certain area depending on findings, areas of concern, or lack thereof in prior examinations. Consequently, the results of IT exams may include different areas and may vary across examinations and from year to year. However, the IT exam program has requirements under the RFE program. Specifically:

NCUA Instruction 5000.20,[29] "Examination Scope" (Instruction), establishes NCUA's requirements for all examinations (minimally-scoped examinations).[30]

- For FCUs with assets greater than $250 million, the NCUA IT exam program has two areas examiners will address in every examination. Those areas are: (1) the *required* review of FCU compliance with 12 CFR Part 748 requirements (Gramm-Leach-Bliley (Privacy) Act member information security compliance),[31] and (2) the *baseline* review of compliance with FFIEC electronic banking authentication guidance.[32] NCUA's Automated Integrated Regulatory Examination System (AIRES[33]) includes one required tool – the Expanded 748 Compliance questionnaire – and an optional tool (the Electronic Banking questionnaire) for examiners to use in assessing FCU compliance with 12 CFR Part 748 and with FFIEC electronic authentication guidance respectively:[34]
    - The required Expanded 748 Compliance questionnaire[35] includes two sections:
        - The required Core Review section, which includes 20 questions examiners *must use* in determining whether an FCU's InfoSec Program addresses the required elements from 12 CFR Part 748.
        - The optional Expanded Review section, which includes an additional 60 questions examiners *can use* to go into more depth in the areas addressed by the Core Review section.

[29] We evaluated NCUA against Revision 6 (effective January 26, 2015) and Revision 7 (effective January 14, 2016) of the Instruction because the effective dates of the examinations we sampled are after January 26, 2015 and prior to January 19, 2017 (the date NCUA issued Revision 8, cancelling Revision 7).
[30] Examinations include Federal Credit Union (FCU) Examinations (Code 10), Federally-Insured State Chartered Credit Unions (FISCU) Examinations (Code 11), Corporate FCU Examinations (Code 12), and Corporate FISCU Examinations (Code 13).
[31] For details on 12 CFR Part 748, see "Federal Legislation, Regulations, and Guidance Influencing NCUA's Current Information Technology Examination Program" on page 7 and 8 of this report
[32] The review of 12 CFR Part 748 compliance is a *required* area examiners must review on every examination. The review of electronic authentication compliance is a *baseline* area, which is an area NCUA deemed as having elevated risk. NCUA indicates that reviews of baseline areas combined with successful reviews of required areas may constitute an adequately scoped examination of some credit unions.
[33] NCUA Examiners use our AIRES to complete examinations on their laptop computers.
[34] For each *required* review area, field staff must complete the associated AIRES questionnaire. In addition, the scope module must provide an administrative record of the procedures performed, the results of the review, and the recommended action.
[35] The scope of the 748 Compliance questionnaire is to determine the extent of compliance with NCUA Rules and Regulations, Part 748, Appendix A, and the overall effectiveness of the credit union's information security program.

- The optional Electronic Banking questionnaire[36] includes 91 questions that address:[37] Critical E-Banking Controls, FFIEC Authentication Guidance (including for Commercial Accounts), Mobile Banking, Online or Mobile Deposits, Bill Pay Controls, E-Statements, Account Aggregation Controls, Credit Union Hosted Internet Banking, Additional Internet Banking Controls, and Employee Access Controls. Although the IT exam program requires examiners to address an FCU's compliance with FFIEC electronic authentication guidance, NCUA stopped requiring examiners to use this available questionnaire effective January 26, 2015.

To see details on NCUA's current IT exam program's requirements, see Appendix B, and to see how the agency adapted those requirements to address information security-related Federal legislation, regulations and guidance, see Chart 3 on page 20.

OIG Assessment of NCUA's Information Technology Examination Program Coverage of NIST Cybersecurity Framework Guidance

The OIG conducted an assessment of NCUA's Expanded 748 Compliance questionnaire and its Electronic Banking questionnaire to correlate (map) each question to the NIST cybersecurity control guidelines.

Mapping the Expanded 748 Compliance Questionnaire

In determining which of the questions in NCUA's Expanded 748 Compliance questionnaire we believe map to the 98 NIST control guidelines, we: (1) assessed each question independently as it pertains to the overall InfoSec components addressed in the questionnaire, e.g., Risk Assessment, Security Awareness Training, etc., and (2) considered the guidance that NCUA included in the questionnaire for examiners to use in assessing each question. Although the majority of the questions in the Core Review section had additional more in-depth questions and guidance in the Expanded Review section related to that particular InfoSec component, we generally mapped those questions based only on what was addressed in that Core Review section.

For example, in Chart 1 (below) we mapped the Core Review question related to "access controls" to the NIST control guidelines based primarily on the question and included guidance specifically included:

[36] The scope of the Electronic Banking questionnaire is to determine whether adequate controls are in place for the credit union to safely deliver electronic banking through multiple channels such as Internet, mobile devices, and telephone banking.
[37] If examiners opt not to review credit union compliance with the FFIEC guidance, they must provide a reason in the examination documentation.

Chart 1.

NCUA's Expanded 748 Compliance Questionnaire		**NIST Cybersecurity Framework Subcategories (NIST control guidelines)**
Review Question	Included Guidance	
[redacted]		
Has management adopted appropriate security measures within the ISP[38] to address access controls on member information systems? (Core)	• Administration of access rights at enrollment, when duties change, and at employee separation. • Perimeter protections including firewalls, malicious code prevention, outbound filtering, and security monitoring • Appropriate application access controls (based on duties). • Remote access controls including wireless, VPN,[39] modems, and Internet-based.	**ID.GV-1**- Organizational information security policy is established
		PR.AC-1 - Identities and credentials are managed for authorized devices and users
		PR.AC-3 - Remote access is managed
		PR.AC-4 - Access permissions are managed, incorporating the principles of least privilege and separation of duties
		PR.AC-5 - Network integrity is protected, incorporating network segregation where appropriate
		PR.DS-5 - Protections against data leaks are implemented
		PR.PT-4 - Communications and control networks are protected
		DE.AE-1 - A baseline of network operations and expected data flows for users and systems is established and managed

[38] Information Security Program.
[39] Virtual Private Network.

However, there was one question in the Core Review section that we believe included guidance at only a high level, but did not include more in-depth questions or guidance in the Expanded Review section.[40] Therefore, we mapped that question based also on what we believe an IT examiner conducting reasonable due diligence might consider in assessing the question. See Chart 2 (below):

Chart 2.

NCUA's Expanded 748 Compliance Questionnaire		**NIST Cybersecurity Framework Subcategories (NIST control guidelines)**
Review Question	Included Guidance	
[redacted]		
Are monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems included in the ISP? (Core)	This [sic] processes addressed should include: • Log monitoring (access, changes, processes run) • Security alerts (firewall, IDS/IPS,[41] 3rd party notices) • Monitoring physical access systems (badge reader reports) • Surveillance camera data	**DE.CM-1** - The network is monitored to detect potential cybersecurity events
		DE.CM-2 - The physical environment is monitored to detect potential cybersecurity events
		DE.CM-4 - Malicious code is detected
		DE.CM-5 - Unauthorized mobile code is detected
		DE.CM-6 - External service provider activity is monitored to detect potential cybersecurity events
		DE.CM-7- Monitoring for unauthorized personnel, connections, devices, and software is performed
		DE.AE-2 - Detected events are analyzed to understand attack targets and methods
		DE.AE-3 - Event data are aggregated and correlated from multiple sources and sensors
		DE.AE-4 - Impact of events is determined
		DE.AE-5 - Incident alert thresholds are established
		DE.DP-1 - Roles and responsibilities for detection are well defined to ensure accountability
		DE.DP-3 - Detection processes are tested
		DE.DP-4 - Event detection information is communicated to appropriate parties
		DE.DP-5 - Detection processes are continuously improved

[40] Although the Expanded Review section included an InfoSec component specific to "Monitoring," we believe the questions under that component are specific to only "log monitoring" functions. Therefore, we mapped these questions to control guidelines under the NIST Cybersecurity Framework Protect (PR) Function rather than the Detect (DE) Function.

[41] Intrusion Detection System/Intrusion Prevention System

We determined that if examiners address only the required 20 Core Review questions in the required Expanded 748 Compliance questionnaire, the IT exam would facilitate assessing FCU cybersecurity programs against just over half (57 percent) of the 98 NIST cybersecurity control guidelines as indicated in Table 1 (below). However, if examiners also address the additional 60 questions in the optional Expanded Review section, the IT exam would facilitate assessing FCU cybersecurity programs against 84 percent of the NIST cybersecurity control guidelines, allowing for more comprehensive oversight of FCUs' cybersecurity programs.

Table 1. OIG Mapping of NCUA's Expanded 748 Compliance Questionnaire to the NIST Cybersecurity Framework

NIST Cybersecurity Framework			**NCUA IT Examination – Expanded 748 Compliance Questionnaire**	
Core Functions	**Underlying Categories**	**Total Underlying Subcategories (NIST cybersecurity control guidelines)**	**The Total Number of the NIST Cybersecurity Framework Subcategories Addressed (Based on OIG Mapping)**	
			Core Review Questions	**Core Review and Expanded Review Questions**
Identify	*Asset Management*	6	6	6
	Business Environment	5	0	2
	Governance	4	4	4
	Risk Assessment	6	6	6
	Risk Management Strategy	3	3	3
Protect	*Access Control*	5	5	5
	Awareness and Training	5	1	5
	Data Security	7	4	5
	Information Protection Processes and Procedures	12	6	10
	Maintenance	2	0	2
	Protective Technology	4	1	3
Detect	*Anomalies and Events*	5	5	5
	Security Continuous Monitoring	8	8	8
	Detection Processes	5	4	4
Respond	*Response Planning*	1	0	1
	Communications	5	0	3
	Analysis	4	0	3
	Mitigation	3	1	3
	Improvements	2	2	2
Recover	*Recovery Planning*	1	0	1
	Improvements	2	0	0
	Communications	3	0	1
		98	**56 (57%)**	**82 (84%)**

We noted that the examination documentation for 47 of the 48 FCUs we sampled included an Expanded 748 Compliance Questionnaire with a completed Core Review section. The documentation for the one anomaly indicated the examiner completed the IT 748A

questionnaire, which is the IT questionnaire NCUA uses to examine credit unions with assets *less than* $250 million.[42] We also noted that although NCUA's IT exam program only requires completing the required Core Review section of the Expanded 748 Compliance questionnaire, examiners also addressed the optional Expanded Review section in 31 of the 47 examinations that included the Expanded 748 Compliance Questionnaire.

Mapping the Electronic Banking Questionnaire

In mapping NCUA's optional Electronic Banking questionnaire to the NIST Cybersecurity Framework, we determined that if examiners were to complete all 91 questions, the exam would facilitate assessing 30 of the 98 (31 percent) NIST cybersecurity control guidelines (See Table 2 below).

[42] We noted the examiner that completed this examination was not identified as an IT Subject Matter Examiner or a Regional Information Systems Officer.

Table 2. OIG Mapping of NCUA's Electronic Banking Questionnaire to the NIST Cybersecurity Framework

NIST Cybersecurity Framework			**NCUA Electronic Banking Questionnaire**	
Core	**Underlying Categories**	**Total**	**The Total Number of the NIST Cybersecurity Framework Subcategories Addressed (Based on OIG Mapping)**	
			Questions in the Critical E-Banking Section and FFIEC Authentication Guidance Section	**Questions in All Sections[43]**
Identify	*Asset Management*	6	1	1
	Business Environment	5	2	2
	Governance	4	1	4
	Risk Assessment	6	3	3
	Risk Management Strategy	3	0	0
Protect	*Access Control*	5	3	4
	Awareness and Training	5	1	2
	Data Security	7	0	1
	Information Protection Processes and Procedures	12	0	3
	Maintenance	2	0	0
	Protective Technology	4	1	2
Detect	*Anomalies and Events*	5	4	4
	Security Continuous Monitoring	8	3	3
	Detection Processes	5	0	0
Respond	*Response Planning*	1	0	0
	Communications	5	0	1
	Analysis	4	0	0
	Mitigation	3	0	0
	Improvements	2	0	0
Recover	*Recovery Planning*	1	0	0
	Improvements	2	0	0
	Communications	3	0	0
		98	**19 (19%)**	**30 (31%)**

Although the IT exam program no longer requires - effective January 26, 2015 - that examiners use the Electronic Banking questionnaire to review an FCU's compliance with FFIEC electronic

[43] The other sections of the Electronic Banking questionnaire are: Mobile Banking, Online or Mobile Deposits, Bill Pay Controls, E-Statements, Account Aggregation Controls, Credit Union Hosted Internet Banking, Additional Internet Banking Controls, and Employee Access Controls.

banking authentication guidance, we determined that examiners used the questionnaire in 30 of the 48 examinations we sampled.

Finally, we noted that completing all questions in both the Expanded 748 Compliance questionnaire and the Electronic Banking questionnaire would facilitate NCUA assessing FCUs against 89 of 98 of the NIST cybersecurity control guidelines (91 percent).

Increased Focus on Cybersecurity Risks and NCUA's Tool for Assessing Credit Union Cybersecurity Programs

The federal community has introduced more recent guidance to address growing concerns regarding the cyber threat to the nation's critical infrastructure. Specifically – as addressed in the Background section of this report:

- On February 12, 2013, the Whitehouse issued Presidential Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (Executive Order).[44] The Executive Order called for the Director of NIST to lead the development of a Cybersecurity Framework to reduce risks to critical infrastructure that shall incorporate voluntary standards and industry best practices.

- On February 12, 2014, NIST published its Cybersecurity Framework, which is a voluntary risk-based set of industry standards and best practices to help organizations manage cybersecurity risks.[45]

- On June 30, 2015, the FFIEC released a Cybersecurity Assessment Tool (Assessment) on behalf of its members to help *institutions* identify their risks and assess their cybersecurity preparedness.[46]

The FFIEC indicated that its member agencies are 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.

Regarding NCUA initiatives, we learned that in the Summer/Fall of 2015, NCUA began working to develop an examination tool based on the Assessment. At the time, NCUA referred to this tool as the CEG (Cybersecurity Examination Guide). In March 2016, NCUA announced the CEG initiative and released its plans for implementing the CEG "over the next 18 months…to be utilized during examinations to review a credit union's cybersecurity risks and controls."

[44] We discuss the Executive Order on page 3 of the Background section of this report.
[45] We discuss the NIST Cybersecurity Framework on page 3 of the Background section of this report.
[46] We discuss the FFIEC Cybersecurity Assessment Tool on page 5 of the Background section of this report.

We also learned the agency renamed the CEG as the Automated Cybersecurity Examination Tool (ACET). The ACET includes: (1) nearly 500 "Declarative Statements" (NCUA control measures) for assessing a credit union; and (2) suggested steps for validating whether a credit union meets each control measure. The ACET will allow examiners to assess:

- A credit union's risk in each of the following categories:
  - Technologies and Connection Types,
  - Delivery Channels,
  - Online/Mobile Products and Technology Services,
  - Organizational Characteristics, and
  - External Threats.

- The maturity level of a credit union's cybersecurity programs in the following five domain areas:[47]
  - Cyber Risk Management and Oversight,
  - Threat Intelligence and Collaboration,
  - Cybersecurity Controls,
  - External Dependency Management, and
  - Cyber Incident Management and Resilience.

The ACET includes a mapping of the NCUA control measures to the NIST Cybersecurity Framework. We noted the ACET is mapped to 87 of 98 (89 percent) of NIST cybersecurity control guidelines, leaving 11 unaddressed.[48] We reviewed the ACET and determined the ACET includes Declarative Statements that we believe address those 11 NIST cybersecurity control guidelines. Consequently, we believe the ACET will address all 98 of the voluntary NIST cybersecurity control guidelines.

On June 27, 2017, NCUA's Office of Examination and Insurance (E&I) indicated in an internal NCUA memorandum it would include the ACET in the December 2017 release of AIRES. Representatives of E&I informed the OIG the agency plans to implement the ACET in January 2018 to obtain a baseline examination of credit union cybersecurity programs. The representatives also indicated the agency would potentially use the ACET to assess those programs every other year.

NCUA's minimally-scoped IT exams provide for a less than comprehensive assessment of FCU cybersecurity programs because the agency has appropriately based its current requirements on information security concerns and risks as addressed in federal legislation, regulation, and

[47] The maturity level of a credit union in each domain will be: Baseline, Evolving, Intermediate, Advanced or Innovative.
[48] The Subcategory codes are: under the Detect Function - DE.AE-5, DE.CM-1, and DE.CM-2; and under the Response Function - RS.CO-4, RS.CO-5, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1 and RS.MI-3.

guidance issued through 2012 (see Chart 3 below). As indicated in the Background section, the cyber threat to the nation's critical infrastructure has been a growing concern. Consequently:

- NIST and the FFIEC have provided more recent voluntary guidance to address cybersecurity risks.

- NCUA is in the process of adapting its IT exam program to incorporate a tool based on the FFIEC and NIST guidance.

Chart 3.

Required Review	Baseline Review
Compliance of FCU InfoSec Programs with 12 CFR 748 (GLBA (Privacy) requirements)	**FCU Compliance with FFIEC Electronic Authentication Guidance**
Required Questionnaire *IT Expanded 748 Compliance questionnaire*	***Optional* Questionnaire** *Electronic Banking* *(91 questions)*
Required Core Review section (20 questions) / Optional Expanded Review section (60 questions)	Critical E-Banking Controls and FFIEC Authentication Guidance / 8 Other sections
InfoSec-related federal legislation, regulation and guidance – influence on IT Exam Program requirements	
1999	**2005**
Gramm-Leach Bliley Act (GLBA) • Required NCUA to set administrative, technical and physical standards for FICUs regarding protecting member information	• FFIEC releases guidance regarding the risks and risk management controls necessary to authenticate the identity of customers accessing Internet-based financial services • NCUA issues LCU regarding *Guidance on Authentication in Internet Banking Environment* o Provides FFIEC guidance to credit unions for use in evaluating and implementing authentication systems and practices o Conformance expected by end of year 2006
2001	**2011**
12 CFR Part 748 (amended) Appendix A • NCUA's implementation of the GLBA requirement • Requires FICUs to develop written security programs designed to meet GLBA requirements	• FFIEC issues supplement to the 2005 authentication guidance o Reinforces the 2005 guidance o Updates supervisory expectations regarding authentication • NCUA issues LCU regarding "Online Member Authentication Guidance Compliance Required by January 2012" o Updated guidance to address significantly changed Internet threats o Expects FICUs to adapt appropriate strategies by January 2012 o Indicates examiners will begin evaluating authentication controls in 2012
2005	**2012**
12 CFR Part 748 (amended) Appendix B • Requires FICU security programs to contain a provision for responding to incidents of unauthorized access to member information.	• NCUA required review of compliance with FFIEC authentication guidance • NCUA required completion of the Critical E-Banking Controls and the FFIEC Authentication Guidance sections of the Electronic Banking questionnaire
	2014
	• NCUA established Required, Baseline and Expanded review areas • Electronic Banking designated as a *Baseline* Review
2015	**2015**
• GLBA member information security compliance became a Required Review	• ****NCUA** no longer required Electronic Banking Questionnaire

NCUA's Automated Cybersecurity Examination Tool Should Ensure NCUA's Oversight of Credit Union's Cybersecurity Programs is Comprehensive.

By adapting its existing IT exam program to incorporate its cybersecurity examination tool – ACET, NCUA is helping facilitate NCUA's IT exam program providing for a more

comprehensive assessment of the strengths and weaknesses of credit union managements' programs and efforts to protect credit union infrastructures from cybersecurity related risks. Therefore, we are making the following recommendation.

Recommendation

We recommend NCUA management:

1. Implement the Automated Cybersecurity Examination Tool and determine how it best fits into NCUA's Risk-Focused Examination program to ensure more comprehensive examinations of credit unions' cybersecurity programs.

Management Response:

Management agreed with the recommendation. Management indicated that after evaluating the results of testing the Automated Cybersecurity Examination Tool and making necessary revisions, it will implement the tool into the exam process by January 2018.

OIG Response:

We concur with management's planned corrective action.

Appendix A: Objective, Scope, and Methodology

The objective of this audit was to determine whether NCUA's IT examination program provides for adequate oversight of credit union cybersecurity programs to assess whether credit unions are taking sufficient and appropriate measures to protect the confidentiality, availability, and integrity of credit union assets and sensitive credit union information 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 the Office of Examination and Insurance and the Office of National Examinations and Supervision and a Regional Information Systems Officer. We reviewed NCUA information security regulations, policies, procedures, and practices pertaining to examining credit union information security programs. We also reviewed a Presidential Executive Order and federal legislation related to information security. In addition, we reviewed federal cybersecurity information, policy, and guidance from the National Institute of Standards and Technology, the Department of Homeland Security, and the Federal Financial Institutions Examination Council.

Furthermore, we randomly selected and reviewed results from IT examinations of 48 of the 387 FCUs in Regions 1 through 5 with assets between $250 million and $10 billion.[49] We reviewed the most recent examination(s) of each FCU recorded in AIRES at the time of our audit.

We conducted this audit from February 2016 through September 2017 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances.[50] 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.

[49] We based our sample on NCUA's listing of federally-insured credit unions (federal credit unions and federally-insured state credit unions) as of December 31, 2015.
[50] Competing priorities within the OIG resulted in delays in completing this audit.

Appendix B: NCUA's Information Technology Program Requirements for Oversight of Federal Credit Unions with Assets greater than $250 Million

As previously indicated, NCUA Instruction 5000.20 establishes NCUA's requirements for all examinations.

- Effective January 5, 2012 (Revision 3) - for federal credit unions (FCUs) with assets greater than $250 million offering home banking, audio response, and/or mobile banking, the Instruction included a requirement for examiners to complete specific sections from the Electronic Banking questionnaire to review FCU compliance with FFIEC authentication guidance. Those sections address: (1) Critical E-Banking Controls and (2) FFIEC Authentication Guidance. The Instruction also indicated examiners would conduct the Electronic Banking review on an as needed basis once the initial review was completed. The Electronic Banking questionnaire includes other sections as follows:

    - Mobile Banking,
    - Online or Mobile Deposits,
    - Bill Pay Controls,
    - E-Statements,
    - Account Aggregation Controls,
    - CU Hosted Internet Banking,
    - Additional Internet Banking Controls, and
    - Employee Access Controls.

- Effective June 25, 2012 (Revision 4) the Instruction updated the requirement for examiners to complete the specific sections of the Electronic Banking questionnaire for FCUs with assets greater than $250 million that deliver financial services electronically, which include Home Banking *via Internet Website*, Audio Response*/Phone Based* or Mobile Banking. (The updates are annotated in italics)

- The February 5, 2014 version of the Instruction (Revision 5) established *required*,[51] *baseline*,[52] and *expanded*[53] review areas for all examinations.[54] The Instruction:

[51] NCUA indicated field staff must complete a review of the required review areas at every examination and must complete the associated AIRES questionnaire.
[52] NCUA indicated baseline review areas include certain credit union areas with elevated risk, which combined with successful reviews of required areas, may constitute an adequately scoped examination of some credit unions.
[53] NCUA indicates: (1) expanded review areas are based on field staff judgment and depend upon the risk profile of the credit union; and (2) completion of the required and baseline reviews will be adequate for a full evaluation of the credit union's risk profile in some instances.
[54] NCUA indicated that field staff do not have to review every baseline area in every examination of every credit union – field staff must use their own judgment and understanding of the circumstances of each credit union to determine which baseline review areas to include in the scope of an examination.

- Designated Electronic Banking as a *baseline* review area and continued the requirement for field staff to complete the specific sections from the Electronic Banking questionnaire.

- Indicated that although field staff do not have to review *baseline* areas in every examination of every credit union, they must document their review of the baseline area or document their reason for choosing not to review the area.

- Indicated that in addition to completing the associated questionnaire for each *required* review area, field staff must provide an administrative record of the procedures performed, the results of the review, and the recommended action.

- Effective January 26, 2015 (Revision 6), the Instruction:

  - Included "Gramm-Leach-Bliley (Privacy) Act member information security compliance" as a *required* review area.[55] As a required review area, this includes – for FCUs with assets greater than $250 million – completing only the Core Review section of NCUA's Expanded 748 Compliance questionnaire.[56] The Core Review section consists of 20 questions that address an FCU's "Information Security Program." The 748 Questionnaire includes an Expanded Review section consisting of an additional 60 questions that provide for an more in-depth review of the following areas addressed by the Core Review section:

    - Risk Assessment,
    - Access Controls
    - Physical Controls,
    - Encryption,
    - Change Management,
    - Monitoring,
    - Incident Response,
    - Disaster Recovery/Business Continuity,
    - Security Awareness Training,
    - Information Destruction,
    - Vendor Oversight, and
    - Response Programs for Unauthorized Access to Member Information.

[55] The specific Privacy Act elements are the Guidelines for Safeguarding Member Information (Appendix A to Part 748 of NCUA Rules and Regulations) and Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice (Appendix B to Part 748 of NCUA Rules and Regulations).
[56] The scope of this 748 questionnaire is to: Determine the extent of compliance with NCUA Rules and Regulations, Part 748, Appendix A, and the overall effectiveness of the credit union's information security program.

- Indicated that although field staff may find AIRES questionnaires associated with the baseline review areas helpful in guiding the reviews, NCUA no longer required field staff to complete those questionnaires.

Appendix C: NCUA Management Response

National Credit Union Administration
Office of the Executive Director

SENT BY E-MAIL

TO: Inspector General Jim Hagen

FROM: Executive Director Mark Treichel

SUBJ: Management Response – Audit of the NCUA Information Technology Examination Program's Oversight of Credit Union Cybersecurity Programs

DATE: September 27, 2017

The following is our response to the recommendation set forth in the Office of Inspector General's draft report titled Audit of the NCUA Information Technology Examination Program's Oversight of Credit Union Cybersecurity Programs.

OIG Report Recommendation

1. Implement the Automated Cybersecurity Examination Tool (ACET) and determine how it best fits into NCUA's Risk-Focused Examination program to ensure more comprehensive examinations of credit unions' cybersecurity programs.

Response: We concur with the implementation of the ACET to review cybersecurity programs as part of the Risk-Focused Examination program. After evaluating the results of the ACET testing and making necessary revisions, implementation into the exam process will occur by January 2018.

Thank you for the opportunity to review and comment on the report. Please contact me if you have any questions.

1775 Duke Street - Alexandria, VA 22314-3428 - 703-518-6320

Appendix D: Acronyms and Abbreviations

AC	NIST Cybersecurity Framework *Access Control* Category
ACET	Automated Cybersecurity Examination Tool
AE	NIST Cybersecurity Framework *Anomalies and Events* Category
AIRES	Automated Integrated Regulatory Examination System
AN	NIST Cybersecurity Framework *Analysis* Category
Assessment	Cybersecurity Assessment Tool
CEG	Cybersecurity Examination Guide
CFR	Code of Federal Regulations
CM	NIST Cybersecurity Framework Security *Continuous Monitoring* Category
CO	NIST Cybersecurity Framework *Communications* Category
DE	NIST Cybersecurity Framework *Detect* Function
DP	NIST Cybersecurity Framework *Detection Processes* Function
E&I	Office of Examination and Insurance
FCU	Federal Credit Union
FFIEC	Federal Financial Institutions Examination Council
FICU	Federally Insured Credit Union
GLBA	Gramm-Leach-Bliley Act
GV	NIST Cybersecurity Framework *Governance* Category
ID	NIST Cybersecurity Framework *Identify* Function
InfoSec	Information Security
ISP	Information Security Program
IDS/IPS	Information Detection System/Intrusion Prevention System
IT	Information Technology
LCU	Letter to Federally Insured Credit Unions
MI	NIST Cybersecurity Framework *Mitigation* Category
NCUA	National Credit Union Administration

Acronyms & Abbreviations (Continued)

NCUA control measures	ACET Declarative Statements
NIST	National Institute of Standards and Technology
NIST control guidelines	NIST Cybersecurity Framework Subcategories
OIG	Office of the Inspector General
PR	NIST Cybersecurity Framework *Protect* Function
RFE	Risk-Focused Examination
RS	NIST Cybersecurity Framework Response Function
VPN	Virtual Private Network