Recommendations and Resources for Financial Institutions: Enhanced Resiliency and Recovery

American Bankers Association

OCCIP

FS-ISAC

Table of Contents

Executive Summary

This resource provides U.S. financial institutions with recommendations, resources, and operational guidance to enhance resilience for and accelerate recovery from significant cyber, physical, natural-disaster, or third party-driven disruptions.

It was jointly developed by the American Bankers Association (ABA), the Financial Services Information Sharing and Analysis Center (FS-ISAC), and the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), and aligns with financial sector-wide playbooks established by FS-ISAC, the Financial Services Sector Coordinating Council (FSSCC), the Financial and Banking Information Infrastructure Committee (FBIIC), and federal/state regulators.

Significant events — whether cyberattacks, technology outages, natural disasters, or man-made incidents — can affect a financial institution's stability, operations, security, and reputation. This guide[1] provides teams responsible for incident response and crisis management with recommendations and considerations when preparing for and responding to events.

Before an Event: Establishing and building strong relationships with federal and local agencies and industry partners is essential for resilience, and this guide describes how to engage the Cybersecurity and Infrastructure Security Agency (CISA) Cyber Security Advisors (CSA), CISA Protective Security Advisors (PSA), Federal Bureau of Investigation (FBI) InfraGard, Domestic Security Alliance Council (DSAC), FS-ISAC, and regional coalitions. It also highlights planning frameworks and tools from CISA, the National Institutes of Standards and Technology (NIST), Federal Financial Institutions Examination Council (FFIEC), Federal Emergency Management Agency (FEMA), and other organizations to strengthen incident response, business continuity, and operational resilience. Institutions can register for government services including the Department of Homeland Security (DHS) Homeland Security Information Network (HSIN), CISA's no-cost cyber hygiene services, and priority telecommunications programs. Institutions can also participate in exercises offered by FS-ISAC, the Global Resilience Federation (GRF), FEMA, and CISA to identify gaps and validate plans.

During a Significant Event: This guide provides practical steps for how to engage regulators, CISA, FBI, Secret Service, FS-ISAC, and trade associations. It also includes steps on how to implement communication strategies for employees, customers, and external stakeholders. Institutions should be mindful of other considerations including the need to engage legal counsel, collect appropriate information for investigators, and prepare to comply with incident notification and reporting requirements. Firms should also note that incidents may require firms to notify or coordinate with entities outside of U.S. jurisdictions.

Following an Event: The guide outlines actions to comply with incident notification and reporting requirements outlined in the computer security incident notification rule by the Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board, and Office of the Comptroller of the Currency (OCC). It also includes the public disclosure requirements for publicly traded institutions per Securities and Exchange Commission (SEC) rules and requirements outlined in the Cyber Incident Reporting for Critical Infrastructure Act of 2022. Financial institutions must also file suspicious activity reports (SARs) based on criteria outlined in federal regulation and the FFIEC manual. Organizations should then conduct lessons-learned reviews, evaluate response effectiveness, update risk assessments and continuity plans, adjust budgets and strategies, and follow up with law enforcement and regulatory partners.

[1] References to private-sector entities do not equate to an endorsement by the United States Government.

How to Use These Recommendations and Resources

WHY: ABA, FS-ISAC, and Treasury's OCCIP developed these recommendations and resources to help financial institutions prepare for and respond to significant events affecting operations. These recommendations and resources align with the response playbooks developed by FS-ISAC, FSSCC, FBIIC, Treasury, and state and federal regulators.[2] ABA and FS-ISAC are members of FSSCC and facilitate communication and information sharing directly with members and state bankers associations during a large-scale, sector-wide incident.

WHO: These recommendations and resources are intended for individuals and teams who are responsible for developing incident-response and responding to significant cyber incidents, natural disasters, or man-made events.

WHAT: A significant event is a large-scale disruption (or disruptions) that affects, or has the potential to affect, the security, stability, operations, and/or reputation of individual financial institutions and the financial services sector. Crisis managers can prepare for a variety of events by addressing common operational functions in their plans instead of having unique plans for every type of hazard or threat. For example, floods, wildfires, hazardous materials release, and radiological-dispersal devices may cause local, state, or federal officials to issue an evacuation order or to open shelters. Even though each hazard's characteristics (e.g., speed of onset, size of the affected area) are different, some tasks for conducting an evacuation and shelter operations may be the same. Planning for all threats and hazards ensures that, when addressing emergency functions, crisis managers identify common tasks and those responsible for accomplishing the tasks.

HOW: These recommendations are aligned with the FS-ISAC All Hazards Playbook (available from FS-ISAC) and provide-sector members and crisis-response groups with tips on who to contact and what steps to take during significant events, regardless of whether they are industry-wide or financial institution-specific. The federal and state contacts and resources outlined in this document are current as of 2026. However, because many significant events are local, users are encouraged to tailor this document with contacts relevant to their specific regions, municipalities, towns, and/or processes specific to their business continuity, disaster recovery, and incident-response plans.

Each section of this document can be tailored by inserting financial institution- and region-specific text where indicated by chevrons (e.g., "Contact <trade association representatives> and participate in <trade association calls>").

The document concludes with information that institutions can tailor according to the region(s) in which they operate to include state-specific contacts and resources.

Many of the government programs listed below are subject to annual appropriations and may be affected by changes in funding and shifting priorities.

[2] Since 2002, there have been numerous incidents for which the FSSCC on the private-sector side and the FBIIC on the public-sector side have coordinated sector-wide responses. FSSCC and FBIIC developed protocols and playbooks and the Core Executive Response Group (CERG) to assess the situation and coordinate response.

Before a Significant Event

1. Establish Contacts and Relationships with Critical Government and Law Enforcement Agencies and Industry Organizations

Federal Agencies

DHS/CISA

Within each CISA Region there are local and regional Cyber Security Advisors (CSAs), Protective Security Advisors (PSAs), and Emergency Communications Coordinators (ECCs). To build stakeholder resilience and form partnerships, these field personnel assess, advise, assist, and provide risk management and response services.

CISA Regions: cisa.gov/about/regions

- **CSAs:** CSAs offer cybersecurity assistance to critical infrastructure owners and operators, and state, local, tribal, and territorial (SLTT) officials. They introduce organizations to various CISA cybersecurity products and services, along with other public and private resources, and act as liaisons to CISA cyber programs. They can provide cyber preparedness assessments and protective resources, working group support, leadership, partnership in public-private development, and coordination and support in times of cyber threat, disruption, or attack.
- **PSAs:** PSAs are trained subject matter experts in critical infrastructure protection and vulnerability mitigation. They facilitate local field activities in coordination with other DHS offices and federal agencies. They also advise and assist SLTT officials, critical infrastructure owners and operators, and provide coordination and support in times of threat, disruption, or attack.
- **ECCs:** ECCs support emergency communications interoperability by offering training, tools, and workshops, and provide coordination and support in times of threat, disruption, or attack. These services assist CISA stakeholders in ensuring they have communications during steady and emergency operations. Through these programs, CISA helps ensure public safety, national security, and emergency preparedness communities can seamlessly and securely communicate.
- **CSS:** Regional Corporate Security Symposia (CSS) are events designed to foster collaboration between public and private-sector partners by addressing current and emerging security threats relevant to specific regions. These symposia serve as a platform to disseminate the latest threat information and generate discussions on pressing national security issues, such as economic security, cybersecurity, counterintelligence threats, terrorism threats to the homeland, infrastructure protection, and information sharing.

  CSS are held in coordination with the DHS Office of Intelligence and Analysis (I&A) and Federal Bureau of Investigation (FBI) through the Domestic Security Alliance Council

(DSAC) partnership, CISA, state and local governments, and private-sector partners. For more information, email I&APrivateSector@hq.dhs.gov.

FBI

The FBI investigates matters involving terrorism, violent crimes, cyber, transnational organized crime, counterintelligence and espionage, weapons of mass destruction, civil rights, public corruption, and white-collar crimes including fraud, theft, and embezzlement occurring within or against the national and international financial community.

FBI Office Locator: fbi.gov/contact-us/field

- **InfraGard:** InfraGard is a unique partnership between the FBI and individuals in the private sector for the protection of U.S. critical infrastructure and the American people. As one of the nation's largest public-private partnerships, InfraGard connects critical infrastructure owners, operators, and stakeholders with the FBI to provide education, networking, and information-sharing on security threats and risks.
  InfraGard: infragard.fbi.gov
- **InfraGard National Members Alliance (INMA):** INMA is an FBI-affiliated independent nonprofit organization dedicated to protecting U.S. critical infrastructure and the American people. Join and participate in a local FBI InfraGard chapter to enhance your knowledge base and regional networking. Participate in and support InfraGard's business continuity and information security training opportunities. Following application and approval, a local coordinator and national coordinators will provide means to access the website.
  INMA: infragardnational.org
- **Internet Crime Complaint Center (IC3):** The mission of the IC3 is to provide the public and private sector with a mechanism to submit information to the FBI concerning suspected cyber-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.
  IC3: ic3.gov
- **Domestic Security Alliance Council (DSAC):** DSAC is a public-private partnership offered by the FBI's Office of Private Sector and the DHS's I&A that enhances communication and promotes the timely and effective exchange of security and intelligence information between the federal government and the private sector.
  DSAC: dsac.gov

OCCIP

OCCIP leads Treasury's efforts as the Sector Risk Management Agency (SRMA) for the financial services sector. OCCIP enhances the security and resilience of sector critical infrastructure, coordinates sector-wide risk management activities, and supports response and recovery during significant cyber or operational incidents. The department works closely with financial sector companies, industry groups, and government partners to share information about cybersecurity and physical threats and vulnerabilities, encouraging the use of baseline protections and best practices, and respond to and recover from significant incidents.

OCCIP: home.treasury.gov/about/offices/domestic-finance/financial-institutions

United States Secret Service (USSS)

While well-known for its protective mission, the U.S. Secret Service — one of America's oldest federal law enforcement agencies — conducts criminal investigations to protect the nation's monetary systems from exploitation, including financial institutions, private companies, and critical infrastructure. USSS responsibilities encompass not only various forms of financial fraud, such as illicit credit card schemes, fraudulent wire transfers, and the illicit use of digital assets, but also unauthorized access or damage to computers. The Secret Service is also one of the main federal agencies tasked with investigating ransomware and the lead federal agency tasked with investigating access device fraud.

The Secret Service's Cyber Fraud Task Forces (CFTF) are the focal point of the agency's investigative efforts and are a partnership between the Secret Service, other law enforcement agencies, prosecutors, private industry, and academia. The strategically located CFTFs combat cybercrime through prevention, detection, mitigation, and investigation. CFTFs continues to expand, now in 42 domestic offices, uniting technical experts and forensic analysts operating in the CFTF Digital Evidence Forensic Labs.

Secret Service Office and CFTF Locator: secretservice.gov/contact/field-offices

United States Postal Inspection Service (USPIS)

Postal Inspectors investigate any crime with a nexus to mail. These crimes include mail theft, mail fraud, financial fraud, identity theft, robberies and burglaries of postal facilities, assaults and threats on postal employees, investigations of dangerous and prohibited mail, narcotics, cybercrime, and much more.

USPIS Office Locator: postalpro.usps.com/ppro-tools/inspection-service

Submit Complaints/Reports of Crime Online: uspis.gov/report

Fusion Centers

Fusion centers are focal points for gathering, analyzing, and disseminating threat-related information between SLTT governments and the private sector, and serve as an essential element of our decentralized and distributed homeland security and counterterrorism architecture. They accomplish this through sharing information, providing partners with a unique perspective and expertise on threats to their state or locality, and being the primary conduit between frontline personnel, state and local leadership, and the rest of the Homeland Security Enterprise, including DHS, the Intelligence Community (IC), and the federal government.

National Fusion Center Association: nfcausa.org

Industry and Cross-Industry Information-Sharing Organizations

ABA

The American Bankers Association is the voice of the nation's $26.1 trillion banking industry, which is composed of small, regional, and large banks that together employ over 2 million people, safeguard $20.5 trillion in deposits and extend $13.7 trillion in loans.

In addition to being active in many industry and cross-industry organizations, ABA has several working groups where member financial institutions may share information and receive important notifications on issues affecting bank security, physical security, cybersecurity, and operational resilience.

ABA: aba.com

FS-ISAC

FS-ISAC is a member-driven, not-for-profit organization that advances cybersecurity and resilience in the global financial system, protecting financial institutions and the individuals they serve. Members of FS-ISAC worldwide receive timely notification and authoritative information designed to help protect critical systems and assets from physical and cyber security threats. FS-ISAC activities include:

- Monitoring and assessing cyber and physical threat information, facilitating information sharing, publishing alerts, and engaging FS-ISAC groups as a threat escalates.
- Serving as a central point for reporting suspicious activity or event impact, monitoring thresholds, and conducting exercises to test/validate and/or update incident-management plans.

FS-ISAC: fsisac.com

Global Resilience Federation (GRF)

GRF is a nonprofit provider and hub for cyber, supply chain, physical, and geopolitical threat intelligence exchange between information sharing and analysis centers (ISAC), organizations (ISAO), and computer emergency readiness/response teams (CERTs) from many different sectors and regions around the world. GRF builds, develops, and connects security information sharing communities for mutual defense through summits, cross-sector exercises, and the GRF's Business Resilience Council.

GRF: grf.org

Multi-State Information Sharing & Analysis Center (MS-ISAC)

As a trusted cybersecurity partner for U.S. SLTT government organizations, MS-ISAC cultivates a collaborative environment for information sharing. They offer members incident response and remediation support through a team of security experts and develop tactical, strategic, and operational intelligence, and advisories that offer actionable information for improving cyber maturity.

MS-ISAC: cisecurity.org/ms-isac

Regional Coalitions

Currently, there are three known regional coalitions that bring financial services sector organizations together to achieve a common goal of facilitating the recovery of the sector following a natural disaster or man-made event. By fostering an environment of cooperation and building relationships with federal, state, and local governments prior to a disaster, regional coalitions promote continuity of critical financial services to the communities they serve.

If a regional coalition does not exist in your region, consider starting one. Groups may be enhanced with nondisclosure agreements and should maintain current contacts for representatives and participating FBI and Secret Service personnel.

Alabama Recovery Coalition for the Financial Sector
alabama.bank/abaimis/alabamabankers/Resources/ARCFS/AlabamaBankers/Resources/ARCFS

Housed within the Alabama Bankers Association, the Alabama Recovery Coalition for the Financial Sector is a nonprofit organization dedicated to ensuring the resiliency and availability of Alabama's financial community by:

- Establishing alliances with the State Emergency Management Agency (EMA) and local EMA offices across the state and other state and local government agencies with emergency-preparedness responsibilities to exchange ideas and resources for action following a disaster or an event affecting financial services.
- Serving the people working in the Alabama financial community.

ChicagoFIRST
chicagofirst.org

ChicagoFIRST is a nonprofit association that provides member firms a collaborative forum to address private-sector resilience and emergency-management planning and response with relevant local, regional, and national public-sector agencies.

Louisiana Emergency Preparedness Coalition
https://www.lba.org/LBA/LBA/CommunicationLayouts/Emergency_Prep_Coalition.aspx

Housed within the Louisiana Bankers Association, the Louisiana Emergency Preparedness Coalition is comprised of financial institutions, regulators, emergency personnel, law enforcement, weather service personnel, and armored carriers.

2. Have an Actionable Plan in Place

There are numerous resources, planning tools, and recommended practices you can use to create an incident-response plan:

- **CISA — Federal Government Cybersecurity Incident & Vulnerability Response Playbooks, Appendix B: Incident Response Checklist:** cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
- **Financial Stability Board — Format for Incident Reporting Exchange (FIRE): A possible way** forward**:** fsb.org/2023/04/format-for-incident-reporting-exchange-fire-a-possible-way-forward
- **FFIEC — Information Security Booklet, Incident Response Section:** ffiec.gov/sites/default/files/media/press-releases/2016/2016-%20it-handbook-information-security-booklet.pdf
- **NIST — Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile:** csrc.nist.gov/pubs/sp/800/61/r3/final

3. Register for Government Services

DHS

Homeland Security Information Network (HSIN): HSIN is DHS's official system for trusted sharing of sensitive but unclassified (SBU) information between SLTT, international, and private-sector partners. Mission operators use HSIN to access Homeland Security data, send requests securely between agencies, manage operations, coordinate planned event safety and security, respond to incidents, and share the information they need to fulfill their missions and help keep their communities safe. For more information about HSIN, please contact HSIN@hq.dhs.gov.

CISA

National Cyber Awareness System: The system provides situational awareness to technical and non-technical audiences by providing timely information about cybersecurity threats and issues and general security topics. Products include technical alerts, control systems advisories and reports, weekly vulnerability bulletins, and tips on cyber hygiene best practices.

- **No-Cost Cybersecurity Services and Tools:** cisa.gov/resources-tools/resources/no-cost-cybersecurity-services-and-tools
- **Cybersecurity Alerts and Advisories:** cisa.gov/news-events/cybersecurity-advisories

Cyber Hygiene Services: CISA offers no-cost cybersecurity services to help organizations reduce their exposure to threats by taking a proactive approach to monitoring and mitigating attack vectors.

- **Vulnerability Scanning:** This service continuously monitors and assesses internet-accessible network assets (public, static IPv4 addresses) to evaluate their host and vulnerability status. In

addition to weekly reports of all findings, you'll receive ad-hoc alerts about urgent findings such as potentially risky services and known exploited vulnerabilities (KEVs).[3]

- **Web Application Scanning:** This service scans publicly accessible web applications to uncover vulnerabilities and misconfigurations that attackers could exploit. This comprehensive evaluation includes, but is not limited to, the vulnerabilities listed in the Open Worldwide Application Security Project (OWASP) Top Ten,[4] which represent the most critical web application security risks. This service provides detailed reports monthly, as well as on-demand reports to help keep your web applications secure.

Priority Telecommunications Services (PTS): Priority in communications is crucial to continuity of operations when facing adverse conditions such as weather events, mass gatherings, cyberattacks, or events arising from human error. CISA's Emergency Communications Division (ECD) promotes communications used by emergency responders and government officials. ECD responds to adversarial and hazardous events as one unified team.

CISA offers three priority services that enable essential personnel to communicate when networks are degraded or congested:

- **Government Emergency Telecommunications Service (GETS)**
  cisa.gov/resources-tools/services/government-emergency-telecommunications-service-gets

  GETS is a free service that provides subscribers with priority access and prioritized processing in the local and long-distance segments of landline telephone networks.

- **Wireless Priority Service (WPS)**
  cisa.gov/resources-tools/services/wireless-priority-service-wps

  WPS is a free service that provides authorized devices with priority calling on all nationwide wireless networks.

- **Telecommunications Service Priority (TSP)**
  cisa.gov/resources-tools/services/telecommunications-service-priority-tsp

  The TSP program mandates that service providers prioritize voice and data circuits provisioning and restoration requests made by organizations with national security and emergency preparedness missions.

OCCIP

Project Fortress: Project Fortress is a whole-of-sector effort to improve the security and resiliency of the financial services sector that leverages existing capabilities and new offerings at no cost to sector participants.

For more information on Treasury's Project Fortress, contact OCCIP at OCCIP-Coord@treasury.gov.

[3] The CISA KEV catalog is available at cisa.gov/known-exploited-vulnerabilities-catalog.
[4] Access the OWASP Top Ten Web Application Security Risks at owasp.org/www-project-top-ten.

4. Test Plans to Identity Gaps

Conduct tests annually or more frequently, depending on changes in the operating environment. If possible, include your identified law enforcement agencies and/or emergency management contact, as well as your critical third-party providers, into the testing process.

Develop a Continuity of Operations Plan

- **FFIEC — Business Continuity Management Booklet**
  ithandbook.ffiec.gov/it-booklets/business-continuity-management

  This booklet is one in a series that comprise the FFIEC Information Technology (IT) Examination Handbook. This booklet provides guidance to assist examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services.

- **FEMA — Continuity Guidance Circular (CGC)**
  fema.gov/emergency-managers/national-preparedness/continuity/circular

  The CGC is a whole community guidance to support the development of continuity capabilities across the nation. It is intended to serve as a resource for organizations to integrate and coordinate continuity efforts to build a more resilient nation. The CGC is flexible and adaptable for a broad range of audiences, threats, and capabilities.

Identify Critical Functions and Key Staff

Identify those with primary responsibility for different and critical elements of an organization's incident response plan, including how they (and backups) may be contacted. Consider:

- Access to and Assessment of Information Assets and Systems
- Access to and Assessment of Physical Assets (Credentialing)
- Vendor Management
- Regulatory and Law Enforcement Liaisons
- An Employee/Customer/External Communications Strategy and Plan

Participate in Industry, State, and Federal Exercises

Industry Exercises

Numerous industry exercise programs have been developed for the financial services industry, including:

- **Sector Exercises:** The FSSCC/FBIIC coordinate efforts to improve the reliability and security of financial-sector infrastructure. (fsscc.org and fbiic.gov)
- **Operations-Based Exercises:** FS-ISAC offers a variety of discussion-based (tabletop) and operations-based (hands-on) exercises keeping up with current day threats and mitigation measures. (fsisac.com/exercises)

- **Hamilton Regional Exercises:** The Hamilton Exercise Series is sponsored by the Treasury, and its regional tabletop exercises allow participants to examine their policies, procedures, and general readiness to identify, manage, and mitigate a significant disruption to their organization. Please reach out to your regional Federal Reserve Bank to express interest in participating in the Hamilton Regional Exercises. (Federal Reserve Bank Office locator: frbservices.org/about/frb-bank-offices.html)
- **SIFMA Quantum Dawn Cybersecurity Exercises:** This crisis simulation series for financial institutions helps firms bolster incident response protocols, improve coordination across the sector, and identify gaps before real-world threats emerge. (https://www.sifma.org/resources/readiness-exercises)

State Exercises

State and local emergency management agencies regularly conduct and/or participate in exercises to assess their preparedness and response to a variety of hazards. Representatives from the private sector are often welcome to participate in these exercises. Using the information available in Appendix B, please contact your state emergency management agency to learn about opportunities for participation.

Federal Exercises and Training

Many federal agencies offer exercise packages that allow organizations to test their internal response processes through tabletop exercise.

- **CISA — Cyber Storm:** cisa.gov/resources-tools/programs/cyber-storm
- **CISA — Tabletop Exercise Packages:** cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
- **CISA — Surveillance Detection for Bombing Prevention Course:** cisa.gov/resources-tools/training/surveillance-detection-bombing-prevention-course-346
- **CISA — Bomb Threat Management Planning Course:** cisa.gov/resources-tools/training/bomb-threat-management-planning-course-mgt-451
- **FDIC — Cyber Challenge: A Community Bank Cyber Exercise:** fdic.gov/regulations/resources/director/technical/cyber/info.pdf
- **FEMA — Preparedness Toolkit (PrepToolkit):** preptoolkit.fema.gov
- **FEMA — Exercise Best Practice Guides:** fema.gov/emergency-managers/national-preparedness/exercises/tools#BestPractice
- **FEMA — Exercise Starter Kit:** preptoolkit.fema.gov/en/web/em-toolkits/private-sector
- **FEMA — Homeland Security Exercise and Evaluation Program:** fema.gov/emergency-managers/national-preparedness/exercises/hseep
- **G-7 — Fundamental Elements of Cyber Exercise Programmes:** home.treasury.gov/system/files/216/G-7-FUNDAMENTAL-ELEMENTS-OF-CYBER-EXERCISE-PROGRAMMES.pdf

During a Significant Event

1. Engage Legal Counsel

Having ready access to advice from lawyers well-acquainted with disaster and cyber incident response can speed up an organization's decision-making and help ensure that a victim organization's incident-response activities remain on firm legal footing.

Counsel may also provide valuable counsel on remediation procedures such as compliance requirements, data breach disclosure laws, industry standards, and federal and state laws and regulations.

2. Share Incident Information

Cyber

There are different mechanisms for voluntary reporting of cybersecurity incidents. No matter which agency is contacted first, information is shared with other agencies to provide an appropriate response[5]

- ✓ To report an intrusion and request technical assistance, contact:
  CISA: central@cisa.dhs.gov or 1-844-Say-CISA/844-729-2472
  FBI local field office: www.fbi.gov/contact-us/field-offices
  IC3: www.ic3.gov
  U.S. Secret Service local field office: secretservice.gov/contact/field-offices
- ✓ Contact FS-ISAC, sharingops@fsisac.com (877-612-2622, prompt 2)
- ✓ Contact <trade association representatives>; participate in <trade association calls>
- ✓ Contact FFIEC and <regulatory representative> to obtain mitigation instructions; communicate impact to critical business processes
- ✓ Implement employee/customer/external communications and response plan

Natural or Man-Made

- ✓ Participate in <regional coalition calls> and email updates
- ✓ Contact <FEMA region private outreach>
- ✓ Participate in <state Office of Emergency Management business outreach office>
- ✓ Contact <local business partnerships>
- ✓ Contact <trade association representatives>; participate in <trade association calls>
- ✓ Contact FS-ISAC, sharingops@fsisac.com (877-612-2622, prompt 2)

[5] See Appendix A for federal notification response requirements.

- ✓ Contact FFIEC and <regulatory representative> to obtain mitigation instructions; communicate impact to critical business processes
- ✓ Implement employee/customer/external communications and response plan

Third-Party Disruption

- ✓ Implement employee/customer/external communications and response plan
- ✓ Contact <third-party vendor> to report event; join status calls to obtain mitigation and contingency information
- ✓ Contact FFIEC and <regulatory representative> to obtain mitigation instructions; communicate impact to critical business processes
- ✓ Contact <trade association representatives>; participate in <trade association calls>
- ✓ Contact FS-ISAC, sharingops@fsisac.com (877-612-2622, prompt 2)

Following a Significant Event

1. Report Incidents to Regulators

- See Appendix A for Federal incident notification requirements.
- Consult your state bankers association[6] for information regarding state requirements.

2. File a Suspicious Activity Report (SAR)

Financial institutions, holding companies, and their subsidiaries are required by federal regulations[7] to file a SAR with respect to:

- ✓ Criminal violations involving insider abuse in any amount.
- ✓ Criminal violations aggregating $5,000 or more when a suspect can be identified.
- ✓ Criminal violations aggregating $25,000 or more, regardless of a potential suspect.
- ✓ Transactions conducted or attempted by, at, or through the financial institution (or an affiliate) and aggregating $5,000 or more, if the financial institution or affiliate knows, suspects, or has reason to suspect that the transaction:
    - May involve potential money laundering or other illegal activity (e.g., terrorism financing).
    - Is designed to evade the Bank Secrecy Act (BSA) or its implementing regulations.
- ✓ Has no business or apparent lawful purpose or is not the type of transaction that the customer would normally engage in, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

A transaction includes a deposit; a withdrawal; a transfer between accounts; an exchange of currency; an extension of credit; a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a financial institution.

Visit the Financial Crimes Enforcement Network (FinCEN) page, SAR Advisory Key Terms, for applicable advisories for filing instructions: fincen.gov/resources/suspicious-activity-report-sar-advisory-key-terms.

You may also consider providing a copy of the SAR to the investigating agency.

For an overview of SAR compliance with BSA regulatory requirements, visit bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/04.

---

[6] See ABA's State Bankers Association Alliance Contact List, available at aba.com/advocacy/state-association-alliance/state-association-contacts.

[7] Refer to 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Board of Governors of the Federal Reserve System) (Federal Reserve); 12 CFR 353 (Federal Deposit Insurance Corporation)(FDIC); 12 CFR 748 (National Credit Union Administration)(NCUA); 12 CFR 21.11 and 12 CFR 163.180 (Office of the Comptroller of the Currency)(OCC); and 31 CFR 1020.320 (FinCEN).

3. Identify Lessons Learned

It is important to regularly review and update all capabilities, resources, and plans, particularly following a specific emergency incident. Risks and resources evolve, and so should your preparedness efforts.

- ✓ Evaluate your financial institution's overall response and incorporate lessons into your planning and response process, including your response to:
  - Customers
  - Employees
  - Shareholders
  - Communities you serve
  - Regulatory agencies

- ✓ Evaluate the messaging in your incident communication plan:
  - Incorporate any new questions received from stakeholders.
  - Ensure that the timing associated with your messaging is appropriate.

- ✓ Prepare for a post-event examination, including incorporating the effect of the event on your:
  - Risk assessment process;
  - Disaster recovery and business continuity plans; and
  - Budget and strategic plan.

- ✓ Follow up with law enforcement and other incident responders:
  - Offer law enforcement continued assistance.
  - Discuss the response to a physical event with community first responders.

Association Contacts

American Bankers Association

John Carlson
Senior Vice President, Cybersecurity Regulation and Resilience
202-663-5589
jcarlson@aba.com
aba.com

Financial Services Information Sharing and Analysis Center (FS-ISAC)

Laura Brown
Director of Global Business Resilience
202-769-0543
lbrown@fsisac.com
fsisac.com

U.S. Department of the Treasury Office of Cybersecurity and Critical Infrastructure Protection (OCCIP)

Incident Coordination Team
202-622-3000
OCCIP-Coord@treasury.gov
home.treasury.gov/about/offices/domestic-finance/financial-institutions

Appendix A: Selected Federal Notification [89]

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (Federal Reserve, OCC, FDIC):
federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incidentnotification-requirements-for-banking-organizations-and-their-bank

- Requires a banking organization to notify its primary Federal regulator of any "computer-security incident" that rises to the level of a "notification incident" as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. Requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours.

SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure:
sec.gov/files/rules/final/2023/33-11216.pdf

- Requires publicly traded companies to standardize disclosures about cybersecurity risk management, strategy, and governance. Companies must report material cybersecurity incidents, including the nature, scope, timing, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations, within four business days. Filing may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety. Companies are also required to provide annual disclosures describing their cybersecurity risk management processes and any material impacts from cybersecurity threats. They must describe the board's oversight and management's role in cybersecurity governance, including relevant expertise and reporting structures.

SEC Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information:
sec.gov/files/rules/final/2024/34-100155a.pdf

- Requires broker-dealers, investment companies, investment advisers, funding portals, and transfer agents to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. Firms must also adopt written incident response policies and procedures to detect, respond to, and recover from unauthorized access to customer information, and notify affected individuals as soon as practicable and no later than thirty days. Notices must describe the incident, the data involved,

[9] Companies should consult with their own legal counsel regarding the applicability of the requirements listed in this appendix and any other notification requirements under federal or state law.

and steps individuals can take to protect themselves. Firms must oversee service providers and safeguard a broadened scope of customer information.

CISA Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) *(In public comment phase as of May 2026)*:
federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-criticalinfrastructure-act-circia-reporting-requirements

- If adopted, may require covered entities to report covered cyber incidents within 72 hours and ransomware payments within 24 hours to CISA. These reports would allow CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims.

U.S. Department of Housing and Urban Development Federal Housing Authority Mortgagee Letter 2024-10, "Significant Cybersecurity Incident (Cyber Incident) Reporting Requirements":
hud.gov/sites/dfiles/OCHCO/documents/2024-10hsgml.pdf

- Requires FHA-approved mortgagees to report cyber incidents to HUD's FHA Resource Center and HUD's Security Operations Center within 12 hours of detection.

State Regulatory and Customer Notification Requirements:

- Check with your state banker association: aba.com/advocacy/state-association-alliance/state-association-contacts

Appendix B: State-Specific Contacts and Information

Access state, district, and territory-specific information here.

- Alabama
- Alaska
- Arizona
- Arkansas
- California
- Colorado
- Connecticut
- Delaware
- Florida
- Georgia
- Hawaii
- Idaho
- Illinois
- Indiana
- Iowa
- Kansas
- Kentucky
- Louisiana
- Maine
- Maryland
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Missouri
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- South Dakota
- Tennessee
- Texas
- Utah
- Vermont
- Virginia
- Washington
- West Virginia
- Wisconsin
- Wyoming

- District of Columbia

U.S. Territories

- Guam
- Puerto Rico
- U.S. Virgin Islands