# NATIONAL CREDIT UNION ADMINISTRATION CYBERSECURITY AUDIT

**Report #OIG 23-05**
**May 2, 2023**

**Office of Inspector General**

SENT BY EMAIL

**TO:** Distribution List

**FROM:** Inspector General James W. Hagen

**SUBJ:** National Credit Union Administration CyberSecurity Audit

**DATE:** May 2, 2023

Attached is the Office of the Inspector General's audit of the National Credit Union Administration's (NCUA) cybersecurity controls related to its firewall and audit logging security technologies.

The OIG engaged CliftonLarsonAllen LLP (CLA) to perform this audit.[1] The contract required that this audit be performed in conformance with generally accepted government auditing standards issued by the Comptroller General of the United States. The OIG monitored CLA's performance under this contract.

This report summarizes the results of CLA's audit and contains four recommendations that will assist the agency in strengthening cybersecurity controls related to its firewalls and the SIEM tool. NCUA management concurred with and has taken or planned corrective actions to address the recommendations.

We appreciate the effort, assistance, and cooperation NCUA management and staff provided to us and to CLA management and staff during this engagement. If you have any questions on the report and its recommendations, or would like a personal briefing, please contact me at 703-518-6350.

[1] CLA is an independent certified public accounting and consulting firm.

Distribution List:
Chairman Todd M. Harper
Board Vice Chairman Kyle S. Hauptman
Board Member Rodney E. Hood
Executive Director Larry Fazio
General Counsel Frank Kressman
Deputy Executive Director Rendell Jones
Chief of Staff Catherine Galicia
OEAC Deputy Director Samuel Schumach
Chief Information Officer Robert Foster
Senior Agency Information Security/Risk Officer David Tillman
Cybersecurity Advisor and Coordinator, Todd Finkler

Attachment

# National Credit Union Administration

# Cybersecurity Audit

# Final Report

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

CliftonLarsonAllen LLP
CLAconnect.com

Inspector General
National Credit Union Administration

CliftonLarsonAllen LLP (CLA) was engaged by the National Credit Union Administration's (NCUA) Office of Inspector General (OIG) to conduct a performance audit of the NCUA's cybersecurity controls related to its firewall and audit logging security technologies.

The objective of our performance audit was to assess the effectiveness of the NCUA's firewalls and Security Information and Event Management (SIEM) solution to determine if they are designed and implemented to prevent and detect cybersecurity threats to the NCUA's network.

For this audit, we reviewed the following:

- NCUA's network firewalls to determine if they are designed to monitor incoming and outgoing network traffic to prevent unauthorized access to the NCUA's network, systems, and data, and the exfiltration of the NCUA's data.
- NCUA's SIEM solution (b) (7)(E) to determine if it is designed to collect and analyze information generated by network devices for the purpose of identifying and responding to vulnerabilities and potential internal and external cybersecurity threats before they can disrupt agency operations.

Audit fieldwork covered NCUA's Headquarters located in Alexandria, VA, from October 19, 2022, to March 16, 2023. The scope of the audit covered the period from October 19, 2022, through March 16, 2023.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

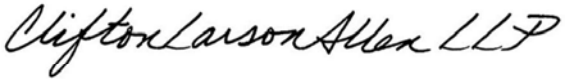
We concluded that overall NCUA adequately designed and implemented its firewall and SIEM security technologies to prevent and detect cybersecurity threats. However, NCUA needs to enhance its implementation of a subset of controls to strengthen the effectiveness of the cybersecurity prevention and detection capabilities these technologies provide. Specifically, we noted weaknesses related to account recertification processes for privileged users with access to cybersecurity tools and controls around the SIEM tool audit logging, visibility, and retention processes. As a result, we are making four recommendations to assist NCUA in strengthening cybersecurity controls related to its firewalls and the SIEM tool.

We considered internal controls that were significant and relevant to our audit objective and therefore, we may not have identified all the internal control deficiencies with respect to the NCUA's firewalls and SIEM cybersecurity controls that existed at the time of this audit. In addition, our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. CLA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their status. The information included in this report was obtained from NCUA on or before April 26, 2023. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to April 26, 2023.

The purpose of this audit report is to report on our assessment of the NCUA's firewalls and SIEM solution and is not suitable for any other purpose.

Additional information on our findings and recommendations are included in the accompanying report. We provided this report to the NCUA OIG.

**CliftonLarsonAllen LLP**



Arlington, Virginia
April 26, 2023

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

The National Credit Union Administration's (NCUA) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct a performance audit of the NCUA's cybersecurity controls related to its firewall and audit logging security technologies.

The objective of our performance audit was to assess the effectiveness of the NCUA's firewalls and Security Information and Event Management (SIEM)[1] solution to determine if they are designed and implemented to prevent and detect cybersecurity threats to the NCUA's network.

The *Executive Order on Improving the Nation's Cybersecurity* (Executive Order (EO) 14208), issued on May 12, 2021, highlighted that "[t]he United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy." In addition, EO 14028 states "[t]he Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors."

NCUA indicated that "[b]ecause of vulnerabilities within the credit union industry and the broader financial system to potential cyberattacks, cybersecurity is one of the NCUA's top supervisory priorities and a top-tier risk under the agency's enterprise risk-management program."[2] NCUA also indicated that its "approach to agency cybersecurity is founded on the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, which guides and constrains how network boundaries, mobile and fixed end points (e.g., an iPhone or computer), and data are provisioned, managed and protected. The Cybersecurity Framework requirements are reinforced by Executive Order 14208."[3]

We conducted this performance audit in accordance with generally accepted government auditing standards. 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Audit Results

We concluded that overall NCUA adequately designed and implemented its firewall and SIEM security technologies to prevent and detect cybersecurity threats. However, NCUA needs to enhance its implementation of a subset of controls to strengthen the effectiveness of the cybersecurity prevention and detection capabilities these technologies provide. Specifically:

- The NCUA needs to enhance the account recertification process for privileged users.

[1] A Security Information and Event Management (SIEM) is an IT security tool that helps organizations collect and analyze information generated by network devices in real-time for the purpose of detecting, identifying, and responding to vulnerabilities and potential internal and external cybersecurity threats before they can disrupt agency operations..

[2] https://ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources

[3] As stated on page 28 of https://ncua.gov/files/publications/budget/budget-justification-2022.pdf

  - Accounts that have access to cybersecurity devices such as firewalls and the SIEM tool were not periodically recertified to determine whether accounts are still needed. The *NCUA Information Security Procedural Manual* requires the review of accounts for compliance with account management requirements at least quarterly.

- The NCUA needs to strengthen its SIEM tool audit logging and collection, visibility, and retention processes. Specifically, the NCUA needs to implement the following logging requirements specified in the Office of Management and Budget (OMB) Memorandum 21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*:

  - Ingesting all required basic logging categories into its SIEM.
  - The capacity for data storage for required minimum logging data retention periods.

These weaknesses are inconsistent with the Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government* (the Green Book)[4] which requires management to:

- Design control activities to achieve objectives and respond to risks; and

- Design the entity's information system and related control activities to achieve objectives and respond to risks.

As a result, we are making four recommendations to assist NCUA in strengthening cybersecurity controls related to its firewalls and the SIEM tool. The following section provides a detailed discussion of the audit findings. Appendix I provides background information on NCUA, Appendix II describes the audit objective, scope, and methodology, and Appendix III includes management's comments.

[4] See principles 10 and 11 in the Green Book.

# Audit Findings

## 1. The NCUA Needs to Enhance the Account Recertification Process for Privileged Users

NCUA did not recertify accounts that have access to cybersecurity devices such as firewalls and the SIEM tool. Management indicated that NCUA's quarterly recertification of user access does not include review of privileged accounts with access to cybersecurity devices such as firewall and SIEM tools due to the low turnover rate of and infrequent role changes for privileged users. This is inconsistent with the *Green Book* [5] which requires management to design control activities to achieve objectives and respond to risks.

NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, control AC-2, Account Management requires organizations to review accounts for compliance with account management requirements at an organization-defined frequency.

The *NCUA Information Security Procedural Manual*, dated November 2018, requires the review of accounts for compliance with account management requirements at least quarterly.

Over time, modifications to a privileged user's access can expand, providing unrestricted access across multiple network and system resources. By performing a periodic review of privileged access to cybersecurity devices, NCUA can decrease the risk of unauthorized and unrestricted access to critical data and resources which can lead to unapproved hardware or software configuration changes, modification of system accounts, or breaches of sensitive NCUA data. Specifically, the quarterly recertifications could identify and correct a privileged user's expanded access to modify firewall rules that could allow paths of entry for malicious actors to the NCUA network.

To assist the NCUA in enhancing the account recertification process for privileged users, we recommend that NCUA management:

**Recommendation 1:** *Include in its quarterly review process, privileged accounts with access to cybersecurity devices such as firewalls and the SIEM tool.*

**Agency Response:**
The NCUA agrees and has already taken corrective action by adding privileged accounts to our quarterly review process.

**OIG Response:**
We concur with the action management indicated it has taken. During the follow-up process, we will review the updated policy and evidence of implementation before closing the recommendation.

[5] See principle 10 in the Green Book.

## 2. The NCUA Needs to Strengthen its SIEM Tool Audit Logging Collection, Visibility, and Retention Processes

NCUA has not fully implemented audit logging requirements. Specifically, NCUA has not:

- Ingested all required basic logging categories into its SIEM.
- Implemented the capacity for data storage for required minimum logging data retention periods.

In association, NCUA has not fully implemented requirements related to Event Logging (EL) maturity levels (EL1 and EL2) for audit logging in accordance with OMB-mandated timelines. For example,[6] some specific logging requirements NCUA has not met for the EL1 maturity level include the following:

- Basic Logging Categories
  - NCUA has not implemented (b) (7)(E) [redacted]
- Minimum Logging Data
  - NCUA has not implemented (b) (7)(E) [redacted] (b) (7)(E) [redacted] t , not have the capacity for 12 months of Active Storage[7] and for 18 months of Cold Data Storage[8] to meet the required minimum logging data retention periods.
- Event Forwarding
  - NCUA has not implemented (b) (7)(E) [redacted] (b) (7)(E)

This is inconsistent with the *Green Book*[9] which requires management to design the entity's information system and related control activities to achieve objectives and respond to risks.

NIST requires agencies to define their event types for logging, the content of audit log data, and audit log retention requirements.[10]

OMB Memorandum 21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021), established a maturity model to guide the implementation of requirements across four Event Logging (EL) tiers shown in the table below that are designed to – over time, help agencies prioritize their efforts and resources

---

6 As specified in the condition, examples were provided rather than a complete listing of all of the EL0 and EL1 requirements that were not implemented.
7 Audit logs stored within the SIEM tool with the ability for review.
8 Backup of audit records not actively searchable by the SIEM tool without being restored.
9 See principle 11 in the Green Book.
10 NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, Audit and Accountability (AU) controls AU-2, AU-3, AU-4, and AU-6.

to achieve full compliance with requirements for implementation, log categories, and centralized access.[11]

| Event Logging (EL) Tiers | Rating[12] | Description | Due Date (From August 27, 2021) |
|---|---|---|---|
| **EL0** | Not Effective | Logging requirements of highest criticality are either **not** met or are only partially met | |
| **EL1** | Basic | Only logging requirements of highest criticality are met | One year |
| **EL2** | Intermediate | Logging requirements of highest and intermediate criticality are met | 18 months |
| **EL3** | Advanced | Logging requirements for all criticality levels are met | Two Years |

The Office of the Chief Information Officer (OCIO) management indicated there are multiple challenges with ingesting basic logging categories into the SIEM tool, implementing minimum logging data, and implementing log storage capacity as specified in OMB M-21-31. Specifically, the NCUA's current SIEM tool limits the agency's log aggregation and retention capabilities. In addition, OCIO management specified that NCUA has limited access to additional tools, staffing, and funding needed to implement the basic logging categories and capture required minimum logging data. Furthermore, OCIO management indicated that cloud vendors' inability to provide all of the log data has limited NCUA's progress in ingesting all required logs. OCIO management stated they are in the process of completing a risk-based evaluation to select the additional tools and resources needed for strengthening the SIEM tool audit logging collection, visibility, and retention processes.

Enhanced audit logging capabilities can improve the detection, investigation, and remediation of threats, incidents, and vulnerabilities. Centralized audit logs that are well managed and retained for an appropriate amount of time can assist NCUA with monitoring and tracking malicious attacks and security breaches, evaluating system damages, and supporting recovery efforts.

We recommend that NCUA management:

**Recommendation 2:** *Complete the risk-based selection and procurement of additional audit logging tools needed to strengthen audit logging, retention, and visibility to fully implement the minimum logging requirements stipulated in OMB M-21-31.*

**Agency Response:**
The NCUA agrees. The NCUA will complete by December 31, 2024.

**OIG Response:**
While management's targeted completion date is outside of the OMB M-21-31 timelines, we concur with management's planned action.

[11] Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021), created cybersecurity event log requirements for federal departments and agencies to enhance cybersecurity. EO 14028 required the Director of OMB to formulate policies for agencies to establish requirements for logging, log retention, and log management, to ensure centralized access and visibility for the highest-level security operations center of each agency.

[12] The rating is based on whether an agency has implemented or met the specified requirements.

**Recommendation 3:** *Acquire the additional resources needed to fully implement the minimum logging requirements stipulated in OMB M-21-31.*

**Agency Response:**
The NCUA agrees. The NCUA will complete by December 31, 2024.

**OIG Response:**
While management's targeted completion date is outside of the OMB M-21-31 timelines, we concur with management's planned action.

**Recommendation 4:** *Complete implementation of OMB M-21-31 to achieve past due Event Logging 1 and 2 maturity levels and to meet the Event Logging 3 maturity due by August 27, 2023.*

**Agency Response:**
The NCUA agrees. Using a risk-based approach, the NCUA prioritized migration of the SIEM to a cloud-based solution to address log retention constraints and will complete the selection, procurement, and implementation of the SIEM by December 31, 2024, to include meeting implementation requirements in OMB M-21-31.

**OIG Response:**
While management's targeted completion date is outside of the OMB M-21-31 timelines, we concur with management's planned action.

**Appendix I**

# BACKGROUND

## National Credit Union Administration

Created by the U.S. Congress in 1970, the NCUA is an independent federal agency that insures deposits at federally insured credit unions, protects the members who own credit unions, and charters and regulates federal credit unions. The NCUA's operating fund contains the attributes of a revolving fund,[13] which is a permanent appropriation. The NCUA's mission is to "Provide, through regulation and supervision, a safe and sound credit union system, which promotes confidence in the national system of cooperative credit."

NCUA operates under the direction of a three-member Board. The agency is responsible for chartering, examining, supervising, and insuring federal credit unions. It also insures state-chartered credit unions that have applied for insurance and have met National Credit Union Share Insurance requirements.

## Information Technology

The NCUA OCIO is located at the headquarters and provides agency employees, as well as contractors, and state examiners with access to the agency's network. The Chief Information Officer (CIO) has overall responsibility for the agency-wide Information Technology (IT) program, including information security. The agency's Senior Agency Information Security/Risk Officer who reports to the CIO, is charged with developing, maintaining, and implementing the agency-wide information security program.

Employees access the agency's network through agency-owned laptops and iPhones/iPads. The majority of the NCUA's employees work remotely and access the network via the agency's Virtual Private Network (VPN), as do any contractor staff or other employees who may be working remotely. State examiners who perform supervision and examination functions over state-chartered credit unions also access the NCUA network via the VPN. The OCIO also provides

(b) (7)(E) the NCUA has implemented a SIEM to help identify potential cybersecurity threats. A SIEM is an IT security tool used to aggregate system logs and traffic to detect and respond to potential threats. Using a SIEM tool improves network visibility and incident response automation. In addition, the NCUA leverages FireEye to detect and prevent potential threats on endpoints and network traffic. Alarms identified by FireEye are forwarded to the SIEM. The NCUA further secures devices within the network with vulnerability scans and monitoring conducted using Tenable.sc (formerly known as SecurityCenter).

NCUA Offices of Primary Interests (OPIs) use OPI-owned applications that reside on the General Support System computing platform. The platform includes all major IT hardware, software, communications, network storage, central databases, operating systems, and other minor infrastructure, security-related, and productivity applications.

[13] A revolving fund amounts to "a permanent authorization for a program to be financed, in whole or in part, through the use of its collections to carry out future operations."

**Appendix II**

# OBJECTIVE, SCOPE, AND METHODOLOGY

## Objective

The objective of this audit was to assess the effectiveness of the NCUA's firewalls and SIEM solution to determine if they are designed and implemented to prevent and detect cybersecurity security threats to the NCUA's network.

## Scope

We conducted this performance audit in accordance with generally accepted government auditing standards. 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Consistent with our audit objectives, the scope of the audit included assessing and reporting on the effectiveness of the following specific NCUA security technologies and controls for protecting against and detecting cybersecurity threats to the NCUA's network:

- The NCUA's network firewalls to determine if they are designed to monitor incoming and outgoing network traffic to prevent unauthorized access to the NCUA's network, systems, and data, and the exfiltration of the NCUA's data.

- The NCUA's SIEM solution (b) (7)(E) to determine if it is designed to collect and analyze information generated by network devices for the purpose of identifying and responding to vulnerabilities and potential internal and external cybersecurity threats before they can disrupt agency operations.

We considered internal controls that were significant and relevant to our audit objective and determined the following Green Book principles[14] applied:

- Design control activities to achieve objectives and respond to risks; and

- Design the entity's information system and related control activities to achieve objectives and respond to risks.

Audit fieldwork covered NCUA's Headquarters located in Alexandria, VA, from October 19, 2022, to March 16, 2023. The scope of the audit covered the period from October 19, 2022, through March 16, 2023.

[14] Ibid. 4.

**Appendix II**

## Methodology

To determine if the NCUA effectively designed and implemented its SIEM and firewall controls, we performed the following actions:

- Conducted interviews with key NCUA personnel responsible for managing the applicable firewalls and SIEM tool to determine how the agency manages its firewalls and SIEM solution.

- Reviewed documentation supporting how the agency configures, implements, manages, and deploys firewalls and SIEM tools.

- Observed how NCUA manages firewalls and SIEM tools. For example, we observed how NCUA configures firewall rule sets and manages firewall changes. In addition, we observed NCUAs ability to review SIEM alarms and alerts and to query audit logs for incident response capabilities.

- Reviewed NCUA's SIEM tuning and development of use cases for specific activities and evaluated SIEM tool coverage.

- Tested data exfiltration from within the NCUA's network boundaries to assess the effectiveness of the network firewalls.

- Assessed the effectiveness of the firewall settings and analyzed what is permitted.

To conduct this testing, we used the following tools:

- Netcat – Open-source utility for reading and writing data across networks using the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) protocols.

- Nmap – Open-source utility for performing network exploration and security auditing.

- EgressBuster – TrustedSec open-source utility for rapid testing of potential Transmission Control Protocol/Internet Protocol (TPC/IP) service ports which would be open for data communication.

In addition, we used applicable NCUA policies and federal criteria to guide our work in support of the audit. The policies and criteria included, but were not limited to, the following:

- NIST Special Publication 800-41 Revision 1, *Guidelines on Firewalls and Firewall Policy.*

- NIST Special Publication 800-61 Revision 2, *Computer Security Incident Handling Guide.*

- NIST Special Publication 800-94, February 2007, *Guide to Computer Security Log Management.*

- NIST Special Publication 800-115, September 30, 2008, *Technical Guide to Information Security Testing and Assessment.*

**Appendix II**

- NIST Special Publication 800-53 Revision 5, September 2020 (Updated 12/10/2020), *Security and Privacy Controls for Information Systems and Organizations.*

- NIST Special Publication 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations.*

- NIST Special Publication 800-53B, Revision 5*, Control Baselines for Information Systems and Organizations*.

- GAO *Government Auditing Standards*, April 2021.

- GAO *Standards for Internal Control in the Federal Government*, September 2014.

In testing the effectiveness of the security controls, we exercised professional judgment in determining the number of items we selected for testing and the method we used to select them. We considered relative risk and the significance or criticality of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity (not the percentage of deficient items found compared to the total population available for review). In some cases, this resulted in selecting the entire population. However, in cases where we did not select the entire audit population, the results cannot be projected and, if projected, may be misleading.

**Appendix III**

# MANAGEMENT COMMENTS

National Credit Union Administration
Office of the Executive Director

OED/OCIO:jb

**SENT BY EMAIL**

**TO:** Inspector General James Hagen

**FROM:** Executive Director Larry Fazio LARRY FAZIO

**Recommendation #4.** Complete implementation of OMB M-21-31 to achieve past due Event Logging 1 and 2 maturity levels and to meet the Event Logging 3 maturity due by August 27, 2023.

**Management Response:** The NCUA agrees. Using a risk-based approach, the NCUA prioritized migration of the SIEM to a cloud-based solution to address log retention constraints and will complete the selection, procurement, and implementation of the SIEM by December 31, 2024, to include meeting implementation requirements in OMB M-21-31.

1775 Duke Street – Alexandria, VA 22314-6113 – 703-518-6360

**Appendix III**



The NCUA has documented the outstanding requirements to achieve the maturity levels set forth by OMB in an acceptance of risk (AOR). The AOR includes a detailed explanation of the need for risk acceptance and the compensating controls used to mitigate risk during the period of exposure.

Please contact Deputy Executive Director (DED) Rendell Jones if you have any questions.

cc: NCUA Board Members
DED Jones
OCIO Director Rob Foster