OFFICE OF INSPECTOR GENERAL

AUDIT OF THE NCUA OFFICE OF NATIONAL EXAMINATIONS AND SUPERVISION OVERSIGHT OF CREDIT UNION CYBERSECURITY PROGRAMS

Report #OIG-19-07
July 31, 2019

National Credit Union Administration

Office of Inspector General

TO: Distribution List

FROM: Inspector General James W. Hagen

SUBJ: Audit of the NCUA Office of National Examinations and Supervision Oversight of Credit Union Cybersecurity Programs

DATE: July 31, 2019

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) conducted this self-initiated audit to determine whether the Office of National Examinations and Supervision (ONES) provides for adequate oversight of its credit unions' cybersecurity programs to assess whether the credit unions are taking sufficient and appropriate measures to protect the confidentiality, availability, and integrity of credit union assets and sensitive credit union data against cyber-attacks.

Results of our audit determined that ONES's examination program provides for adequate oversight of credit union cybersecurity programs. We learned the ONES's examination program includes the NCUA's Automated Cybersecurity Examination Tool (ACET) Maturity Assessment (ACET Assessment) the NCUA implemented effective for 2018. We also learned ONES completed required ACET Assessments of its credit unions during 2018 and plans to complete its remaining ACET Assessments during 2019. Furthermore, we learned the NCUA is in the process of updating its IT examination program for continued and enhanced oversight of its credit unions' cybersecurity programs beyond 2019. As a result, we are not making any recommendations at this time.

We appreciate the effort, assistance, and cooperation NCUA management and staff provided to us during this audit.

Distribution:
Chairman Rodney E. Hood
Board Member J. Mark McWatters
Board Member Todd M. Harper
Executive Director Mark Treichel
General Counsel Michael McKenna
Assistant to the Chairman and Director of External Affairs H. Lenwood Brooks, V
Deputy Executive Director John Kutchey
Director, Office of National Examinations and Supervision Scott Hunt
Director, Office of Examination and Insurance Larry Fazio
Special Advisor to the Chairman for Cybersecurity Johnny E. Davis Jr.

Attachment

TABLE OF CONTENTS

Section **Page**

EXECUTIVE SUMMARY

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) conducted this self-initiated audit to further assess NCUA's Information Technology (IT) examination program.[1] The objective of our audit was to determine whether the Office of National Examinations and Supervision (ONES) provides for adequate oversight of its credit unions' cybersecurity programs to assess whether the credit unions are taking sufficient and appropriate measures to protect the confidentiality, availability, and integrity of credit union assets and sensitive credit union data against cyber-attacks.

Results of our audit determined that ONES's examination program provides for adequate oversight of credit union cybersecurity programs. ONES's examination program includes: (a) the NCUA's Automated Cybersecurity Examination Tool (ACET) Maturity Assessment, (ACET Assessment) which the NCUA implemented effective for 2018; and (b) a supplementary program, which offers its credit unions a selection of voluntary cybersecurity assessments. ONES completed required ACET Assessments of its credit unions during 2018 and plans to complete its remaining ACET Assessments during 2019. Also, ONES provided 23 voluntary assessment reports during the scope period of this audit (2016 through 2018).

In addition, we learned the NCUA is in the process of updating its IT examination program to include continued and enhanced maturity assessments of its credit unions' cybersecurity programs beyond 2019. Specifically, the NCUA's plans include conducting enhanced maturity assessments along with alternate year review work plans that are based on the Center for Internet Security®[2] Controls (CIS Controls™) over a four-year maturity assessment life cycle.[3] NCUA management indicated this modernization will include: enhanced solutions with updated policies, procedures, standards, guidelines, training, supporting technology, and a comprehensive quality assurance and continuous improvement capability. NCUA management believes this approach will ensure the NCUA's ability to consistently identify cybersecurity risk trends required to establish the priorities and scope of future IT examinations. Ultimately, NCUA management believes this will consistently drive the credit unions toward a more robust and resilient security posture.

[1] In 2017, the OIG conducted an audit of the NCUA's IT examination program, addressing the examination of federal credit unions with assets between $250 million and $10 billion under the supervision of the Office of Examination and Insurance.

[2] According to its website, the CIS® "…is a nonprofit organization whose mission is to identify, develop, validate, promote, and sustain best practices in cyber security; deliver world-class cyber security solutions to prevent and rapidly respond to cyber incidents; and build and lead communities to enable an environment of trust in cyberspace."

[3] The trademarked CIS Controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks.

Considering the NCUA requires ONES use the ACET Assessment as the baseline criteria in completing its IT examinations; and the NCUA's plans for updating its IT examination program for continued and enhanced cybersecurity assessments of its credit unions with alternate year reviews based on the CIST Controls, we are not making any recommendations at this time. We may conduct additional reviews of the NCUA's cybersecurity examination program after the agency has incorporated its planned enhancements into its risk-focused examination program.

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

BACKGROUND

NCUA's Risk-Focused Examination Program (RFE)

NCUA uses an RFE program the agency implemented in 2002 "[t]o effectively supervise and examine FICUs…." NCUA Instruction 5000.20 (Examination Scope) establishes requirements for federally insured credit union (FICU) examinations including for IT examinations.[4] The NCUA issues revisions approximately once each year to respond to the NCUA's annual supervisory focus.

One of the objectives of the NCUA's IT examination is to evaluate management's ability to recognize, assess, monitor, and control *information systems and assurance* related risks. Risks associated with credit union information systems and assurance programs include reputation risk, transaction risk, compliance risk, operational risk, and strategic risk. Reputation risk stands out primarily due to the risks associated with Internet services for credit union members. The information security risks facing the corporate credit union (corporate) network represent a systemic risk for the credit union industry overall. Problems with information systems at the corporate level can have a downstream effect on the security, reputation, and well-being of credit unions.

Cyber Threats[5] to the Critical Infrastructure on the Rise

The Department of Homeland Security (DHS) indicates: "Cyberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes are now being perpetrated through cyberspace."[6]

DHS also indicates: "Cyberspace is particularly difficult to secure due to….the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As IT becomes

[4] The Office of Examiner and Insurance (in coordination with ONES and other NCUA components) is primarily responsible for updating the NCUA's Examination Scope (NCUA Instruction 5000.20).

[5] Cyber Threat - An internal or external circumstance, event, action, occurrence, or person with the potential to exploit technology-based vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

[6] Cyberspace - The interdependent network of IT infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend."

Federal Requirements and Guidance Aimed at Improving and Protecting the Critical Infrastructure[7] from Cyber Threats

On February 12, 2013, the Whitehouse issued Presidential Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (Executive Order). The Executive Order established that "[i]t is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

The Executive Order called for the Director of the National Institute of Standards and Technology (NIST) to lead the development of a Cybersecurity Framework to reduce risks to critical infrastructure that shall incorporate voluntary standards and industry best practices. The resulting Cybersecurity Framework—created through collaboration between government and the private sector, which NIST published on February 12, 2014—is a voluntary risk-based set of industry standards and best practices to help organizations manage cybersecurity risks. The Cybersecurity Framework is composed of the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Cybersecurity Framework Core is: a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors; and consists of five Functions[8]—Identify,[9] Protect,[10] Detect,[11] Respond,[12] and Recover[13]—that when considered together, provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies 22 underlying key Categories[14] and 98 Subcategories[15] for each Function.

[7] The critical infrastructure sectors are those sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

[8] Functions aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

[9] Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

[10] Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

[11] Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

[12] Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

[13] Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

[14] Categories are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes."

[15] Subcategories provide a set of results that help support achievement of the outcomes in each Category. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."

The Federal Financial Institutions Examination Council (FFIEC) Efforts toward Increased Awareness, Assessment, and Oversight of Cybersecurity at Financial Institutions[16]

The FFIEC indicated financial institutions need a robust cybersecurity program to identify, assess, mitigate, and monitor cybersecurity risks. The FFIEC also indicated its members were taking a number of initiatives to raise the awareness of financial institutions and their critical third-party service providers with respect to cybersecurity risks and the need to identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats.

On June 30, 2015, the FFIEC released a Cybersecurity Assessment Tool (Assessment). The FFIEC indicated that it developed the Assessment, on behalf of its members "[i]n light of the increasing volume and sophistication of cyber threats, to help institutions identify their risks and determine their cybersecurity maturity." In addition, the FFIEC indicated "[t]he Assessment provides institutions with a repeatable and measureable process to inform management of their institution's risks and cybersecurity preparedness." The FFIEC indicated the Assessment includes a mapping to the NIST Cybersecurity Framework.[17]

The National Credit Union Administration's Efforts toward Increased Awareness, Assessment, and Oversight of Cybersecurity at Financial Institutions

In 2017, we conducted an audit of the NCUA's IT examination program to determine whether the program provided for adequate oversight of credit union cybersecurity programs. The scope of this audit focused on federal credit unions (FCUs) with assets between $250 million and $10 billion, which are under the supervision of the Office of Examination and Insurance (E&I). We issued report OIG-17-08 – *Audit of the NCUA Information Technology Examination Program's Oversight of Credit Union Cybersecurity Programs*, on September 28, 2017. During the audit, we learned E&I was in the process of adapting its IT examination program to incorporate an ACET Assessment to specifically assess credit unions' cybersecurity programs based on the NIST Cybersecurity Framework. We believed the ACET Assessments would address all of the voluntary control guidelines in the NIST Cybersecurity Framework, providing for comprehensive oversight of credit union cybersecurity programs. NCUA management indicated the agency would implement the ACET Assessments in January 2018.

[16] The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau and to make recommendations to promote uniformity in the supervision of financial institutions.

[17] The Assessment indicates NIST reviewed and provided input on the mapping to ensure consistency with Framework principles.

RESULTS IN DETAIL

We determined that ONES provides for adequate oversight of its credit unions' cybersecurity programs to assess whether the credit unions are taking sufficient and appropriate measures to protect the confidentiality, availability, and integrity of credit union assets and sensitive credit union data against cyber-attacks.[18] Specifically, we determined:

- The NCUA implemented its planned ACET Assessments of FICUs[19] effective for 2018 as part of the agency's RFE program,[20] which includes examination requirements for FICUs under the supervision of ONES.

- During its 2018 examination cycle,[21] ONES completed ACET Assessments on the consumer credit unions under its supervision and applicable corporates, meeting the requirements of the NCUA's 2018 RFE program as delineated in the Examination Scope.

- The NCUA's 2019 Examination Scope requires ONES complete ACET Assessment in 2019 on corporates that did not require an assessment during 2018. In addition, the 2019 Examination Scope delineates other required and discretionary baseline review areas and required and optional tools that can facilitate ONES in providing continued cybersecurity oversight of its consumer and corporates that already received ACET Assessments during 2018.

- "[O]utside of its normal examination and supervision process…" ONES offers a selection of voluntary cybersecurity assessments to its credit unions. ONES contracts with an independent third party to conduct these assessments.

During our audit, we also learned the NCUA is in the process of updating its IT examination program to include continued and enhanced maturity assessments and alternating reviews of credit union cybersecurity programs beyond 2019.

[18] ONES is responsible for supervising FCUs and federally insured state-chartered credit unions (FISCUs) (hereafter collectively referred to as consumer credit unions) with assets of $10 billion or more and the corporates.

[19] Federally insured credit unions include consumer credit unions and corporates.

[20] We briefly discuss the NCUA's prior plans for implementing ACET Assessments in the Background section on page 5 above.

[21] FCU examinations begin 8 to 12 months from the prior examination completion date. Examinations of the following FISCUs will also begin eight to 12 months from the prior examination: (a) assets greater than $1 billion; (b) a composite CAMEL code 4 or 5 with assets greater than $50 million; ***or*** (c) a composite CAMEL code 3 with assets greater than $250 million. All other FISCUs will receive an NCUA examination based on risk and emerging trends or on a sample basis as part of the agency's overall due diligence. All corporates must be examined once each calendar year. The maximum time between the completion dates of corporate examinations is 12 months unless an extension is approved. NCUA's examination scheduling program incorporates an extended examination cycle for eligible FCUs.

The NCUA Implemented ACET Maturity Assessments in 2018

In response to the recommendation in our 2017 audit of E&I's oversight of credit union cybersecurity programs, the NCUA management agreed it would implement the ACET Assessment into its examination process by January 2018.[22] We learned the NCUA incorporated ACET Assessment requirements into its Examination Scope effective for 2018 (NCUA Instruction 5000.20, Revision 9; effective December 27, 2017).[23] We also learned the NCUA's Examination Scope includes the requirements and options for not only consumer credit unions that fall under the supervision of E&I, but also for the corporates and consumer credit unions that fall under the supervision of ONES.[24]

ACET Assessment Requirements for 2018

Specific to ONES's examinations, Revision 9 of the Examination Scope required examiners to use the ACET Assessment during 2018 to assess consumer credit unions with assets greater than $10 billion. In addition, on February 8, 2018, E&I issued a memorandum—*Automated Cybersecurity Examination Tool (ACET) Review for Credit Unions Greater than $1 Billion in Assets*, which indicated that "[f]or 2018, all federally insured credit unions (FICUs) over $1 billion in assets as of 3/31/2017 require an ACET review." This memorandum incorporated required ACET Assessments during 2018 for corporates with assets greater than $1 billion.

Mapping the NCUA's Current ACET Assessment to the NIST Cybersecurity Framework

During our 2017 audit, we reviewed the mapping of the nearly 500 Declarative Statements (NCUA control measures) in the 2017 version of the NCUA's ACET Assessment (2017 ACET Assessment) to the 98 voluntary guidelines in the NIST Cybersecurity Framework[25] (NIST control guidelines) and concluded that we believed the NCUA's ACET Assessment would address all the NIST control guidelines.

For our current audit, we reviewed the NCUA's 2017 ACET Assessment against the current version of the NCUA's ACET Assessment (2018 ACET Assessment[26]) and determined there were no changes to the nearly 500 NCUA control measures. In addition, we learned NIST did not make any changes to its 2014 Cybersecurity Framework until April 16, 2018, which was after NCUA published the 2018 ACET Assessment (March 28, 2018). Therefore, we determined the mapping we reviewed during the 2017 audit between the NCUA's ACET Assessment and the voluntary NIST Cybersecurity Framework remains valid for the scope of this audit. Consequently, we still believe the NCUA's control measures address all the NIST control guidelines.

[22] We briefly discuss our 2017 audit report in the Background section on page 5 above.
[23] The NCUA issues revisions to its Examination Scope approximately once each year.
[24] We introduce NCUA Instruction 5000.20 and the RFE program on page 3 of the Background section above.
[25] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014.
[26] ACET V1.0.032618.

ONES Completed ACET Maturity Assessments and Other Assessments

We determined ONES completed ACET Assessments on the majority of its credit unions during 2018 as required. We also learned ONES plans to complete ACET Assessments on its remaining credit unions during 2019 as required. For those credit unions ONES assessed during 2018, the 2019 Examination Scope continues to include other required and optional review areas and tools that can facilitate ONES in continuing its oversight of credit union cybersecurity programs. Furthermore, we learned ONES provided for an independent third party to conduct several voluntary cybersecurity assessments on a few of its credit unions throughout the scope period of this audit (2016 through 2018).

ONES ACET Assessments During 2018

We determined that during 2018, ONES staff completed ACET Assessments on the six consumer credit unions under its supervision[27] and seven of its 11 corporates as required by the Examination Scope. The remaining four corporates had less than $1 billion in assets and did not require an ACET Assessment during 2018.

We obtained and reviewed the 13 ACET Assessments and other documentation NCUA used to track the completion of those assessments. Table 1 lists reported completion dates for the ACET Assessments on the six consumer credit unions under the supervision of ONES and the seven corporates during 2018.

Consumer Credit Unions	Assets as of 2018	ACET Completion Date
Boeing Employees	$17.16 billion	Nov 19, 2018
Navy	$91.79 billion	Nov 13, 2018
Pentagon	$22.40 billion	Oct 22, 2018
SchoolsFirst	$13.64 billion	Nov 19, 2018
State Employees'	$36.51 billion	Oct 22, 2018
The Golden 1	$11.07 billion	Sep 4, 2018
Corporate Credit Unions		
Alloya	$3.22 billion	Aug 31, 2018
Catalyst	$2.59 billion	Sep 13, 2018
Corporate America	$2.63 billion	Aug 8, 2018
Corporate Central	$1.53 billion	Nov 19, 2018
Corporate One	$3.16 billion	Dec 1, 2018
Vizo Financial	$4.17 billion	Aug 15, 2018
Volunteer	$1.33 billion	Sep 24, 2018

Table 1: Completion of ACET Assessments for ONES's consumer credit unions and corporates during 2018.

[27] ONES informed us that effective January 2019 three additional consumer credit unions were assigned to ONES. While these three consumer credit unions fall outside of the scope of this audit, we learned the NCUA completed ACET Assessments on them during 2018 as required.

ONES ACET Assessments and Other Examination Scope Requirements For 2019

We reviewed the Examination Scope for 2019 (NCUA Instruction 5000.20, Revision 10; effective January 2, 2019) to determine how the NCUA incorporated ACET Assessments into its RFE program for the year. The 2019 Examination Scope requires ACET assessments for certain credit unions that have not yet received them. Specifically, for ONES examinations, it requires ACET Assessments for credit unions with less than $1 billion in assets, which encompasses the four remaining corporates. A representative speaking on behalf of ONES informed us that while three of the four remaining corporates are on extended examination cycles, the directorate plans to complete all four ACET Assessments during 2019.[28]

The 2019 Examination Scope does not require ACET Assessments for consumer credit unions with assets greater than $10 billion or for corporates with assets greater than $250 million that previously received an ACET Assessment.[29] Table 2 identifies the 2019 Examination Scope required review areas and questionnaires for these credit unions.

	Assets	Required Review Area	Required Questionnaire
Consumer Credit Unions	> $10B	GLBA[30] Compliance	IT-E-748 Compliance[31]
Corporate Credit Unions	> $250M	Information Technology Security	IT-E-748 Compliance

Table 2: 2019 Examination Scope Requirements for ONES's consumer credit unions and corporates that had a prior completed ACET Assessment.

For the consumer credit unions under the supervision of ONES and for the corporates, the 2019 Examination Scope also includes the discretionary baseline review of credit union compliance with electronic banking authentication guidance (electronic banking measures).[32] As we reported in our 2017 audit, completing the required and optional questions in the IT-E-748 Compliance questionnaire and the optional Electronic Banking questionnaire would allow NCUA to assess more than 90 percent of the NIST cybersecurity control guidelines.

[28] See footnote 21 for a discussion of the NCUA's examination cycle.

[29] As discussed previously, ONES completed ACET Assessments during 2018 for consumer credit unions with assets greater than $10 billion and for its corporates with assets greater than $1 billion. Ultimately, for 2019 ONES's outstanding required ACET Assessments include only its corporates with assets between $250 million and $1 billion.

[30] Gramm-Leach-Bliley Act P.L. 106-102, Title V, Subtitle A. § 501 (Nov. 12, 1999), codified at 15 U.S.C. § 6801.

[31] Expanded 748 Compliance questionnaire—used to assess whether credit union Information Security Programs address the required elements of 12 C.F.R. Part 748. The questionnaire includes required and optional questions.

[32] A *baseline* area is an area NCUA deemed as having elevated risk. If field staff determine that a baseline review area is immaterial or low risk, they may opt out of completing the relevant baseline review. Use of the electronic banking questionnaire to review this area is optional.

Independent Third Party Cybersecurity Assessments

During the audit, we learned ONES has a program through which it offers (at no cost) to its credit unions—on a voluntary basis—a selection of cybersecurity assessments. A ONES management official informed us that ONES started this program in 2013 to assess the IT posture and level of risk of its credit unions. The ONES management official also stated these assessments are a supplement to the supervision examinations to help scope the examinations; and the results of the assessments are for sharing information between ONES and the credit union and do not count against the credit union. The types of assessments available to ONES's credit unions include, but are not limited to penetration tests (external and internal), vulnerability assessments (external and internal), social engineering (onsite and remote), incident response controls, etc. Five corporates and one consumer credit union received assessments between 2016 and 2018. The independent third party published a total of 23 reports among the six credit unions.

We believe these voluntary supplemental assessments can serve to enhance ONES's cybersecurity oversight of the credit unions that opt to take advantage of the assessments, ultimately strengthening the credit unions' cybersecurity postures.

Based on: (a) the NCUA's implementation of its ACET Assessment; (b) our re-validation that the NCUA's ACET Assessment is a tool we believe provides for addressing all of the voluntary control guidelines in the NIST Cybersecurity Framework; (c) ONES completing its ACET Assessments as required by the NCUA's Examination Scope; and (d) ONES' voluntary supplemental cybersecurity assessment program, we are not making any recommendations at this time.

Credit Union Cybersecurity Assessments Beyond 2019

We learned the NCUA is in the process of updating its IT examination program to include continued and enhanced assessments of its credit unions' cybersecurity programs. Specifically, NCUA management informed us that their plans for assessing credit union cybersecurity programs beyond 2019 involve alternating ACET Assessments with optional cybersecurity control (CSC) reviews based on CIS Controls.

An NCUA representative informed us the initial ACET Assessments: (a) established a baseline for each of the FICUs the agency assessed during 2018; (b) provide a uniform measurement for all FICUs' security postures; and (c) determine whether additional supervision is necessary to address any concerns. Based on the 2019 Examination Scope, we wondered whether the NCUA might not require ACET Assessments every year as part of its RFE program going forward. Therefore, we inquired about the agency's plans for completing future ACET Assessments. An E&I management official informed us the NCUA's overall goal is to evaluate 100 percent of FICUs on a rolling basis over a four year maturity assessment life cycle. The official outlined the NCUA's plans for the maturity assessment portion of the agency's overall cybersecurity examination program, which includes a new Automated Cybersecurity Examination Toolbox

(ACET Solution) to conduct enhanced maturity assessments of all FICUs to: (a) get a perspective on the state of the credit union industry; and (b) identify areas of focus to guide communications and examination program priorities. Specifically, the official informed us the Idaho National Laboratory (INL) is building the new ACET Solution for the NCUA, which leverages the DHS's nationally recognized CSET® (Cyber Security Evaluation Tool).[33] The official announced this initiative to field staff on January 11, 2019 and indicated the NCUA is: "…in [the] process of designing alternate year reduced question sets based on [the] size and complexity [of the credit unions] that are founded in the Center for Information [sic] Security 20 Critical Security Controls. These streamlined review work plans will be incorporated into the examination program in subsequent years as an optional or baseline review…where an ACET review [Assessment] is not completed."[34] In summary, NCUA management indicated the ACET Solution will incorporate ACET Assessments and enhanced examination procedures to ensure the NCUA's ability to consistently identify cybersecurity risk trends.

The following highlight the history (and cybersecurity significance) of the CIS Controls, which are the foundation for the NCUA's CSC reviews:

- According to the SANS Institute (SANS),[35] the National Security Agency (NSA), the U.S. Department of Energy nuclear energy labs, law enforcement organizations, and some of the nation's top forensics and incident response organizations created the controls. The following further detail the history of the CIS Controls:

    - In 2008, the Office of the Secretary of Defense asked the NSA for help in prioritizing the myriad security controls that were available for cybersecurity.

    - The NSA, the CIS®, and SANS, participated in a public-private consortium to share its attack information to provide the same type of control-prioritization knowledge for civilian government agencies and critical infrastructure [to protect critical communications, power and financial sectors].

    - In early 2009, the consortium circulated the draft of the CIS Critical Controls to several hundred IT and security organizations for further review and comment. Over 50 organizations commented and endorsed the concept of a focused set of controls and the selection of the CIS Critical Controls.

[33] The E&I management official informed us the INL built the CSET for the DHS.

[34] The official further explained that the goal is to evaluate all credit unions on a rolling basis and then alternate with a specialized program that: (a) embodies some or all of the 20 critical security controls; (b) reflects specialized focus based on the results of the ACET Assessments; and (c) covers compliance with Consumer Privacy Laws.

[35] According to its website, SANS is the most trusted and the largest source for information security training and security certification in the world; develops, maintains, and makes available at no cost, the largest collection of research documents on information security; and operates the Internet's early warning system - the Internet Storm Center.

- The State Department validated the list of controls and found they aligned with the 3,085 real-world attacks the State Department experienced in FY 2009. The State Department then launched a project to implement the controls across the entire State Department's cyber environment. In achieving a more than 88 percent reduction in vulnerability-based risk across 85,000 systems, the State Department's program became a model for large government and private sector organizations.

- In May 2012, the Commander of the U.S. Cyber Command and Director of NSA announced that he believed adopting the CIS Controls was a good foundation for effective cybersecurity.

- In June 2012, the INL completed a very favorable analysis of how the CIS Controls applied in the electric sector as a first step in assessing the applicability of the controls to specific industrial sectors.

Currently, there are 20 CIS Controls (and 171 sub-controls) across the following three categories:[36]

- Basic: The key controls which should be implemented in every organization for essential cyber defense readiness.

- Foundational: The technical best practices that provide clear security benefits and are a smart move for any organization to implement.

- Organizational: Have many technical elements, but are more focused on the people and processes involved in cybersecurity.

With the NCUA's plans to update its IT examination program to include continued and enhanced ACET Assessments with alternate year review plans based on the CIS Controls, we believe the NCUA is proactively taking measures for continuous comprehensive oversight of its credit unions' cybersecurity programs. We may review the NCUA's cybersecurity examination program again after the agency has incorporated its planned enhancements into its RFE program.

[36] CIS Controls^{TM}, Version 7.1, April 1, 2019.

APPENDIX A

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine whether ONES provides for adequate oversight of its credit unions' cybersecurity programs to assess whether the credit unions are taking sufficient and appropriate measures to protect the confidentiality, availability, and integrity of credit union assets and sensitive credit union data against cyber-attacks.

To accomplish our objective, we conducted fieldwork at NCUA's Central Office in Alexandria, VA. We interviewed NCUA management and staff from ONES and E&I. We reviewed NCUA information security regulations, policies, and procedures pertaining to examining credit union information security programs. We also relied on our review of the following from our 2017 audit: a Presidential Executive Order, federal legislation related to information security, and federal cybersecurity information, policy, and guidance from NIST, the DHS, and the FFIEC. In addition, we reviewed information and guidance pertaining to the Center for Internet Security, Inc. Finally, we reviewed ACET Assessments (from the NCUA's Automated Integrated Regulatory Examination System) that ONES staff completed during 2018 on the six consumer credit unions and the seven corporates that required ACET Assessments in that year.

We conducted this audit from January 2019 through July 2019 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.

Appendix B

National Credit Union Administration
(Office of the Executive Director)

SENT BY EMAIL

TO: Inspector General Jim Hagen

FROM: Executive Director Mark Treichel Mark

SUBJ: Management Response – Audit of the NCUA Office of National Examinations and Supervision Oversight of Credit Union Cybersecurity Programs

DATE: July 30, 2019

This memorandum responds to your request for comment on the report titled "Audit of the NCUA Office of National Examinations and Supervision Oversight of Credit Union Cybersecurity Programs." We concur with the report and its conclusions and noted there are no official recommendations.

Thank you for the opportunity to review and comment on your report.

.

APPENDIX C

ACRONYMS AND ABBREVIATIONS

Acronym	Term
ACET	Automated Cybersecurity Examination ***Tool***
ACET Assessment	ACET Maturity Assessment
ACET Solution	Automated Cybersecurity Examination ***Toolbox***
Assessment	Cybersecurity Assessment Tool
CIS Controls	CIS Controls^{TM}
CIS®	Center for Internet Security, Inc.
Corporate	Corporate Credit Union
CSC	Cybersecurity Controls
CSET	Cybersecurity Evaluation Tool
DHS	Department of Homeland Security
E&I	Office of Examination and Insurance
Examination Scope	NCUA Instruction 5000.20
Executive Order	Presidential Executive Order 13636
FCU	Federal Credit Union
FFIEC	Federal Financial Institutions Examination Council
FISCU	Federally Insured State-Chartered Credit Union
FICU	Federally Insured Credit Union
GLBA	Gramm-Leach-Bliley Act (Privacy)
INL	Idaho National Laboratory
IT	Information Technology

Acronym	Term
NCUA	National Credit Union Administration
NCUA control measures	ACET Declarative Statements
NIST	National Institute of Standards and Technology
NIST control guidelines	NIST Cybersecurity Framework Subcategories
NSA	National Security Agency
OIG	Office of Inspector General
ONES	Office of National Examinations and Supervision
RFE	Risk-Focused Examination
SANS	The SANS Institute