Nonbank Cyber and IT Examination Program
American Association of Residential Mortgage Regulators // August 7, 2019
TODAY’S PRESENTERS

Chuck Cross  - SVP Nonbank Supervision & Enforcement, CSBS

Jessica Ruzic  - Senior Information Security Policy Analyst, CSBS
MORTGAGE POLICY SUMMIT

Save the Date: AARMR and CSBS are hosting a National Mortgage Policy Summit on November 13.

Learn More
The American Association of Residential Mortgage Regulators (AARMR) and CSBS will host a summit to bring together policymakers, regulators and the industry to elevate the discussion around mortgage policy on November 13 at Jones Day in Washington, DC.

The summit event will include keynote presentations and panels representing viewpoints on mortgage policy at the national level. Invited speakers include members of Congress, federal agency leadership, industry leaders, consumer advocates, state regulators and other policy stakeholders.
Nonbank Cyber and IT Examination Program
CSBS Initiatives

Train Nonbank Examiners in Cybersecurity/IT - $1.5 million commitment

Develop a cybersecurity model law or regulation for states to adopt

Develop a cybersecurity/IT work program that would cover all nonbanks

Conduct industry outreach and education
Work Group Established

Develop a cybersecurity work program applicable to all nonbanks

Drawing from existing expertise on the banking side and utilizing what already was in use: Bank, MTRA, etc.

Establish a work group of both bank and nonbank experts
WORKING GROUP OVERVIEW

Background

In 2018, the CSBS Board of Directors tasked the State Supervisory Processes Committee with developing cyber exam procedures for all nonbank institutions.

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matthew Fujikawa</td>
<td>CA</td>
</tr>
<tr>
<td>Robert Lipot</td>
<td>CA</td>
</tr>
<tr>
<td>Spenser Staton</td>
<td>IL</td>
</tr>
<tr>
<td>Kevin Stouder</td>
<td>IN</td>
</tr>
<tr>
<td>Holly Chase</td>
<td>MA</td>
</tr>
<tr>
<td>Henry Hallman</td>
<td>NC</td>
</tr>
<tr>
<td>Denise Sandy</td>
<td>PA</td>
</tr>
<tr>
<td>Crystal Flaten</td>
<td>WA</td>
</tr>
<tr>
<td>Hung Nguyen</td>
<td>WA</td>
</tr>
<tr>
<td>Phillip Hinkle</td>
<td>TX</td>
</tr>
<tr>
<td>Chuck Cross</td>
<td>CSBS</td>
</tr>
<tr>
<td>Mary Beth Quist</td>
<td>CSBS</td>
</tr>
<tr>
<td>Mike Bray</td>
<td>CSBS</td>
</tr>
<tr>
<td>Jessica Ruzic</td>
<td>CSBS</td>
</tr>
</tbody>
</table>
WORKING GROUP OVERVIEW // Process

- Met in-person and online from September 2018 – July 2019
- Leveraged expertise from banking supervision, nonbank, and cybersecurity worlds
- Considerations
  - Wide variety of nonbank institution types
  - Varying state standards
  - Varying degrees of state oversight
  - State resources
  - Versatility and helpfulness
• Discussed what cyber standard would be most comprehensive, understandable, and widely recognized
  • Washington State, CAT, InTREX, CIS Top 20, and NIST 800-53
• Settled on NIST Cybersecurity Framework (CSF)
  • **Capability-based**: Identify, Protect, Detect, Respond, and Recover
  • Allows for true **risk management** and **threat prioritization**
  • Closest to a living, breathing standard
National Institute of Standards and Technology

Cybersecurity Framework

- Recover
- Identify
- Protect
- Respond
- Detect

5 Year Anniversary
WORKING GROUP OVERVIEW // Process

- Mapped all other standards to the NIST CSF
- Created questions for missing CSF capabilities
Sorted all questions into Identify, Protect, Detect, Respond, and Recover
Eliminated duplicates
Adjusted stringency of requirements
Ended up with 147 controls/exam questions
WORKING GROUP OVERVIEW // Process

- Explained the reasoning behind each question
  - Cyber, IT, and/or nonbank examiners
  - Useful for communication with entity employees
WORKING GROUP OVERVIEW // Process

- Established **core controls**, which are mandatory for every exam
  - Establish minimum level of acceptable cybersecurity
  - Primary emphasis on Identify and Protect (preparation)
  - 74/147 core
- Identified controls for which examination is optional (but encouraged)
  - Decision left to Examiner based on personal expertise, previous exam results, state priorities, and current events
  - 73/147 non-core
WORKING GROUP OVERVIEW // Result

- Pre-Exam Questionnaire
  - Entity IT and information security information
  - POCs
  - Document Request List

- Nonbank Cyber and IT Workprogram
  - Sorted by NIST function
  - Document Request Checklist
  - Questionnaire Information (including suggestions for non-core controls)
  - Customizable within each worksheet

- No standardized report
WALKTHROUGH

Questionnaire and Customizable Workprogram
TRAINING, FEEDBACK,& REVISIONS // Training

• COMING SOON!
• Regulator and industry webinars, handouts, and trainings
• Happening Now: 2019 Conferences

<table>
<thead>
<tr>
<th>Conference</th>
<th>Dates</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>AARMR Annual Conference</td>
<td>August 5-8</td>
<td>San Diego, CA</td>
</tr>
<tr>
<td>CSBS IT/Cyber Risk</td>
<td>September 9-12</td>
<td>Portland, ME</td>
</tr>
<tr>
<td>MTRA Annual Conference</td>
<td>September 9-13</td>
<td>Pittsburgh, PA</td>
</tr>
<tr>
<td>NACARA Annual Conference</td>
<td>September 16-18</td>
<td>Santa Fe, NM</td>
</tr>
</tbody>
</table>
TRAINING, FEEDBACK,& REVISIONS // Feedback & Revisions

• “Agile” process
• Available for use beginning August/September 2019
  • Emailed out
  • Posted on website (password protected)
• Send feedback to targeted CSBS mailbox (TBD)
  • Reviewed at end of each month
Find the web version and downloadable PDF at:

HTTPS://WWW.CSBS.ORG/CYBER101
QUESTIONS?