance (QA). Agency provided additional RM training for agency personnel using the ERMS.
10	Accidental disposal/deletion by agency personnel	Agency reissued comprehensive RM training modules for ERMS users, redesigned system controls to limit disposition/deletion responsibility to program office supervisory staff, implemented a new verification process for applying records disposition and included new RM best practices to SOPs.

11	Accidental disposal/deletion by agency personnel	Agency reviewed current change management processes, established new procedures to implement Amazon Web Services lifecycle management policies, and verified system back-up procedures.
12	Inadvertent deletion of cellular data	Agency RM program will reissue electronic RM policies and procedures associated with mobile device usage to end users prior to scheduled system upgrades advising agency personnel to capture and transfer all electronic records from mobile phones before system upgrades are performed. The RM program will reissue RM training materials that emphasize recordkeeping responsibilities for government-furnished mobile device users.
13	Inadvertent deletion of cellular data	Agency IT staff were advised to perform mobile device backup procedures prior to re-registering mobile devices that disconnect from the agency network.
14	Lost in transit during shipment from offsite storage to agency	Offsite storage vendor retrained specific offsite storage staff on relevant shipping policies and procedures.
15	Lost in transit during shipment from offsite storage to agency	Agency created new reporting procedures for missing records associated with offsite storage shipments and updated SOPs.
16	Lost in transit during shipment from offsite storage to agency	Agency created new reporting procedures for missing records associated with shipments and updated SOPs.
17	Lost in transit during shipment from offsite storage to agency	Agency created new reporting procedures for missing records associated with shipments and updated SOPs.
18	Lost in transit during shipment from offsite storage to agency	Agency developed, implemented and began validating new check-in and QC procedures including a new tracking system to manage shipments received from offsite storage.
19	Lost in transit during shipment to offsite storage from agency	Agency representatives discussed additional packaging steps that could maintain the integrity of shipping boxes for future shipments of specific record types.
20	Lost in transit during shipment to offsite storage from agency	Custodial agency reported making considerations for approving travel and per diem for agency personnel to drive future transfers to offsite storage.
21	Lost in transit during shipment to offsite storage from agency	Custodial agency requested that offsite storage provide immediate notification of missing shipments.

22	Lost in transit during shipment to offsite storage from agency	Custodial agency staff discussed possible ways to mitigate lost boxes shipped by UPS and requested offsite storage to conduct more timely reviews of received shipments so that shipment inconsistencies could be reported to the agency sooner.
23	Missing - unknown causation	Agency supervisor reviewed RM policies and procedures with relevant agency staff.
24	Missing - unknown causation	Agency personnel developed and implemented new recordkeeping procedures.
25	Missing - unknown causation	Agency provided a brief overview of current RM procedures and described the monthly auditing process that agency record managers will conduct to reconcile loaned or charged out records.
26	Missing - unknown causation	Agency developed and implemented new procedures prohibiting personnel from hand-carrying records throughout the organization and reissued RM training materials to educate agency personnel on recordkeeping requirements.
27	Missing - unknown causation	Agency outlined current RM procedures, education, controls and systems that were recently implemented to automate electronic record transfers within the organization.
28	Missing - unknown causation	Agency provided a brief statement describing current RM procedures.
29	Missing - unknown causation	Agency projects establishing digitization initiatives to eliminate historic hardcopy records and disclosed that contemporary records are born and managed electronically.
30	Missing - unknown causation	Agency concluded that the missing records were accounted for and the UD report was made in error. However, the agency updated and reissued UD reporting policy and procedures throughout relevant program offices.
31	Unauthorized destruction related to FOIA requests	Immediate changes made to agency FOIA policy and procedures instructing agency personnel when record searches must be conducted after receiving a FOIA request. Eventual changes include developing RM disposition controls in a new automated FOIA processing system.
32	Unauthorized destruction related to FOIA requests	Immediate changes made to agency FOIA policy and procedures instructing agency personnel when record searches must be conducted after receiving a FOIA request. Eventual changes include developing RM disposition controls in a new automated FOIA processing system.
33	Unauthorized destruction related to FOIA requests	Developed and implemented new legal hold validation process, executed supplemental searches to confirm receipt of responsive records, modified administrative processes to include appropriate electronic flags within FOIA processing system, and updated SOPs and training materials. Eventual changes include developing RM disposition controls in a new automated FOIA processing system.
34	Unauthorized destruction related to FOIA requests	Immediate changes include SOP updates regarding enhanced QA procedures to identify and flag cases under legal hold, appropriate staff completed mandated training, program office will maintain backup copies of deleted FOIA records for one year after deletion. Eventual changes include

		automating the legal hold flagging process in a new automated FOIA processing system.
35	Unauthorized destruction related to FOIA requests	Agency made changes to FOIA policy and procedures instructing agency personnel when record searches must be conducted after receiving a FOIA request. Eventual changes include developing RM disposition controls in a new automated FOIA processing system.
36	Unauthorized destruction related to FOIA requests	Agency updated controls to improve system backup capabilities and retention policy, modified and reissued SOPs to all staff and executed training with specific agency personnel on proper disposition procedures of FOIA records after legal holds are lifted.
37	Unauthorized removal by departing agency personnel	Agency's redress included recovering removed records. Agency mandated annual training on handling records and conducted periodic awareness campaigns regarding protecting agency records, reporting UD threats or incidents and disciplinary/criminal consequences for UD.
38	Unauthorized removal by departing agency personnel	Agency's redress included recovering removed records. Agency mandated annual training on handling records and conducted periodic awareness campaigns regarding protecting agency records, reporting UD threats or incidents and disciplinary/criminal consequences for UD. Agency will increase awareness of all applicable policies relevant to UD.