Overview

- Cybersecurity Threat Update
- Information Security Examination & Cybersecurity Assessment Program
- Guidance and Risk Alerts
- Cybersecurity Resources Webpage
- Industry Outreach and Partner Engagement
Cybersecurity Threat Update

Threat Environment

Cyber Risks
- Ransomware
- Supply Chain Vulnerabilities
- Business Email Compromises

FBI Internet Crime Complaint Center
Cybersecurity Risks - Ransomware

- **Upward Trend**
- **10% of All Cyber Breaches**
- **FS-ISAC – “Amongst Largest Cybersecurity Threats”**
- **Shifted to Exfiltration of Sensitive Data**
- **Threats to Publicize Company Data**
- **Enabled by Cryptocurrency**

* 2021 Verizon Data Breach Investigations Report - DBIR Incident Classification Patterns*
Third party/supply chain risk will dominate threat landscape discussions

- FS-ISAC Annual Cyber Threat Review (2021)
Cybersecurity Risks – Business Email Compromise

Business Email Compromise

- 19,369 Complaints
- Adjusted Losses - Over $1.8 billion
- Targeted both businesses and individuals

*FBI Internet Crime Complaint Center - Internet Crime Report 2020*
Information Security and Cybersecurity Assessment Program

NCUA Maturity Assessment + NCUA Examination based on NCUA Rules
The Toolbox

Automated Cybersecurity Evaluation Toolbox
• Maturity Assessment
• Ransomware Readiness Assessment

Statements
Cyber Risk Management & Oversight
Governance

Stmt 1: Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs.
## Cybersecurity Maturity

<table>
<thead>
<tr>
<th>Domain</th>
<th>Maturity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain 1: Cyber Risk Management &amp; Oversight</td>
<td>Baseline</td>
</tr>
<tr>
<td>Domain 2: Threat Intelligence &amp; Collaboration</td>
<td>Baseline</td>
</tr>
<tr>
<td>Domain 3: Cybersecurity Controls</td>
<td>Baseline</td>
</tr>
<tr>
<td>Domain 4: External Dependency Management</td>
<td>Baseline</td>
</tr>
<tr>
<td>Domain 5: Cyber Incident Management and Resilience</td>
<td>Baseline</td>
</tr>
</tbody>
</table>
Information Security Examination Program

Information Security and Cybersecurity Assessment Program
Guidance and Risk Alerts

- FFIEC Authentication Guidance
- Business Email Compromise Risk Alert
- FFIEC Architecture, Infrastructure and Operations (AIO) Handbook
Cybersecurity Resources Webpage

UPDATING CYBERSECURITY RESOURCES WEBPAGE

PROVIDING ADDITIONAL CYBERSECURITY TOOLS AND RESOURCES
Supply Chain Vulnerabilities and Cyber Hygiene

Oct. 14, 2021

TBD, 2021

Ransomware: Law Enforcement Perspective

Oct. 28, 2021

Automated Cybersecurity Evaluation Toolbox

Nov. 3, 2021

Authentication Guidance Webinar
Architecture, Infrastructure, and Operations Webinar
ncua.gov/cybersecurity
Office Contact Page

Office of Examination and Insurance

eimail@ncua.gov

(703) 518-6360