NCUA
National Credit Union Administration

OFFICE OF INSPECTOR GENERAL

AUDIT OF THE NCUA'S CONTINUITY OF OPERATIONS PROGRAM

Report #OIG-22-09
12/30/2022

Office of Inspector General

TO: Distribution List

FROM: Inspector General James W. Hagen

SUBJ: Audit of the NCUA's Continuity of Operations Program

DATE: December 30, 2022

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) conducted this self-initiated audit to assess the NCUA's Continuity of Operations (COOP) program. Our objectives were to determine whether the NCUA's COOP program was: (1) in accordance with applicable laws, regulations, policies, and procedures and (2) ready and able to execute should the need arise. The scope of our audit covered all COOP program activities from January 1, 2018, through December 31, 2021.

Our audit determined the NCUA's COOP program is operating in accordance with applicable laws, regulations, policies, and procedures and that it is ready and able to execute should the need arise. However, we also identified several areas that need improvement. Specifically, we determined the NCUA should perform a full failover test of its IT network to ensure management is made aware of any potential weaknesses and correct them, as necessary. We also determined that the Office of Continuity and Security Management (OCSM) and the Office of the Chief Information Officer (OCIO) need to improve communication with each other regarding COOP and security matters. We are making four recommendations in our report 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 and its recommendations, please contact me at 703-518-6350.

Distribution List:
Chairman Todd M. Harper
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 D. Galicia
OEAC Director Elizabeth Eurgubian
OCSM Director Kelly Gibbs
OCIO Director Rob Foster

Attachment

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) conducted this self-initiated audit to assess the NCUA's Continuity of Operations (COOP) program. Our objectives were to determine whether the NCUA's COOP program was: (1) in accordance with applicable laws, regulations, policies, and procedures and (2) ready and able to execute should the need arise. The scope of our audit covered all COOP program activities from January 1, 2018, through December 31, 2021.

Our audit determined the NCUA's COOP program is operating in accordance with applicable laws, regulations, policies, and procedures and that it is ready and able to execute should the need arise. Specifically, we determined the NCUA took actions to ensure the NCUA is complying with applicable laws and regulations and that it was consistently aware of disasters and potential threats that faced the agency. However, based on our audit work, we believe the NCUA should perform a full failover[1] test of its IT network to ensure management is made aware of any potential weaknesses and correct them, as necessary. In addition, we determined that the Office of Continuity and Security Management (OCSM) and the Office of the Chief Information Officer (OCIO), which are the two main NCUA offices involved in the COOP and security matters, should work to improve communication between each other regarding these matters. We are making four recommendations in our report to address the issues we identified.

We appreciate the cooperation and courtesies NCUA management and staff provided to us during this audit.

[1] Failover is the capability to switch over automatically (typically without human intervention or warning) to a redundant or standby system upon the failure or abnormal termination of the previously active system. (NIST SP 800-53, Rev.5)

BACKGROUND

The NCUA is an independent federal agency created by the U.S. Congress to regulate, charter, and supervise federally insured credit unions (FICU). The NCUA's organizational structure consists of a Headquarters, Asset Management and Assistance Center, and three regional offices.[2]

NCUA's Office of Continuity and Security Management

The mission of the agency's OCSM is to promote confidence in the credit union system by establishing policy and directing agency operations to analyze and share classified information on threats to the agency and to detect, deter, and mitigate insider threats, prepare for and respond to emergencies, protect NCUA personnel and critical infrastructure, screen employees, contractors, and affiliates to work for, or on behalf of, the NCUA, and provide preparedness and security training for all NCUA staff.

The OCSM is responsible for the continuity of operations and emergency management, physical security at NCUA facilities, personnel security, and national security and intelligence activities. OCSM provides a link between the intelligence community and the credit union system by managing NCUA's threat analysis processes and working with the intelligence community and other partners to provide information on threats to the credit union system. OCSM also manages the agency's pandemic response plan, which includes monitoring public health indicators.

Laws, Guidance and Policy Relevant to the COOP Plan

Presidential Policy Directive 40 (PPD-40),[3] National Continuity Policy, directed the Secretary of Homeland Security through the Administrator of the Federal Emergency Management Agency (FEMA) to coordinate the implementation, execution, and assessment of continuity activities among executive departments and agencies. The Administrator of FEMA was directed to develop and promulgate Federal Continuity Directives to establish continuity program and planning requirements. FEMA issued *Federal Continuity Directive 1 and Federal Continuity Directive 2* in 2017.[4] In May 2020, FEMA issued *a Guide to Continuity Program Management*.

[2]The three regional offices are the Eastern, Southern, and Western regions. However, for part of our audit's scope period, the NCUA operated five regional offices, regions 1 through 5. The agency closed two of those offices at the end of 2018, and the current three-region structure became effective on January 7, 2019.
[3] On July 15, 2016, the President signed PPD-40, National Continuity Policy, which replaced National Security Presidential Directive (NSPD-51)/Homeland Security Presidential Directive (HSPD-20) and the National Continuity Policy Implementation Plan (NCPIP), addressing lessons learned, best practices, and the integrating of new technologies and processes since 2007.
[4] Federal Continuity Directive 1, U.S. Department of Homeland Security, Federal Emergency Management Agency (Jan. 17, 2017); Federal Continuity Directive 2, U.S. Department of Homeland Security, Federal Emergency Management Agency (June 13, 2017).

The National Essential Functions (NEFs) are the focal point of all continuity programs and capabilities and represent the overarching responsibilities of the Federal Government to lead and sustain the Nation before, during, and in the aftermath of a catastrophic emergency. The NEFs:

1. Ensure the continued functioning of our form of government under the United States Constitution, including the functioning of three separate branches of government.

2. Provide leadership visible to the Nation and the world and maintain the trust and confidence of the American people.

3. Defend the United States against all enemies, foreign and domestic and prevent or interdict attacks against the United States or its people, property, or interest.

4. Maintain and foster effective relationships with foreign nations.

5. Protect against threats to the homeland and bring to justice perpetrators of crimes of attacks against the United States or its people, property, or interests.

6. Provide rapid and effective response to and recovery from the domestic consequences of an attack or other incident.

7. Protect and stabilize the Nation's economy and ensure public confidence in its financial systems; and

8. Provide for Federal Government services that address the national health, safety, and welfare needs of the United States.

The NCUA is responsible for supporting NEF 7: "Protecting and stabilizing the nation's economy and ensuring public confidence in its financial systems." On June 1, 2009, the White House further assigned certain agencies Primary Mission Essential Functions (PMEFs) in support of these NEFs. The NCUA was assigned a PMEF to "Ensure public confidence in the Nation's credit unions by maintaining continuous system-wide liquidity and preserving member access to funds and services." The NCUA supports NEF 7 by executing the duties and responsibilities for its PMEF through its four Mission Essential Functions (MEFs) or essential functions) as follows:

1. Ensure emergency liquidity to individual credit unions and the National Credit Union Share Insurance Fund (NCUSIF).

2. Communicate with the public and credit unions regarding the NCUA's response activities and respond to related inquiries.

3. Supervise impacted credit unions and monitor and report on issues.

4. Manage liquidation of credit unions.

The NCUA has five Essential Supporting Activities (ESAs) that it considers critical to the continued execution of its MEFs. They are as follows:

- Manage the NCUA workforce.
- Manage the NCUA's security and continuity of operations activities.
- Share information on credit union operational status and on potential threats and mitigation strategies.
- Manage the NCUA's critical financial resources, contracting, and facilities.
- Manage the NCUA's IT systems required to support the NCUA's MEFs and ESAs.

The NCUA must continuously perform its essential functions during COOP plan activation or resume them within 12 hours of an event and must maintain them until it can resume normal operations. The NCUA's prioritization of essential functions will depend on the scope and impact of the event.

The NCUA COOP plan[5] provides that in support of the NCUA's essential functions, the agency will plan, establish necessary capabilities, and be prepared to perform its MEFs and ESAs with little or no warning under any operating conditions. It is the NCUA's policy that all continuity planning and programming will:

- Be based on the assumption that warnings of threats may not be received.
- Ensure the safety of all NCUA personnel to successfully perform the mission.
- Leverage the permanent and routine geographic distribution of leadership, staff, and infrastructure to maintain uninterrupted capability to accomplish essential functions.
- Maximize the use of technology to provide information to staff and other users, facilitate decision making, maintain situational awareness, and issue orders and direction.
- Leverage telecommuting (telework) capabilities to better ensure continued operation in all hazard conditions; and,
- Integrate threat warning, critical infrastructure protection, information assurance, and operations security, as appropriate.

The NCUA's continuity objectives are to:

[5] NCUA Instruction 9901.1 NCUA Continuity of Operations Plan, September 3, 2014, with attached 2019 Plan.

- Ensure the safety of staff, contractors, and visitors.
- Minimize property damage and loss.
- Ensure the NCUA can perform its MEFs and ESAs under all conditions.
- Designate positions as Essential Continuity Positions (ECPs) and execute a successful order of succession with accompanying authorities in the event members of the NCUA leadership team are incapacitated.
- Recover and reconstitute from an emergency with minimal disruption to NCUA staff and programs.
- Ensure and validate continuity readiness through a dynamic and integrated continuity test, training, and exercise program and operational capability.

The NCUA has a mobile workforce, regional distribution of staff, and an information system located outside the Washington, DC metropolitan area. Over 70 percent of personnel (not including contractors) are in the field and conduct duties that are mobile in nature. Of the employees assigned directly to the Central Office or regional offices, 13 percent perform at least 75 percent of their work in a remote location. In addition, the majority of NCUA personnel are approved for, and have the full capability to telework, as needed.

The Continuity of Operations Plan is divided into phases. Phase one is Readiness and Preparedness, which documents the agency's ability to respond to an incident. Phase two is COOP plan Activation, which involves the NCUA's Executive Director (ED) or Southern Region Director activating the COOP plan whenever the NCUA or federal government deems a situation worthy of action. Phase three is Operations, where the COOP plan provides the process for attaining the operational capability to perform its PMEF and essential functions within 12 hours and sustaining those operations until normal operations resume. The fourth and final phase is Reconstitution, which is the reconstituted staff, equipment, and documents are in place at the new or restored Central Office. The following are the responsibilities for the OCSM and OCIO as they pertain to the COOP plan:

OCSM

- Director of OCSM serves as the NCUA's Continuity Coordinator.
- Conducts an annual review of COOP plan and capabilities.
- Maintains working knowledge of all COOP-related regulations and directives and briefs agency staff as necessary.

- Reviews, updates, and maintains the NCUA's essential functions.
- Plans and conducts all COOP training, testing, and exercises.
- Assesses risk to the NCUA and the credit union system from potential COOP situations and provides information to the ED and Emergency Response Group (ERG), as necessary.
- Manages, tests, and updates the NCUA's secure communications and facilities, as required in accordance with the Office of Science and Technology Policy/Office of Management and Budget Directive D-16-1 (OSTP/OMB Directive D-16-1) Minimum Requirements for Federal Executive Branch Continuity Communications Capabilities.
- Serves as a resource to the ED and ERG during an emergency.
- Maintains the Incident Management System (IMS), including testing, updates, and instructions.
- Maintains the OCSM SharePoint site, which serves as a repository for continuity-related guidance, information, and program updates.

OCIO

- Executes the Critical IT Systems ESA.
- Conducts regular disaster recovery exercises; and
- Ensures all vital NCUA voice and data circuits are enrolled in the Department of Homeland Security, Office of Emergency Communication's Telecommunications Service Priority (TSP) program.

In addition to the COOP plan, the NCUA has a Devolution Plan that supports the overall NCUA COOP plan to ensure the continuation of the agency's essential functions in the event the Central Office or a Regional Office is inaccessible or the ED, ERG members, and ECP staff are incapacitated or otherwise unavailable. If these circumstances exist, operational responsibility will devolve (transfer) from the ERG to the Devolution Emergency Response Group (DERG). The NCUA also has an alternate site in the event of a disaster for information technology and secure communications.

The NCUA COOP Test, Training, and Exercise (TT&E) Program[6] is used to provide the standards and processes needed to improve NCUA's capabilities to perform essential functions during all hazards. This program measures the agency's preparedness for a COOP plan event, and its capability to continually execute essential functions during and after COOP plan

[6] NCUA Instruction 9901.2 Continuity of Operations Test, Training and Exercise Program, September 3, 2014.

activation. As such, the overall goals of the TT&E Program are to improve mission readiness and mission assurance. Specific objectives of this program include:

- Review and validate NCUA COOP plans, policies, and procedures.
- Ensure NCUA personnel are familiar with alert, notification, response, and deployment procedures during any continuity event – including natural or man-made disasters.
- Ensure NCUA personnel are sufficiently trained to carry out agency mission essential functions when teleworking or deployed at an alternate COOP site.
- Exercise procedures by deploying designated personnel and equipment to a teleworking or COOP site.
- Ensure backup data and records required to support essential functions at COOP facilities are sufficient, complete, and current.
- Test and validate equipment to ensure both internal and external interoperability.
- Ensure NCUA personnel understand the procedures to reconstitute from COOP operations and transition to normal activities when appropriate.

The NCUA established an Essential Continuity Records (ECR) management program[7] as part of the COOP program and it has the following objectives:

(a) Provide access to the information the NCUA needs to conduct its PMEF, MEFs, and ESAs during an emergency or disaster and

(b) Identify and protect the records necessary to accomplish the NCUA's continuing essential functions and resumption of normal operations during an emergency or disaster and protect the legal and financial rights of the government and citizens.

[7] NCUA Instruction 9901.3 (Rev.1), Essential Continuity Records Management Program, April 24, 2019.

RESULTS IN DETAIL

The objectives of our audit were to determine whether the NCUA's COOP program was: (1) in accordance with applicable laws, regulations, policies, and procedures; and (2) ready and able to execute should the need arise.

Based on our audit work, we determined that the NCUA's COOP program is operating in accordance with applicable laws, regulations, policies, and procedures, and it is ready and able to execute should the need arise. However, based on the results of our audit work, we believe there are two areas that need attention. Specifically, the NCUA needs to: (1) conduct a full failover test on its IT network to identify any potential weaknesses before they cause a disruption; and (2) communication between certain NCUA offices involved with the COOP program needs improvement. The detailed results of our audit follow.

The NCUA Needs Failover Testing

The NCUA's testing efforts of its disaster recovery capabilities need improvement. Specifically, OCIO needs to perform full failover testing of its IT network to identify any weaknesses in its ability to recover from a network outage. NCUA Instruction 9901 (Rev. 1), COOP policy, requires NCUA's OCIO to manage the NCUA's IT systems required to support the NCUA's MEFs and ESAs. Furthermore, the Federal Information Security Modernization Act of 2014 (FISMA) requires the agency's CIO to establish and maintain plans and procedures to ensure continuity of operations for IT systems that support the operations and assets of the agency. Due to resource limitations and unwarranted concerns, OCIO currently only performs limited failover testing on portions of the agency's network and systems and, has never performed a full-scale failover test due to the expectation that performing such a test would cause an agency-wide loss in productivity. As a result, the NCUA does not know exactly where its IT systems and network are potentially weak in its capabilities, which does not provide a comprehensive assessment of its disaster recovery capabilities.

Details

The NCUA has five ESAs that are critical to the continued execution of its MEFs, which are as follows:

1. Manage the NCUA workforce.

2. Manage NCUA security and continuity of operations activities.

3. Share information on credit union operational status, and on potential threats and mitigation strategies.

4. Manage NCUA critical financial resources, contracting, and facilities.

5. Manage NCUA IT systems that are required to support NCUA's MEFs and ESAs.

Expectations/Recovery Time Objectives: The NCUA's COOP plan provides the process for attaining the operational capability to perform its PMEF and essential functions within 12 hours and sustaining those functions for at least 30 days or until normal operations resume. Additionally, the agency's alternate site has been equipped with communications, systems, equipment, and resources to sustain continuity operations for at least 30 days or until normal operations resume.

2022 NCUA Annual Performance Plan

One of the NCUA's strategic goals is "maximizing organizational performance to enable mission success." For the NCUA to achieve this goal, effective communication, collaboration, and coordination by all staff across all offices within the agency are essential. The NCUA must be effective in its administration of human capital, employee and operational security, data, information technology systems and assets, financial management, and employee engagement.

Current Practices

- OCIO currently conducts tabletop exercises[8] and disaster recovery drills to meet the requirements for FISMA and related statutes.
- OCSM conducts annual assessments of the COOP plan and makes any necessary changes, as do other offices for their sections of the COOP plan.
- OCSM conducts the Eagle Horizon[9] exercises annually to test the agency's preparedness in the event of a disaster.
- OCIO currently conducts limited failover tests in the following areas:
    - All infrastructure networks (internal and external (inter-site telecommunication circuits)
    - Platforms
    - Business productivity applications (Active Directory, M365 apps)

[8] A tabletop exercise is a discussion-based event where personnel with roles and responsibilities specified in an IT plan, validate the content of the plan by discussing their roles during an emergency and their response to a particular emergency situation. NIST SP 800-84.
[9] The National Continuity Policy requires all federal agencies to participate in the annual Eagle Horizon Continuity of Operations exercise, with the goal of demonstrating and assessing the ability of both federal and non-federal government organizations to implement continuity plans and, perform essential functions appropriate for incident conditions to sustain NEFs.

- Business systems/services (e.g., MERIT[10])
- Web services (ncua.gov)

- Only segments that are tested are shut down and failover is tested between sites.
  - Not all systems and services are replicated but all users route through disaster recovery for authentication currently.

During our audit, an OCIO management official indicated that OCIO had not conducted a failover test for the NCUA's entire IT network to expose any unknown weaknesses. The same official noted that there are questions about which IT systems should have failover capability in the event of a disaster (in which the primary system/network would automatically switch to a standby system) and how to best conduct testing on those systems. The official told the OIG that it is one thing to be compliant but another to be prepared. While not within the scope of our audit, during fieldwork we observed that on June 7, 2022, the NCUA experienced an unexplained agency-wide network outage due to system weaknesses that had not been discovered through the limited failover testing that OCIO had performed. The outage left NCUA staff without access to the entire network and systems for hours, which resulted in a loss of employees' productivity.

Performing a full failover test of the agency's entire IT network would validate backups and replication to minimize data loss and downtime. At a minimum, such a test would be performed on agency programs that support mission-essential functions. The NCUA would need to have a written test plan and would produce a report of findings and conclusions after the test. Although conducting a failover test of the NCUA's network is something that the OCIO could perform, doing so depends on resources and expectations. OCIO officials advised us they are planning to move systems authentication/authorization to the cloud in the future, which will make failover capabilities easier for the agency. We believe an annual failover test should be performed and graded during the annual FISMA audit. Currently, the agency uses tabletop exercises and limited failover tests rather than a full failover test of the network during the annual FISMA audit to meet the requirement of the statute and to determine readiness from a COOP and disaster recovery standpoint for the IT systems.

To ensure NCUA management is aware of all potential weaknesses in its IT network and systems, we are making the following three recommendations.

Recommendations

We recommend NCUA management:

[10] MERIT is the NCUA's examination platform designed to provide improvements to streamline the examination process for credit unions and examiners. MERIT replaced NCUA's previous examination system in the fall of 2021.

1. Perform a business impact analysis to define the IT network as essential and determine timelines for restoration to be used as a measurement for a full failover test of the NCUA IT network.

Management Response

Management agreed with our recommendation. Management has already begun this effort and will ensure the IT network is explicitly identified as essential as part of the update of the business impact analysis. Management estimated a completion date of December 31, 2023.

OIG Response

We concur with Management's planned actions.

2. Ensures the Chief Information Officer plans, conducts, and reports on a full failover test of the NCUA's IT network to identify and correct any identified weaknesses.

Management Response

Management agreed with our recommendation. Management will update NCUA's related procedures to require a full failover test and conduct an initial full failover test of the NCUA's IT network by December 31, 2024.

OIG Response

We concur with Management's planned actions.

3. Ensures the results of the failover test from Recommendation 2. (above) are communicated in writing to the NCUA Board, the Office of the Executive Director, and the Director, Office of Continuity and Security Management, to ensure the agency's Continuity of Operations program and disaster recovery capabilities are thoroughly managed and reported on.

Management Response

Management agreed with our recommendation. Management will update their related procedures and require them to be inputted by December 31, 2023.

OIG Response

We concur with Management's planned actions.

More Open Communication Needed Among Offices

Our audit determined that OCIO needs to inform OCSM about the results of IT system testing, including system functionality and other capabilities. Currently, OCSM officials learn little from OCIO officials about NCUA's disaster recovery capabilities. OCSM officials need more detailed information regularly communicated to them such as: a) dates and results of disaster recovery drills, b) lessons learned from drills and network tests, and c) status of network resiliency. We learned during our audit that OCIO does not involve other offices when conducting system tests and does not share results or details on any lessons learned from their tests. Because OCSM is the office that has safety and security responsibilities, OCIO should share testing information with OCSM. This would be consistent with the NCUA's value of transparency, defined to be open, direct, and frequent in communications. The lack of communication between OCIO and OCSM is not consistent with this value, and we believe it results in NCUA not being as prepared as it could be should there ever be a disaster.

Details

GAO's Standards for Internal Control in the Federal Government[11] provide the following principles associated with communication.

- Principle 3 - Establish Structure, Responsibility, and Authority
    - As part of establishing an organized structure, management considers how units interact to fulfill their overall responsibilities. Management establishes reporting lines within an organizational structure so that units can communicate the quality information necessary for each unit to fulfill its overall responsibilities. Reporting lines are defined at all levels of the organization and provide methods of communication that can flow down, across, up, and around the structure.
- Principle 14 - Communicate Internally
    - Management should internally communicate the necessary quality information to achieve the entity's objectives.
    - The following attributes contribute to the design, implementation, and operating effectiveness of this principle:
        - Communication throughout the entity
        - Appropriate methods of communication

[11] GAO Standards for Internal Control in the Federal Government, "Control Environment" at p. 28 and "Information and Communication" at p. 60 (Sept. 2014).

OCSM is responsible for managing and reporting the COOP plan for the NCUA. Part of that responsibility includes reporting on the availability of NCUA's disaster recovery capabilities, which includes the agency's IT systems. OCSM officials told us one challenge they face is their lack of technical expertise to evaluate the true functionality of NCUA's disaster recovery capabilities. Although OCSM officials coordinate with other offices in identifying critical IT systems and acceptable down times, it is OCIO alone that is responsible for ensuring the network and its systems are available. OCSM officials explained to us that they receive assurances from OCIO officials that the disaster recovery capability is functional, but do not receive additional detail. In addition, OCSM staff explained that the OCIO's role is a key component in the COOP program, but that OCIO also has a disaster recovery plan separate from the COOP plan. OCSM staff noted this is the reason why they need to regularly connect with OCIO officials, so that everyone can fully understand their role in disaster recovery.

OCIO management said that they have little to no communication with OCSM officials regarding tabletop exercises because OCIO has been limited in its involvement with those exercises. Rather, OCIO performs its own separate tabletop exercises. In addition, an OCIO management official said that the OCIO aimed to integrate the COOP plan and the disaster recovery plan but have not yet connected the plans. The OCIO official explained they planned to integrate the two areas in 2019 but demands from the COVID-19 pandemic impacted the timing of the integration.

The OCIO official also explained that when OCIO performs its own tabletop exercises, the focus is on OCIO's immediate area of responsibility, so it does not invite OCSM or other offices to participate. However, this same official indicated offices that have interest in the results would benefit from being included in OCIO's tabletop exercise/drills. An OCSM staff told us that given the OCSM's role in disaster recovery they should receive, at a minimum, the results from the OCIO's tabletop exercises/drills for disaster recovery so they can also see how long it takes to recover the network and its systems. An OCIO official agreed and said that they should make it a point to involve OCSM in OCIO's tabletop exercises/drills for disaster recovery.

To ensure the NCUA is prepared for a disaster and that the agency's disaster recovery capabilities are as strong as they can be, we are making the following recommendation.

Recommendation

We recommend NCUA management:

4. Ensures OCIO management shares all necessary NCUA IT network, systems, disaster recovery information and details with the Director of OCSM, including dates and results of the OCIO's tabletop exercises and other disaster recovery drills, such as failover tests.

Management Response

Management agreed with our recommendation. Management has already begun sharing applicable information and will update related procedures and require this action by December 31, 2023.

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 2021 Annual Work Plan. Specifically, our objectives were to determine whether the NCUA's COOP program was: (1) in accordance with applicable laws, regulations, policies, and procedures; and (2) ready and able to execute should the need arise.

To accomplish our audit, we performed fieldwork with information relevant to the NCUA's COOP program and disaster recovery plan obtained from various NCUA sources. The scope of this audit covered all COOP activities from January 1, 2018, through December 31, 2021. To achieve our objective, we:

- Reviewed laws relevant to the COOP.
- Reviewed NCUA's policies and procedures related to COOP.
- Interviewed OCIO and OCSM staff and management.
- Reviewed the FEMA review for the NCUA's COOP plan.
- Reached out to the NCUA's Regions regarding their use of the COOP plan.
- Reviewed other COOP-related documentation.
- Reviewed the NCUA's annual risk assessments for the COOP plan.
- Evaluated internal controls.

We conducted this audit from December 2021 through November 2022 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We assessed the effectiveness of the internal controls and determined they were significant to the audit objective. Specifically, we assessed 4 of the 5 internal control components and 7 of the 17

associated underlying principles defined in the Government Accountability Office's Standards for Internal Control in the Federal Government.[12]
We summarize in Table 2 below the components and principles we assessed.

Table 2: Internal Control Components and underlying Principles Assessed

Component: Control Environment	
	Principle #3 – Establish Structure, Responsibility and Authority
Component: Risk Assessment	
	Principle #7 – Identify, Analyze, and Respond to Risks
Component: Control Activities	
	Principle #10 – Design Control Activities
	Principle #11 – Design Information System
	Principle #12 – Implement Control Activities
Component: Information and Communication	
	Principle #13 – Use Quality Information
	Principle #14 - Internally Communicate

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

[12] The Standards for Internal Control in the Federal Government organizes internal control through a hierarchical structure of 7 components and 17 principles. The five components, which represent the highest level of the hierarchy, consist of the Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. The 17 principles support the effective design, implementation, and operation of the components, and represent the requirements for establishing an effective internal control system.

Appendix B

NCUA MANAGEMENT RESPONSE

National Credit Union Administration
Office of the Executive Director

TO: Inspector General James Hagen

FROM: Executive Director Larry Fazio LARRY FAZIO Digitally signed by LARRY FAZIO Date: 2022.12.30 10:13:45 -05'00'

SUBJ: Audit of the NCUA's Continuity of Operations Program

DATE: December 30, 2022

We have reviewed the Office of the Inspector General's (OIG) draft audit report titled *Audit of the NCUA's Continuity of Operations Program*. We concur with the four recommendations.

OIG Recommendation 1: Perform a business impact analysis to define the IT network as essential and determine timelines for restoration to be used as a measurement for a full failover test of the NCUA IT network.

Management Response: We agree and have already begun this effort. We will finalize the business impact analysis by December 31, 2023. The NCUA's IT network is treated as essential given systems explicitly identified in the NCUA's Continuity of Operations Program as essential rely on the network to operate. We will ensure the IT network is explicitly identified as essential as part of the update of the business impact analysis.

OIG Recommendation: Ensures the Chief Information Officer plans, conducts, and reports on a full failover test of the NCUA's IT network to identify and correct any identified weaknesses.

Management Response: We agree. Over the last several years, NCUA has invested in enhanced IT network resiliency, including replacing older network switches and routers and migrating certain services to the cloud. We will update our related procedures to require a full failover test and conduct an initial full failover test of the NCUA's IT network by December 31, 2024.

OIG Recommendation: Ensures the results of the failover test from Recommendation 2. (above) are communicated in writing to the NCUA Board, the Office of the Executive Director, and the Director, Office of Continuity and Security Management, to ensure the agency's Continuity of Operations program and disaster recovery capabilities are thoroughly managed and reported on.

Management Response: We agree. We will update our related procedures by December 31, 2023, to require this.

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

OIG Recommendation: Ensures OCIO management shares all necessary NCUA IT network, systems, disaster recovery information and details with the Director of OCSM, including dates and results of the OCIO's tabletop exercises and other disaster recovery drills, such as failover tests.

Management Response: We agree and OCIO has already begin sharing applicable information. We will update our related procedures by December 31, 2023, to require this.

Thank you for the opportunity to comment. If you have any questions regarding this response, please contact Shameka Sutton at (703) 548-2485 or at SSutton@ncua.gov.

Appendix C

ACRONYMS AND ABBREVIATIONS

Acronym	Term
COOP	Continuity of Operations
DERG	Devolution Emergency Response Group
ECP	Essential Continuity Positions
ECR	Essential Continuity Records
ED	Executive Director
ERG	Emergency Response Group
ESA	Essential Supporting Activities
FICU	Federally Insured Credit Union
IMS	Incident Management System
MEF	Mission Essential Function
NCUSIF	National Credit Union Share Insurance Fund
NEF	National Essential Function
NCUA	National Credit Union Administration
OCIO	Office of the Chief Information Officer
OCSM	Office of Continuity and Security Management
OIG	Office of Inspector General
PMEF	Primary Mission Essential Function
PPD-40	Presidential Policy Directive 40
TT&E	Test, Training and Exercise