



NCUA
National Credit Union Administration

OFFICE OF INSPECTOR
GENERAL

**AUDIT OF THE NCUA'S INFORMATION TECHNOLOGY ASSET
SANITIZATION PROCESS**

**Report #OIG-25-10
December 17, 2025**





National Credit Union Administration

Office of Inspector General

SENT BY EMAIL

TO: Distribution List

FROM: Acting Inspector General Marta Erceg *Marta Erceg*

SUBJ: Audit of the NCUA's IT Asset Sanitization Process

DATE: December 17, 2025

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) conducted this self-initiated audit to assess the NCUA's information technology (IT) asset sanitization process. The objective of our audit was to determine whether the NCUA adequately managed and sanitized its IT assets before disposal or reuse.

Our audit determined the NCUA adequately sanitized its IT assets before disposal or reuse. However, we determined the NCUA should make improvements to its IT asset accountability process because the process did not include a clear chain of custody and other controls. We are making three recommendations in our report and note that NCUA management plans to take corrective action to address the issues we identified.

We appreciate the cooperation and courtesies NCUA management and staff provided to us during the audit. If you have any questions on the report or its recommendations, please contact me at 703-518-6352.

Distribution List:

Chairman Kyle S. Hauptman

Executive Director Larry Fazio

Chief of Staff Sarah Bang

General Counsel Frank Kressman

Acting Deputy Executive Director Towanda Brooks

Acting Deputy Executive Director Kelly Lay

Acting Chief Information Officer Amber Gravius

Director, Office of External Affairs and Communications Sierra Robinson

Attachment



Table of Contents

EXECUTIVE SUMMARY	1
BACKGROUND	2
RESULTS IN DETAIL.....	6
Improvements Are Needed for the IT Assets Return and Safeguarding Process.....	6
APPENDIX A.....	10
Objective, Scope, and Methodology	10
APPENDIX B	12
NCUA Management Response	12
APPENDIX C	14
Acronyms and Abbreviations.....	14



EXECUTIVE SUMMARY

The NCUA OIG conducted this self-initiated audit to assess the NCUA's information technology (IT) asset sanitization process. The objective of our audit was to determine whether the NCUA adequately managed and sanitized its IT assets before disposal or reuse. The scope of our audit covered the NCUA's IT asset sanitization activities from January 2022 through December 2024.

Our audit determined the NCUA adequately sanitized its IT assets before disposal or reuse. However, we determined the NCUA should make improvements to its IT asset accountability process because the process did not include a clear chain of custody and other controls.

We are making three recommendations in our report to address the issues we identified.



BACKGROUND

The NCUA is an independent federal agency created by the U.S. Congress. It insures deposits at federally insured credit unions, protects credit union members, and charters and regulates federal credit unions. The NCUA's organizational structure consists of a headquarters (central office), the Asset Management and Assistance Center, and three regional offices.¹

NCUA conducts examinations and other supervisory activities regarding credit unions. There were over 4,455 federally insured credit unions as of December 31, 2024. The NCUA has access to sensitive information that may include information about a person or organization that is not public information, including nonpublic personally identifiable information, which employees may store on electronic devices, including their laptops and cell phones.² Improper disclosure of sensitive information stored on employees' electronic devices could result in harm to an NCUA employee, credit union, consumer, or other parties external to the NCUA. Thus, the NCUA requires employees to comply with agency policies to secure laptops and mobile devices.³

Guidelines for Media Sanitization, National Institute of Standards and Technology (NIST) Special Publication 800-88 Revision 1 (Dec. 2014)

NIST Special Publication 800-88 Revision 1 provided guidelines to assist federal agencies in implementing a media sanitization program with techniques and controls for sanitization and disposal decisions based on the confidentiality of the system's information. NIST Special Publication 800-88 Revision 1 defines the term "media" as material on which data may be recorded. Media sanitization refers to a process that renders access to data on the media infeasible (inaccessible). Media sanitization is one of the key elements in assuring confidentiality. For agencies to have appropriate controls of the information they are responsible for safeguarding, they must properly secure IT assets.

The types of sanitization are:

- **Clear:** Applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; it is typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state.
- **Purge:** Applies physical or logical techniques that render Target Data recovery infeasible using state-of-the-art laboratory techniques.
- **Destroy:** Renders Target Data recovery infeasible and results in the subsequent inability to use the media for storage of data.

¹ The three regional offices are the Eastern, Southern, and Western regions.

² Our audit focused on laptops and cell phones. Other IT assets include hotspots, hard drives, and tablets, but because there are far fewer of these assets, we did not include them in this audit.

³ NCUA Instruction 13500.09 (Rev. 1), Security of Sensitive Information.



NIST 800-88 Special Publication Revision 1 states that cryptographic erase may be used when data is encrypted. This is a method of sanitization in which the media encryption key is sanitized, making recovery of decrypted data infeasible.

Office of the Chief Information Officer

The NCUA's Office of the Chief Information Officer (OCIO) is responsible for ensuring the resilience of the NCUA's IT infrastructure, including managing and supporting IT services and solutions and the availability and reliability of technological applications for the NCUA's workforce. The Federal Information Security Modernization Act of 2014 requires federal agencies to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access or use of information. NCUA's information security practice includes agency-wide and program-specific policies and procedures for collecting, retaining, and destroying data. OCIO's responsibilities include managing and sanitizing IT assets to ensure that sensitive data is protected against unauthorized disclosure. For organizations to have appropriate controls of the information they are responsible for safeguarding, they must properly secure IT assets. Sanitization is one of the key elements in assuring confidentiality and refers to the process that renders data in computers, phones, and other IT assets unrecoverable. OCIO has an IT service management system for tracking.

OCIO indicated it managed approximately 1,550 laptops and 1,300 cell phones (including some tablets), as well as other electronic devices, during the scope period of our audit. Laptops are replaced according to a scheduled cycle. The last laptop replacement was in 2022, which resulted in sanitizing and disposing of old laptops. The contract for this process included the following sanitization requirements:

- Asset Data Sanitization Services
 - The contractor shall sanitize all recovered NCUA legacy laptops in accordance with NIST Special Publication 800-88, Revision 1, Guidelines for Media Sanitization.
 - NIST Special Publication 800-88 Revision.1 Conformant Sanitization: The contractor shall perform NIST Special Publication 800-88 Rev. 1 conformant sanitization in a secure and insured facility and provide NCUA with the facility's complete address.
 - NIST Special Publication 800-88 Revision.1 Sanitization Certification Report: The contractor shall provide a report certifying each legacy laptop has been successfully sanitized in conformance with NIST Special Publication 800-88 Rev.1 guidelines.

OCIO's Media Protection Control Family Policy addresses the protection, marking, sanitization, production input/output, and disposal of media (such as laptops and cell phones) containing sensitive information. The policy states that all levels of NCUA management must ensure



employees, contractors, vendors, and other third-party entities protect information system media, both paper and digital; limit access to information-on-information system media to authorized users; and sanitize or destroy information system media before disposal or release for reuse.

The policy further states that the NCUA must sanitize all digital and non-digital media using approved equipment, techniques, and procedures prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organizational standards and policies. Sanitization mechanisms include clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction. Specific safeguards include:

- Workstations are reimaged from standard images prior to reissuance to users.
- NCUA-issued cell phones are wiped by the service desk prior to reissuance.
- All electronic information and licensed software are removed when disposing of computers with hard drives.
- IT resources and digital storage media are cryptographically erased of all information.
- Non-digital media are disposed of through shredding or locked box for later shredding.

Litigation Holds

The Enforcement and Litigation Division (E&L) of the Office of General Counsel is responsible for the issuance and management of litigation holds in connection with all enforcement matters and all active or reasonably anticipated litigation. A litigation hold is an internal process to identify and ensure the preservation of relevant information concerning a current or reasonably anticipated future legal action involving the agency. A litigation hold serves to avoid spoliation (the destruction, alteration, or mutilation of evidence) and any court-ordered sanctions or other consequences associated with noncompliance with the litigation hold. All IT devices for NCUA employees subject to litigation holds are not sanitized and kept locked in a storage closet by OCIO. The steps of E&L's litigation hold process are as follows:

- Step 1: When an E&L staff attorney determines that a litigation hold is necessary in a matter or case, the attorney will notify the Associate General Counsel for E&L and provide the names of all property custodians⁴ likely to possess relevant evidence.
- Step 2: The Associate General Counsel issues a litigation hold memo to the property custodians by email at the earliest possible opportunity, no later than 30 calendar days following a determination that litigation is reasonably anticipated or after the case has been filed/assigned.

⁴ Property custodians are OCIO staff who are responsible for the accountability and safeguarding of all property and the completeness and accuracy of the information recorded in the asset management system.



- Step 3: Once the litigation hold memo has been sent to the property custodians, an E&L paralegal confirms with the property custodians that they received the memo.
- Step 4: The paralegal enters the names of all custodians into the E&L litigation hold tracker.
- Step 5: Until a litigation hold is lifted, the paralegal periodically will send an email to property custodians to remind them of their continuing obligation to preserve documents.
- Final Step: Once litigation is finalized and appeal period has ended, the Associate General Counsel will notify the property custodians that the litigation hold has been lifted and that preserving relevant information is no longer required.



RESULTS IN DETAIL

The objective of our audit was to determine whether the NCUA adequately managed and sanitized IT assets before disposal or reuse. Based on our audit work, we determined the NCUA adequately sanitized IT assets before disposal or reuse. We determined through interviews, a walkthrough of the IT service management system, and a review of supporting documents that OCIO staff and contractors consistently performed the following to sanitize IT assets:

- Appropriate staff and contractors wiped IT assets, including deleting the image⁵ that held the user's data,
- Reset and cleared data from cell phones, and
- Stored IT assets and did not wipe them when there was a litigation hold.

However, we concluded the NCUA should make improvements to its process regarding the managing of IT assets. Specifically, we found that NCUA's IT asset accountability process lacked a chain of custody for the IT assets⁶ and other controls. We are making three recommendations in our report to address the issues we identified.

The detailed results of our audit follow.

Improvements Are Needed for the IT Assets Return and Safeguarding Process

We determined the NCUA needed to improve the return process for IT assets to track and safeguard assets. Specifically, we determined that IT assets were often left in an unlocked or unattended OCIO office without appropriate tracking by OCIO, such as a document timely recording OCIO's receipt of the IT asset.

NCUA Instruction 1710.6, Receipt, Transfer, and Disposal of Accountable Property, states: "All NCUA employees, contractors, and agency partners are to act in a reasonable and prudent manner to properly use, care for, and safeguard all NCUA property in accordance with the best interest of the NCUA." Additionally, the instruction requires "locking and securing all accountable property not in use in a location to which only authorized NCUA employees have access." Also, Government Accountability Office's Standards for Internal Control, GAO-14-704G (Sept. 2014)(the Green Book) states:

- Roles in an Internal Control System

⁵ An image is an exact copy of all electronic data on a device, performed in a manner that ensures the information is not altered.

⁶ Chain of custody is a process used to track the movement and control of an asset through its lifecycle by documenting each person and organization who handles an asset, the date/time it was collected or transferred, and the purpose of the transfer. Maintaining the chain of custody increases transparency and enables accountability for actions taken on the asset.



- OV2.24: Management designs an internal control system to provide reasonable assurance regarding prevention or prompt detection and correction of unauthorized acquisition, use, or disposition of an entity's assets.
- Principle 8 - Assess Fraud Risk
 - Types of Fraud
 - Misappropriation of assets - Theft of an entity's assets. This could include theft of property, embezzlement of receipts, or fraudulent payments.
- Principle 10 - Design Control Activities
 - Physical control over vulnerable assets
 - Management establishes physical control to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment that might be vulnerable to risk of loss or unauthorized use. Management periodically counts and compares such assets to control records.

OCIO employees did not know when employees returned their IT assets, and these assets were left unattended and unaccounted for an unknown period. Because OCIO did not have a documented return process for IT assets that required timely tracking and safeguarding, OCIO did not comply with the instruction or these principles occurred. Without appropriate tracking and safeguarding of assets, the chain of custody was not maintained, which could have affected litigation holds and increased the risk for assets to be lost, misplaced, or stolen.

Details

We determined the NCUA should improve its process for tracking and safeguarding IT assets returned to OCIO by employees, especially for IT assets subject to a litigation hold. Our audit determined that employees returned IT assets by leaving them in an unlocked and sometimes unattended OCIO office for OCIO staff (including contractors) to document receipt as staff were available to do so. On occasion, departing employees left their equipment with others to give to OCIO. Some employees returned IT assets to the Division of Procurement and Facilities Management (DPFM) instead of OCIO. We could not determine the amount of time between an IT asset being dropped off to when it was entered into the IT service management system for tracking. The process did not allow for appropriate tracking, including not providing a clear chain of custody for IT assets.

While not within the scope of our audit, as part of the NCUA's voluntary separation program,⁷ the exit procedures for departing employees stated: "Employees will be provided key information of where to return their equipment or where they may mail the equipment to include

⁷ The NCUA's voluntary separation program was designed to comply with Executive Order 14210, Implementing the President's "Department of Government Efficiency" Workforce Optimization Initiative, dated February 11, 2025, to reduce the size of the federal workforce. Although the voluntary separation program caused a large volume of IT asset returns during a short period of time, the process of returning IT assets to OCIO remained substantially the same.



self-addressed FedEx packaging for return to the NCUA.” The agency told employees that they should take their IT assets to a designated OCIO office and leave the IT assets on the table in that office, which generally was unattended. That was also the process for any time an employee dropped off an IT asset, not just for when an employee departed the agency.

The Inspector General stated that when he left his cell phone in a designated OCIO office, he saw other cell phones sitting on a desk unattended. He noticed that the cell phones had been previously assigned to other NCUA employees who may have been subject to litigation holds. This is significant because it is essential that there be a chain of custody for the IT assets to ensure the data on them is preserved in the event they are needed for litigation. OCIO’s lead IT specialist/property custodian stated that he instructed employees to leave laptops and other IT assets in an unlocked OCIO office for employee convenience. He also stated that he was not aware of any current standard operating procedures (SOPs) for collecting and tracking returned IT assets. His supervisor confirmed that the practice was to instruct employees to leave their IT assets on the table in the designated OCIO office for OCIO staff to enter a tracking ticket and dispose of or store the device when staff are available to do so. Another property custodian stated that he was concerned about IT asset storage because laptops were stored in the unlocked OCIO office and there was not always enough space to store the laptops.

During the scope of this audit, OCIO was unable to provide a list of all IT assets held in the past by employees because the IT service management system only contained employees’ current IT assets and was not configured to track IT assets by employee. An OCIO contractor indicated that OCIO planned to add tracking assets by employee to the IT service management system. The DPFM director stated that he had received requests from the Executive Director’s office regarding an employee’s IT asset history and he and OCIO staff were unable to easily respond to these requests for information because IT assets were not tracked by employee, only by the IT asset itself. An employee’s IT asset history could provide a basis for discipline or otherwise hold an employee accountable if the employee has lost or damaged their cell phone or laptop, including previous devices. Based on the Rules of Behavior each employee signs, “It is the responsibility of each user to properly care for and maintain agency-owned equipment they are assigned or use. This responsibility includes taking reasonable actions to prevent damage to or loss of the equipment.”

Also, we determined that OCIO did not have the personal identification numbers for some cell phones that employees turned in, thus making the cell phones inaccessible once the service to the phone is terminated. This is particularly a problem for cell phones of employees subject to a litigation hold when the data on the cell phones could be needed for litigation.

Based on the identified issues related to the IT asset management process, we are making the following recommendations.

Recommendation

We recommend NCUA management:



1. Update and implement the Accountable Property Handbook to address returning IT assets that requires a secure chain of custody process, including IT assets subject to litigation holds.

Management Response

Management agreed with our recommendation. Management will update the Accountable Property Handbook and implement the chain of custody procedures by March 31, 2026.

OIG Response

We concur with management's planned actions.

2. Update the offboarding procedures to include instructions to employees to ensure exiting employees return their IT assets in accordance with the updated Accountable Property Handbook.

Management Response

Management agreed with our recommendation. Management will revise the offboarding procedures to align with the updated Accountable Property Handbook by September 30, 2026.

OIG Response

We concur with management's planned action.

3. Improve the IT asset accountability process going forward to include historical IT asset tracking by employee and by addressing and implementing data access procedures for returned cell phones on litigation holds.

Management Response

Management agreed with our recommendation. Management will review processes and implement procedures by September 30, 2026, consistent with agency business needs and retention schedules.

OIG Response

We concur with management's planned action.



Appendix A

Objective, Scope, and Methodology

We developed our objective for this engagement based on OIG's 2024 Annual Work Plan. Specifically, our objective was to determine whether the NCUA adequately managed and sanitized its IT assets before disposal or reuse.

To accomplish our audit, we performed fieldwork with information relevant to the NCUA's IT asset sanitization process obtained from various NCUA sources. The scope of the audit covered the NCUA's IT asset sanitization activities from January 2022 through December 2024. To achieve our objectives, we:

- Reviewed the NCUA's policies and procedures.
- Interviewed Office of the Chief Financial Officer, OGC, and OCIO personnel.
- Obtained an understanding of the NCUA's IT asset sanitization process.
- Evaluated internal controls related to the NCUA's IT asset sanitization process.

We did not rely on computer-processed data from NCUA systems to answer the audit objective. We conducted this audit from December 2024 through November 2025 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. 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. Specifically, we assessed 4 of the 5 internal control components, and 4 of the 17 associated underlying principles defined in the Government Accountability Office's Standards for Internal Control in the Federal Government. We determined that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We summarize in Table 1 below the internal control components and underlying principles we assessed.

Table 1: Internal Control Components and Underlying Principles Assessed

Component #1: Control Environment
Principle #3 – Establish Structure, Responsibility, and Authority
Component #2: Risk Assessment
Principle #8 – Assess Fraud Risk
Component #3: Control Activities
Principle #10 – Design Control Activities
Component #4: Information and Communication
Principle #14 – Communicate Internally



The report presents within the findings the internal control deficiency we identified. However, because our audit was focused on these significant internal control Components and underlying Principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.



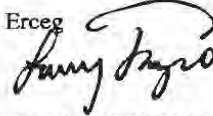
Appendix B

NCUA Management Response



National Credit Union Administration
Office of the Executive Director

SENT BY EMAIL

TO: Acting Inspector General Marta Erceg
FROM: Executive Director Larry Fazio 
SUBJ: Management Response: OIG Audit of the NCUA's Information Technology Asset Sanitization Process
DATE: December 16, 2025

Thank you for the opportunity to review the Office of Inspector General's draft report *Audit of the NCUA Information Technology Asset Sanitization Process*. The report includes three recommendations for strengthening the information technology asset sanitization process.

Recommendation #1

Update and implement the Accountable Property Handbook to address returning IT assets that requires secure chain of custody process, including IT assets subject to litigation holds.

Management Response:

Management concurs. The NCUA will update the Accountable Property Handbook and implement chain of custody procedures by March 31, 2026.

Recommendation #2

Update the offboarding procedures to include instructions to employees to ensure exiting employees return their IT assets in accordance with the updated Accountable Property Handbook.

Management Response:

Management concurs. The NCUA will revise offboarding procedures to align with the updated Accountable Property Handbook by September 30, 2026.

Recommendation #3

Improve the IT asset accountability process going forward to include historical IT asset tracking by employee and by addressing and implementing data access procedures for returned cell phones on litigation holds.

Management Response:

Management concurs. NCUA management will review processes and implement procedures by September 30, 2026, consistent with agency business needs and retention schedules.

1775 Duke Street – Alexandria, VA 22314-6113 – 703-518-6320



Page 2

cc: Acting Chief Information Officer Amber Gravius
Acting Deputy Chief Information Officer Dave Matheu



Appendix C

Acronyms and Abbreviations

Acronym	Term
DPFM	Division of Procurement and Facilities Management
E&L	Enforcement and Litigation Division
IT	Information Technology
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General