©2015 CliftonLarsonAllen LLP

# FFIEC's 2014 Cybersecurity Assessments: Findings and Recommendations

Amy McHugh, Senior Consultant

CliftonLarsonAllen

CLAconnect.com

# Disclaimers

*The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.*

©2015 CliftonLarsonAllen LLP

# Housekeeping

- If you are experiencing technical difficulties, please dial: **800-422-3623.**

- **Q&A session will be held at the end of the presentation.**
  - Your questions can be submitted via the **Questions Function at any time during the presentation.**

- The **PowerPoint presentation,** as well as the **webinar recording,** will be sent to you within the next 10 business days.

- Please complete our online survey.

©2015 CliftonLarsonAllen LLP

# CPE Requirements

- Answer the polling questions

- If you are participating in a group, complete the CPE sign-in sheet and return within two business days
  - Contact sada.kempf@CLAconnect.com

- Allow four weeks for receipt of your certificate; it will be sent to you via email

** This webinar, once recorded, has not been developed into a self study course. Therefore, watching the recording will not qualify for CPE credit.*

©2015 CliftonLarsonAllen LLP

# About CliftonLarsonAllen

- A professional services firm with three distinct business lines
  - Wealth Advisory
  - Outsourcing
  - Audit, Tax, and Consulting
- 3,600 employees
- Offices coast to coast
- Serve more than 1,100 financial institutions

©2015 CliftonLarsonAllen LLP

# Speaker Introduction

- **Amy McHugh, JD, CISA, Network+, Security+**
  - Senior Associate, IT Consulting
  - Areas of Specialization include:
    - ◊ Information Security Regulatory Compliance Consulting and Auditing
    - ◊ Electronic Banking Consulting and Auditing
    - ◊ Information Security Risk Assessment and Policy Development
    - ◊ Vendor Management and Contract Review
    - ◊ Emerging Payments and Technologies

©2015 CliftonLarsonAllen LLP

# Learning Objectives

- At the end of this session, you will be able to:
  - Understand why there is an increased emphasis on cybersecurity
  - Describe the elements and results of the 2014 Cybersecurity Assessments
  - Expand your current information security program to incorporate the FFIEC's preliminary cybersecurity assessment recommendations

©2015 CliftonLarsonAllen LLP

©2015 CliftonLarsonAllen LLP

# Executive Order 13636

## Improving Critical Infrastructure Cybersecurity

# Executive Order 13636

## Improving Critical Infrastructure Cybersecurity

- Issued on February 12, 2013
- The cyber threat to **critical infrastructure** … represents one of the most serious national security challenges…to the national and economic security of the US
  - Enhance the security and resilience of the Nation's critical infrastructure
  - Maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.
  - Partnership with the owners and operators of critical infrastructure

©2015 CliftonLarsonAllen LLP

# Executive Order 13636

## Improving Critical Infrastructure Cybersecurity

- Definition of Critical Infrastructure
  - Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

©2015 CliftonLarsonAllen LLP

# Executive Order 13636

## Improving Critical Infrastructure Cybersecurity

- Cybersecurity Information Sharing
  - Increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities
  - The Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence shall each issue instructions … to ensure the timely production of unclassified reports of cyber threats that identify a specific targeted entity.
    - ◊ Also includes the dissemination of classified reports to authorized critical infrastructure entities.
    - ◊ Will establish a system for tracking the production, dissemination, and disposition of these reports.

©2015 CliftonLarsonAllen LLP

# Executive Order 13636

## Improving Critical Infrastructure Cybersecurity

- Cybersecurity Information Sharing (cont.)
  - **<u>Voluntary</u> information sharing program** to provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers
  - Expedite the processing of security clearances to critical infrastructure personnel
  - Expand the use of programs that bring private sector SMEs into Federal service
- Privacy and Civil Liberties Protections
- Consultative Process

©2015 CliftonLarsonAllen LLP

# Executive Order 13636

## Improving Critical Infrastructure Cybersecurity

- Baseline Framework to Reduce Cyber Risk to Critical Infrastructure
  - NIST to lead the development of a framework to reduce cyber risks to critical infrastructure (the "**Cybersecurity Framework**").
    - ◊ A set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks
    - ◊ Incorporates voluntary consensus standards and industry best practices
    - ◊ Consistent with voluntary international standards when appropriate

©2015 CliftonLarsonAllen LLP

# Executive Order 13636

## Improving Critical Infrastructure Cybersecurity

- Baseline Framework to Reduce Cyber Risk to Critical Infrastructure (cont.)
  - The Cybersecurity Framework shall:
    - ◊ Provide a prioritized, flexible, repeatable, performance-based, and cost effective approach to identify, assess, and manage cyber risk.
    - ◊ Focus on cross-sector security standards and guidelines
    - ◊ Identify areas for improvement
    - ◊ Technology-neutral guidance
    - ◊ Guidance for measuring implementation of the Cybersecurity Framework.

©2015 CliftonLarsonAllen LLP

# Executive Order 13636

## Improving Critical Infrastructure Cybersecurity

- Identification of Critical Infrastructure at Greatest Risk
  - Risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.
    - ◊ Expertise of Sector-Specific Agencies.
    - ◊ Application of consistent, objective criteria in identifying such critical infrastructure.
    - ◊ **Shall not** identify any commercial information technology products or consumer information technology services ….
    - ◊ Review and update the list of identified critical infrastructure on an annual basis

©2015 CliftonLarsonAllen LLP

# Executive Order 13636

## Improving Critical Infrastructure Cybersecurity

- Adoption of Cybersecurity Framework
  - Responsible agencies shall review sufficiency of the preliminary Cybersecurity Framework with DHS, OMB, and National Security personnel
  - Two years after publication of the final Cybersecurity Framework, agencies shall report on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements.

©2015 CliftonLarsonAllen LLP

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

## Improving Critical Infrastructure Cybersecurity

# Cybersecurity Framework

**NIST's Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (February 12, 2014)**

- Provides a common taxonomy and mechanism for organizations to:
  - Describe their current cybersecurity posture;
  - Describe their target state for cybersecurity;
  - Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
  - Assess progress toward the target state;
  - Communicate among internal and external stakeholders about cybersecurity risk.
- **Does not replace an organization's risk management process and cybersecurity program.**

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

## Critical Infrastructure Sectors and Agency Oversight

- Chemical
  - Department of Homeland Security
- Commercial Facilities
  - Department of Homeland Security
- Communications
  - Department of Homeland Security
- Critical Manufacturing
  - Department of Homeland Security
- Dams
  - Department of Homeland Security
- Defense Industrial Base
  - Department of Defense
- Emergency Services
  - Department of Homeland Security
- Energy
  - Department of Energy
- **Financial Services**
  - **Department of the Treasury**
- Food and Agriculture
  - Department of Agriculture
  - Department of Health and Human Services
- Government Facilities
  - Department of Homeland Security
  - General Services Administration
- Healthcare and Public Health
  - Department of Health and Human Services
- Information Technology
  - Department of Homeland Security
- Nuclear Reactors, Materials, and Waste
  - Department of Homeland Security
- Transportation Systems
  - Department of Homeland Security
  - Department of Transportation
- Water and Wastewater Systems
  - Environmental Protection Agency

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

- Cybersecurity Framework identifies "**areas for improvement**"
  - **Authentication**
    - ◊ Poor authentication mechanisms are a commonly exploited vector of attack by adversaries
    - ◊ Multifactor Authentication
      - Something you know
      - Something you have
      - Something you are
    - ◊ User AND automated device authentication
    - ◊ Inadequacy of passwords

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

- Cybersecurity Framework identifies "**areas for improvement**"
  - **Automated Indicator Sharing**
    - ◊ Timely, actionable information to detect/respond to cybersecurity events as they are occurring.
    - ◊ Sharing indicators based on information discovered prior to and during incident response activities enables other organizations to deploy measures to detect, mitigate, and possibly prevent attacks as they occur.
  - **Conformity Assessment**
    - ◊ Show that a product, service, or system meets requirements for managing cybersecurity risk.
    - ◊ Enhance an organization's understanding of its implementation of a Framework profile

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

- Cybersecurity Framework identifies "**areas for improvement**"
  - **Cybersecurity Workforce**
    - ◊ To meet the unique cybersecurity needs of critical infrastructure
    - ◊ Shortage of qualified cybersecurity experts who understand challenges posed to critical infrastructure
  - **Data Analytics**
    - ◊ Big data and the associated analytic tools coupled with the emergence of cloud, mobile, and social computing
    - ◊ Address issues such as situational awareness of complex networks and large-scale infrastructures
    - ◊ Address issues of provenance, attribution, and discernment of attack patterns

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

- Cybersecurity Framework identifies "**areas for improvement**"
  - **Federal Agency Cybersecurity Alignment**
    - The Federal Information Security Management Act (FISMA) requires federal agencies to implement agency-wide information security programs
    - FISMA directed NIST to develop standards and guidelines to provide a Risk Management Framework to guide agencies
    - The Cybersecurity Framework and NIST Risk Management Framework address management of cybersecurity risk
  - **International Aspects, Impacts, and Alignment**
    - Domestic and international organizations can use the Framework to operate and manage new and evolving risks

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

- Cybersecurity Framework identifies "**areas for improvement**"
  - **Supply Chain Risk Management**
    - ◊ Greater awareness and understanding of the risks associated with the time-sensitive interdependencies throughout the supply chain
  - **Technical Privacy Standards**
    - ◊ The lack of risk management models, standards, and privacy metrics, makes it difficult to assess the effectiveness of an organization's privacy protection methods.

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework Elements

- **Framework Core**
  - Set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles
- **Framework Implementation Tiers**
  - A mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk
- **Framework Profiles**
  - Help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework Elements

- **NOT "one-size-fits-all"** – multiple industries, international
  - Organizations have different threats, vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary.
  - Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent.
- Living document
- Voluntary…?

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework Core

| Functions | Categories | Subcategory | Informative References |
|---|---|---|---|
| IDENTIFY | Asset Management | | |
| | Business Environment | | |
| | Governance | | |
| | Risk Assessment | | |
| | Risk Management Strategy | | |
| PROTECT | Access Control | | |
| | Awareness and Training | | |
| | Data Security | | |
| | Information Protection Processes and Procedures | | |
| | Maintenance | | |
| | Protective Technology | | |
| DETECT | Anomalies and Events | | |
| | Security Continuous Monitoring | | |
| | Detection Processes | | |
| RESPOND | Response Planning | | |
| | Communications | | |
| | Analysis | | |
| | Mitigation | | |
| | Improvements | | |
| RECOVER | Recovery Planning | | |
| | Improvements | | |
| | Communications | | |

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework Implementation Tiers

- Provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.
  - Tier 1 – Partial
  - Tier 2 – Risk Informed
  - Tier 3 – Repeatable
  - Tier 4 – Adaptive
- Organizations determine the desired Tier based on goals, feasibility, reducing risk to acceptable levels.
- Tiers do not represent maturity levels. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective.

©2015 CliftonLarsonAllen LLP

# How to Use the Cybersecurity Framework

- Establishing or Improving a Cybersecurity Program
  - Step 1: Prioritize and Scope
  - Step 2: Orient
  - Step 3: Create a Current Profile
  - Step 4: Conduct a Risk Assessment
  - Step 5: Create a Target Profile
  - Step 6: Determine, Analyze, and Prioritize Gaps
  - Step 7: Implement Action Plan

©2015 CliftonLarsonAllen LLP

# How to Use the Cybersecurity Framework

## Communicating Cybersecurity Requirements with Stakeholders

- The Cybersecurity Framework provides a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure services

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

## **Update on the Cybersecurity Framework** (December 5, 2014)

- RFI (August 26, 2014) and Sixth Cybersecurity Framework Workshop, University of South Florida (October 29-30, 2014)
  - Focused on the use of the Framework and sector-specific guidance
- **Sector Awareness**
  - General Awareness of the Framework, but need additional government- and industry-led efforts to expand awareness
  - Need real-world applications, lessons learned, case studies, and mapping of existing standards to the Framework

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

## Update on the Cybersecurity Framework (December 5, 2014)

- **Initial Experiences Using the Framework**
  - Raising awareness and communicating with stakeholders
  - Improving communications across organizations
  - Framework core mappings show alignment with standards, guidelines, best practices, and **regulatory requirements**.
  - Strategic planning tool
  - Benchmark performance within the organization
  - Need "Getting started" guides, case studies, terminology etc. in common public repository

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

## Update on the Cybersecurity Framework (December 5, 2014)

- **Framework Updates**
  - Too early; more time is needed to understand and use
  - NIST will consider producing additional guidance
- **Small/Medium-Sized Businesses**
  - Challenging for some organizations that without existing cybersecurity programs
  - May benefit from incremental, iterative application of the Framework
  - Need specific guidance from NIST and Sector-Specific Agencies due to limited resources

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

## Update on the Cybersecurity Framework (December 5, 2014)

- **Regulation and Regulatory Concerns**
  - Concerned that agencies/Congress will make the Framework mandatory as a compliance mechanism
  - Increased outreach to regulators for a consistent understanding of the Framework and to reinforce that it is voluntary and not designed to create additional regulation
- **Guidance and Metrics/Measurability**
  - Value of additional guidance about how to use the Framework and real-world examples
- **International Aspects, Impacts, and Alignments**
  - Global alignment is important to avoid confusion, duplication of effort, and conflicting expectations
  - Important to have international standards

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

## Update on the Cybersecurity Framework (December 5, 2014)

- **Roadmap**
  - Authentication
    - ◊ High-risk area and need better coverage of advances in authentication solutions
    - ◊ Tailor to each organization's needs
  - Automated Indicator Sharing
    - ◊ Interest in real-time indicator sharing, in-context threat intelligence, and integration of tailored intelligence in risk management practices
    - ◊ Legal issues with sharing private sector information
    - ◊ Draft of **NIST Special Publication 800-150 (SP 800-150)** on cyber threat information sharing

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

## Update on the Cybersecurity Framework (December 5, 2014)

- **Roadmap**
  - Supply Chain and Conformity Assessment
    - ◊ Supply Chain Risk Management recognized as a serious concern
    - ◊ Develop private sector and industry-specific conformity assessment activities
  - Cybersecurity Workforce
    - ◊ Critical to attract and retain a multidisciplinary cybersecurity workforce, but should be addressed outside of the Framework
    - ◊ Connect educators to industry
    - ◊ Public-Private Sector efforts
  - Standards Supporting the Framework
    - ◊ Encourage alignment among standards already in use
    - ◊ Framework's direct mapping to ISO/IEC 27001 and NIST SP 800-53

©2015 CliftonLarsonAllen LLP

# Cybersecurity Framework

## Update on the Cybersecurity Framework (December 5, 2014)

- **Roadmap**
  - Privacy Methodology
    - ◊ Whether organizations were implementing the privacy and civil liberties methodology and any benefits/concerns
    - ◊ Integration of privacy compliance programs with cybersecurity programs
  - Next Steps
    - ◊ NIST will continue efforts to raise awareness of the Framework
    - ◊ Priority to develop and disseminate information and training materials and aligning Framework with business processes
    - ◊ Explore options for public information depository and training

©2015 CliftonLarsonAllen LLP

©2015 CliftonLarsonAllen LLP

# Cybersecurity Assessments

July – August 2014

# Current FFIEC IT Examination Process

- Each FFIEC agency (FDIC, Federal Reserve, OCC, NCUA) perform periodic information technology examinations at regulated financial institutions.
- Examination procedures are based on the FFIEC IT Handbooks (http://ithandbook.ffiec.gov/) and supplemented by periodic agency guidance.
- IT Examinations review the financial institution's Information Security Program.

©2015 CliftonLarsonAllen LLP

# Information Security Program

- Section 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLBA) for the safeguarding of customer information
  - Board of Directors will develop an **Information Security Program** that addresses the requirements of:
    - ◊ Section 501(b) of the GLBA;
    - ◊ Federal Financial Institutions Examination Council's (FFIEC) "Interagency Guidelines Establishing Information Security Standards" (501[b] Guidelines); and
    - ◊ Agency-specific guidelines (i.e. Appendix B to Part 364 of the FDIC's Rules and Regulations)
- The Information Security Program is comprised of:
  - Risk Assessment
  - Risk Management
  - Audit
  - Business Continuity/Disaster Recovery/Incident Response
  - Vendor Management
  - Board and Committee Oversight

©2015 CliftonLarsonAllen LLP

# Information Security Program

## Risk Assessment and Risk Management

- Assess risk periodically to identify reasonably foreseeable internal and external threats to data and information technology assets that could negatively impact confidentiality and integrity of data and/or availability of systems.
- Risk is determined based on the likelihood of a given threat-source's ability to exercise a particular potential vulnerability, and the resulting impact of that adverse event on the organization.
- The results of the risk assessment are used as a basis for establishing and implementing appropriate administrative, technical, and physical controls to reduce or eliminate the impact of the threat.

©2015 CliftonLarsonAllen LLP

# Information Security Program
## Audit

- ISP-related Audits/Reviews
  - ISP Review/IT General Controls Review
  - External/Internal Vulnerability and Penetration Assessments
  - Social Engineering Assessments
    - Phishing
    - Pretext calling
    - In person
    - Seeding
- E-Banking Reviews
  - ACH Audit
  - Wire Transfer Audit
  - Remote/Mobile Deposit Capture Audit
- Audit/Exam Recommendation Tracking/Reporting

©2015 CliftonLarsonAllen LLP

# Information Security Program
## Business Continuity/Disaster Recovery Incident Response

- Business Continuity/Disaster Recovery Plan
  - Annual Testing of Critical Systems
  - Annual Employee Tabletop/Scenario Testing
  - Board Reporting
- Incident Response Plan
  - Compromise of customer information
  - Annual Testing
  - FS-ISAC
  - Cybersecurity Examinations?

©2015 CliftonLarsonAllen LLP

# Information Security Program
## Vendor Management

- Vendor Management Policy
- Vendor Risk Assessment
  - Access to Customer Information
  - Criticality to Bank Operations
  - Ease of Replacement
- New Vendor Due Diligence and Annual Reviews
- Continuous Monitoring

©2015 CliftonLarsonAllen LLP

# Information Security Program
## Board and Committee Oversight

- Information Technology Steering Committee
- Board of Directors
  - *May 7, 2014 FFIEC Executive Leadership Cybersecurity webinar*
    - ◊ Importance of identifying emerging cyber threats and the need for Board/C-suite involvement, including:
      - Setting the tone at the top and building a security culture
      - Identifying, measuring, mitigating, and monitoring risks
      - Developing risk management processes commensurate with the risks and complexity of the institutions
      - Aligning cybersecurity strategy with business strategy and accounting for how risks will be managed now and in the future
      - Creating a governance process to ensure ongoing awareness and accountability
      - Ensuring timely reports to senior management that include meaningful information addressing the institution's vulnerability to cyberrisks

©2015 CliftonLarsonAllen LLP

# FFIEC Cybersecurity Assessments

- In the summer of 2014, the Federal Financial Institutions Examination Council (FFIEC) agencies piloted new Cybersecurity Assessment procedures at over 500 community financial institutions to raise awareness of and evaluate their preparedness to mitigate cybersecurity risks.
- Integrated into regular IT Examination process
  - Cyber Risk Management and Oversight
  - Cyber Security Controls
  - External Dependency Management
  - Threat Intelligence and Collaboration
  - Cyber Resilience
- Launched a cybercrime website https://www.ffiec.gov/cybersecurity.htm

©2015 CliftonLarsonAllen LLP

# FFIEC Cybersecurity Assessments

## FFIEC Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement (11/3/14)

- All FIs AND their critical technology service providers must have appropriate **threat identification, information sharing, and response procedures**.
- Recommendation to participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC)
  - Improved identification and mitigation of attacks
  - Better identification and understanding of specific vulnerabilities and necessary mitigating controls for systems
  - Sharing information to help other FIs

©2015 CliftonLarsonAllen LLP

# FFIEC Cybersecurity Assessments

## FFIEC Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement (11/3/14)

- FI Management should:
  - Monitor and maintain sufficient awareness of cybersecurity threats and vulnerability information so they may evaluate risk and respond accordingly
  - Establish procedures to evaluate and apply the various types and quantity of cyber threat and vulnerability information to meet the needs of their organization
    - ◊ FS-ISAC: www.fsisac.com
    - ◊ FBI Infragard: www.infragard.org
    - ◊ U.S. Computer Emergency Readiness Team at US-CERT: www.us-cert.gov
    - ◊ U.S. Secret Service Electronic Crimes Task Force: www.secretservice.gov/ectf.shtml

©2015 CliftonLarsonAllen LLP

# FFIEC Cybersecurity Assessments

## FFIEC Cybersecurity Assessment General Observations

- **Cybersecurity Inherent Risk**
  - Management must understand the FIs INHERENT RISK when assessing cybersecurity preparedness
    - ◊ **Connection Types:** identify and assess the threats to all access points to the internal network
      - VPN
      - Wireless
      - Telnet/FTP
      - Vendor LAN/WAN access
      - BYOD

©2015 CliftonLarsonAllen LLP

# FFIEC Cybersecurity Assessments

## FFIEC Cybersecurity Assessment General Observations

- **Cybersecurity Inherent Risk (cont.)**
  - Management must understand the FIs INHERENT RISK when assessing cybersecurity preparedness
    - ◊ **Products and Services:** identify and assess threats to all products and services currently offered and planned
      - Online ACH and Wire Transfer origination
      - External funds transfers (A2A, P2P, bill pay)

©2015 CliftonLarsonAllen LLP

# FFIEC Cybersecurity Assessments

## FFIEC Cybersecurity Assessment General Observations

- **Cybersecurity Inherent Risk (cont.)**
  - Management must understand the FIs INHERENT RISK when assessing cybersecurity preparedness
    - ◊ **Technologies Used**: identify and assess threats to all technologies currently used and planned
      - Core systems
      - ATMs
      - Internet and mobile applications
      - Cloud computing

©2015 CliftonLarsonAllen LLP

# FFIEC Cybersecurity Assessments

## FFIEC Cybersecurity Assessment General Observations

- **Cybersecurity Preparedness**
  - Current cybersecurity practices and overall preparedness should include:
    - ◊ **Risk Management and Oversight**: Governance, allocation of resources, employee, and BOARD training and awareness
      - Set a "tone from the top" includes regular board and senior management discussion of an involvement in cyber and information security programs
      - Ongoing employee training and testing, including social engineering attack vectors

©2015 CliftonLarsonAllen LLP

# FFIEC Cybersecurity Assessments

## FFIEC Cybersecurity Assessment General Observations

- **Cybersecurity Preparedness**
  - Current cybersecurity practices and overall preparedness should include:
    - ◊ **Cybersecurity Controls**: Preventive, detective, or corrective procedures for mitigating identified cybersecurity threats
      - Patching, encryption, limited user access
      - Intrusion detection/prevention systems, firewall alerts
      - Formal audit program with scope and schedule based on an asset's inherent risk, prompt and documented remediation of findings, regular activity report reviews

©2015 CliftonLarsonAllen LLP

# FFIEC Cybersecurity Assessments

## FFIEC Cybersecurity Assessment General Observations

- **Cybersecurity Preparedness**
  - Current cybersecurity practices and overall preparedness should include:
    - ◊ **Cyber Incident Management and Resilience**: Incident detection, response, mitigation, escalation, reporting, and resilience
      - Formal Incident Response Programs, including regulatory and customer notification guidelines and procedures
      - Senior management and board incident reporting

©2015 CliftonLarsonAllen LLP

# FFIEC Cybersecurity Assessments

## FFIEC Cybersecurity Assessment Implications?

- Increased Board and C-Suite Involvement
  - Periodic information security and cybersecurity training
  - Expanded reporting on information security and cybersecurity issues
- Participation in information-sharing group(s)
  - FS-ISAC
  - Industry groups (American Banker Association, state banking associations)
  - Local/state/regional peer groups
- Cybersecurity scenario testing with employees and management
  - Incident Response Scenario Testing
  - FS-ISAC Cyber Attack (against) Payment Processes (CAPP) Exercise (https://www.fsisac.com/fs-isac-cyber-attack-against-payment-processes-capp-exercise)

©2015 CliftonLarsonAllen LLP

# FFIEC Cybersecurity Assessments

## FFIEC Cybersecurity Assessment Implications? (cont.)

- Increased oversight of third-party service providers
  - Risk assess ALL vendors
  - Obtain vendor information security, incident response, and business continuity/disaster recover policies and security test results
  - SSAE 16 SOC 2 reviews, including a review of "User Control Considerations" section and auditor findings and management's responses
  - Service Level Agreement (SLA) monitoring
- Document how the FI is addressing the FFIEC Cybersecurity Assessment findings
  - Review the FFIEC Cybersecurity Assessment General Observations (http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf)
  - Monitor the FFIEC's Cybersecurity Awareness website (http://www.ffiec.gov/cybersecurity.htm) for updates

©2015 CliftonLarsonAllen LLP

©2015 CliftonLarsonAllen LLP

# Questions?

©2013 CliftonLarsonAllen LLP

# Thank you!

Amy McHugh
319-558-0275
amy.mchugh@CLAconnect.com