FFIEC Cybersecurity Resource Guide
Use of these materials by participants, including video and audio recording of this presentation, is strictly prohibited except by written permission of the FFIEC or its members.¹ The views expressed in this presentation are individual views, intended for informational purposes, and are not formal opinions of, nor binding on, the FFIEC or its members.

¹Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, National Credit Union Administration, and State Liaison Committee.
Introductory Remarks

Mary Aiken
Federal Reserve Board of Governors
The Cyber Security Resources Guide

Ernie Chambers
Description of the Guide

- Assessment Resources
- Exercises Resources
- Information Sharing Resources
- Response and Reporting Resources
Assessment Resources

- Department of Homeland Security’s (DHS) Nation Cybersecurity and Technical Services, (NCATS)
- DHS’s Cyber Resilience Review (CRR)
- Center for Internet Security (CIS) Benchmarking Resources
DHS National Cybersecurity Assessments and Technical Services

- NCATS supports U.S. government and industry critical infrastructure by providing proactive testing and assessment services.
- Its Cyber Hygiene program aims to secure internet accessible systems by continuously scanning for known vulnerabilities and configuration errors.
- NCATS services are available at no cost to financial institutions.
The Cyber Resilience Review (CRR) is a free, voluntary, and non-technical tool for assessing an organization’s operational resilience and cybersecurity practices.
Center for Internet Security

• CIS Benchmarks: 100+ configuration guidelines for various technology groups to safeguard systems cyber threats.

• CIS Configuration Assessment Tool: A detailed assessment of systems in conformance with CIS Benchmarks.
Exercise Resources

• FDIC *Cyber Challenge: A Community Bank Cyber Exercise*
• Financial Sector Cyber Exercise Template
• FS-ISAC Cyber Attack Against Payment Systems (CAPS) Exercise
FDIC Cyber Challenge: A Community Bank Cyber Exercise

• The FDIC created unique scenarios, cyber challenges, to encourage community financial institutions to discuss operational risk issues and the potential impact of information technology disruptions on common banking functions.
Financial Sector Cyber Exercise Template

• The Financial Sector Cyber Exercise Template is designed for smaller financial sector institutions to test their preparedness.

• The template helps institutions run their own internal cyber exercises and facilitates discussion on how best to engage with the national architecture for coordinating responses to significant cybersecurity incidents among government and industry.
FS-ISAC Cyber-Attack Against Payment Systems (CAPS) Exercise

• FS-ISAC CAPS exercise is a two-day, tabletop exercise held annually that simulates an attack on payment systems and processes.

• The exercise is free and open to non-FS-ISAC members.
Information Sharing Resources

• DHS Automated Information Sharing Program
• Financial Services Information Sharing and Analysis Center (FS-ISAC)
• Infragard
• National Credit Union Information Sharing and Analysis Organization (NCU-ISAO)
• U.S. Secret Service Electronic Crimes Task Force
• Financial Crimes Task Force
• United States Computer Emergency Readiness Team
The Automated Information Sharing Program, or AIS, is a part of the DHS’s effort to create an ecosystem where as soon as a company or federal agency observes an attempted compromise, indicators can be shared in real time with all partners, protecting them from that particular threat.
Financial Services Information Sharing and Analysis Center (FS-ISAC)

- The FS-ISAC is a global financial industry resource for cyber and physical threat intelligence analysis and sharing.
- Membership in the FS-ISAC is tiered and based upon institution size, but it also offers a free service to provide the most critical public alerts through its Critical Notification Only Participant (CNOP) program.
Infragard

- Infragard is a partnership between the FBI and members of the private sector. Infragard provides a vehicle for seamless public-private collaboration that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure.
National Credit Union Information Sharing and Analysis Organization

- Presidential Executive Order 13691 directed DHS to encourage the development of ISAOs to address information sharing beyond the traditional infrastructure sectors.

- NCU-ISAO’s mission is to enable and sustain credit union critical infrastructure cyber resilience and preserve the public trust by advancing trusted security coordination and collaboration to identify, protect, detect, respond, and recover from threats and vulnerabilities.
Financial Crimes Task Force

- **Electronic Crimes Task Forces:** The mission of this national network is to prevent, detect, and investigate electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

- **Financial Crimes Task Force:** Combines the resources of the private sector and other law enforcement agencies in an organized effort to combat threats to U.S. financial payment systems and critical infrastructures.
United States Computer Emergency Readiness Team

• As part of the NCCIC, the United States Computer Emergency Readiness Team (US-CERT) responds to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world.

• US-CERT regularly publishes timely information about current vulnerabilities, exploits, and other security issues.
Response and Reporting

- DHS Cyber Incident Reporting Guide
- FBI’s Internet Crime Complaint Center (IC3)
- Financial Crimes Enforcement Network (FinCEN)
- Sheltered Harbor
- Reporting to Primary Regulator
The DHS Cyber Incident Reporting Guide provides information on the importance of reporting cyber incidents.

Victims of a cyber incident can receive assistance from government agencies, which are prepared to investigate incidents, mitigate consequences, and help prevent future incidents.
FBI’s Internet Crime Complaint Center (IC3)

- The Internet Crime Complaint Center provides the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.
Financial Crimes Enforcement Network (FinCEN)

• Financial institutions can play an important role in protecting the U.S. financial system from these threats.

• Institutions should determine if filing a Suspicious Activity Report (SAR) is required or appropriate, as in the case of an unauthorized electronic intrusion intended to damage, disable, or otherwise affect critical systems.

• When filing is not required, institutions may file a SAR voluntarily to aid law enforcement in protecting the financial sector.
Sheltered Harbor

- Sheltered Harbor is a voluntary industry initiative launched in 2015 following a series of cybersecurity simulation exercises between public and private sectors, known as the Hamilton Series. Its purpose is to promote the stability and resiliency of the financial sector and to preserve public confidence in the financial system.
Regulatory Reporting

• If a cyber incident results in unauthorized access to or use of sensitive customer information, the institution should notify its primary federal or state regulator(s). In all other instances where institutions are victims of cyber-attacks, they are encouraged to inform law enforcement authorities and notify their primary regulator(s).
DHS Introduction

• Rick Lichtenfels
• Cyber Hygiene Branch Chief
• DHS NCATS
Questions

Patrick Kelly
OCC

Tim Segerson
NCUA

Chris Olson
Federal Reserve Board

James Brignac
FDIC

Jami Flynn
CSBS

Jeff Perdue
BCFP