GEORGIA

2019 INCIDENT RESPONSE PLAYBOOK

GBA

FS-ISAC

American Bankers Association

Table of Contents

The information and contacts included in this Playbook are accurate as of August 2019. Going forward, all information and contacts will be reviewed and updated on an annual basis in the fourth quarter of each year. The next review will be conducted in Q2 2020. Should you have any questions or comments regarding this Playbook please send an e-mail to statealliance@aba.com.

How to Use the Playbook

Why

The Financial Services Information Sharing and Analysis Center (FS-ISAC), the American Bankers Association (ABA), the ABA-State Association Alliance, and its members and critical infrastructure partners have developed this all-hazards state and regional crisis Incident Response Playbook (hereafter referred to as "the Playbook"). The Playbook guides how state bankers' associations and their bank membership will respond during a crisis event, how activities will be coordinated, and how information will be shared to achieve resiliency in the financial sector.

In the event of a crisis, FS-ISAC, trade associations, U.S. Department of Treasury, and other regulatory agencies will work through the Financial Services Sector Coordinating Council to assess and respond to the incident. The ABA will facilitate communication and information sharing directly with state bankers' associations.

Who

This Playbook is intended for use by those responsible for leading or participating in an organization's incident or crisis management team, regardless of whether it is a cyber event, natural disaster, technological hazard or man-made event.

What

In this Playbook, "crisis" is defined as a large-scale disruption (or disruptions) that affects, or has the potential to affect, the security, stability, operations, and/or reputation of the financial services sector. Although the causes of crises can vary greatly, many of the effects of these crises do not. Crisis managers can address common operational functions in their basic plans instead of having unique plans for every type of hazard or threat. For example, floods, wildfires, hazardous materials releases, and radiological dispersal devices may lead a jurisdiction to issue an evacuation order and open shelters. Even though each hazard's characteristics (e.g., speed of onset, size of the affected area) are different, the general 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

This state-specific Playbook is designed to be used in conjunction with the FS-ISAC All Hazards Playbook (available from FS-ISAC) and to provide sector members and crisis response groups with a roadmap of whom to contact and what steps to take during actual crisis events, regardless of whether they are industry-wide or bank-specific. The contacts provided in this Playbook are for federal and state agencies. However, because many incidents are local, users are encouraged to tailor this document to include additional contacts for their specific regions, municipalities, towns, and/or processes specific to their incident response plans.

Playbook resources will be continually updated to include lessons-learned from exercises and actual crises, as well as enhanced contingency planning guidance.

Playbook Organization

To facilitate use of the Playbook, it has been organized as follows:

- **Before an Incident**: Identifies actions that Playbook users can take now to prepare for crises
- **During an Incident**: Provides examples of critical information needs and information-sharing protocols to facilitate rapid response to and recovery from the incident
- **Following an Incident**: Provides recommendations both to ensure rapid recovery from the incident, and to better prepare the users for the next incident

As noted above, each section of the document can be tailored to the user's region by inserting region-specific text where noted by chevrons (e.g., "Contact <*trade association representatives*> and participate in <*trade association calls*>").

The Playbook concludes with a comprehensive listing of state-specific association and government contacts to be used in the event of a natural, technological, man-made, or cyber crisis.

Establish Contacts and Relationships with Local Law Enforcement, U.S. Department of Homeland Security, and Regional Coalitions

☐ **Federal Bureau of Investigation (FBI)**

FBI investigates matters involving violent crimes; bank and armored car robberies; and other financial crimes, including fraud, theft, and embezzlement occurring within or against the national and international financial community.

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

☐ **FBI Infragard**

Join and participate in your local FBI Infragard chapter to enhance your knowledge base and networking. Participate in and support their business continuity and information security training opportunities. Following application and approval, you will be contacted by your local coordinator and national coordinators with means to access the website.

FBI Infragard, www.infragard.org

☐ **United States Secret Service (USSS)**

The primary mission for USSS investigations is the prosecution of those involved in financial crimes as they relate to the protection of the financial infrastructure of the United States. USSS has Financial Crimes Task Forces and Electronic Crimes Task Forces (ECTFs) throughout the country that are ready to carry out this mission. An ECTF coordinates regular meetings in each region to discuss the evolving threat environment; provide training and build awareness; and provide an opportunity to network with local law enforcement and state computer crime lab representatives.

USSS Office Locator, http://www.secretservice.gov/field_offices.shtml
USSS ECTF and Working Groups Locator,
https://www.secretservice.gov/investigation/#field

☐ **United States Postal Inspection Services (USPIS)**

One of the overall objectives of USPIS is to investigate complaints where the U.S. Mail and/or U.S. Postal Service products or services are used to facilitate identity theft. The agency also investigates cases of violent crimes involving robberies, burglaries, assaults, and workplace violence.

USPIS Office Locator, http://locator.uspis.gov/locator/
USPIS Phone, 1-877-876-2455

☐ **U.S. Department of Homeland Security Protective Security Advisor (PSA) Program**

The PSA Program's primary mission is to proactively engage with federal, state, and local governments and members of the private sector to protect critical infrastructure. During incidents, PSAs serve as the infrastructure liaisons at

Federal Emergency Management Agency (FEMA) Joint Field Offices, Regional Coordination Centers, and state and county emergency operations centers.

PSAs also conduct site visits and vulnerability assessments of critical infrastructure assets. They work with the U.S. Secret Service to provide vulnerability assessments, security planning, and coordination during large-scale special events.

PSA Program, PSCDOperations@hq.dhs.gov

Determine Whether Any Regional Coalitions Exist

☐ **Regional Coalitions**

Currently, 16 regional coalitions exist across the United States in which critical firms and businesses collaborate with one another and, as a group, with government at all levels, in order to promote the resilience of their individual firms through local, regional, and national relationships. Under RPCfirst, these coalitions share lessons learned and best practices about how to coordinate with local, county, and state government.

Regional Coalition Locator, http://rpcfirst.org/us-coalitions/

Research networking groups in your area/state and participate. If such a networking group does not exist, consider starting one. Groups may be enhanced with Nondisclosure Agreements and should maintain current cell contacts for representatives and participating FBI and USSS personnel.

Join FS-ISAC

☐ **FS-ISAC**

The Financial Services Information Sharing and Analysis Center is the only financial services industry forum for collaboration on critical security threats facing the global financial services sector. Members of FS-ISAC worldwide receive timely notification and authoritative information specifically designed to help protect critical systems and assets from physical and cyber security threats. Among FS-ISAC activities, they:

- ✓ *Monitor and assess cyber and physical threat information, facilitate information sharing, publish alerts, and engage FS-ISAC groups as a threat escalates.*
- ✓ *Serve as a central point for reporting suspicious activity or event impact, monitor thresholds, and conduct surveys.*

FS-ISAC, http://www.fsisac.com/

Participate in Industry, State, and Federal Exercises

☐ **Industry Exercises**

Numerous industry exercise programs have been developed for the banking industry:

- ✓ *The Financial Services Sector Coordinating Council/Financial and Banking Information Infrastructure Committee coordinates efforts to improve the reliability and security of financial-sector infrastructure.* https://www.fsscc.org/
- ✓ *FS-ISAC offers an annual, two-day Cyber-Attack Against Payment Systems tabletop exercise to simulate an attack on payment systems and processes. http://www.fsisac.com/Exercises-CAPS*
- ✓ *The Federal Deposit Insurance Corporation (FDIC) has distributed an "exercise in a box" containing a number of cybersecurity scenarios for community bankers.* https://www.fdic.gov/regulations/resources/director/technical/cyber/cyber.html

☐ **State Exercises**

State and local emergency management agencies regularly conduct and/or participate in exercises to assess their preparedness for and response to a variety of hazards. Representatives from the private sector are often welcome to participate in these exercises. Using the contact information found in the ***State Contacts*** *section of this Playbook, please contact your state emergency management agency to learn of upcoming opportunities to participate in exercises.*

☐ **Federal Exercises**

At the federal level, FEMA conducts a series of tabletop exercises to help private-sector organizations advance their continuity, preparedness, and resiliency. These exercises are designed to help an organization test a hypothetical situation, such as a natural or man-made disaster, and evaluate the organization's ability to cooperate and work together, as well as test its readiness to respond. https://www.fema.gov/emergency-planning-exercises.

General information about partnering with FEMA, as well as contact information for the FEMA Private Sector Liaison in your region, can be obtained by contacting the FEMA Private Sector Division via e-mail at: FEMA-Private-Sector@fema.dhs.gov.

Register for the Following Government Services

☐ **Government Emergency Telecommunications Service (GETS)**

GETS prioritizes calls over wireline networks when the landline network is congested and the probability of completing a normal call is reduced.

GETS, http://www.dhs.gov/government-emergency-telecommunications-service-gets

☐ **Wireless Priority Service (WPS)**

WPS prioritizes calls over wireless networks when the wireless network is congested and the probability of completing a normal call is reduced.

WPS, http://www.dhs.gov/wireless-priority-service-wps

☐ **Telecommunications Service Priority (TSP)**

TSP authorizes priority restoration for vital voice and data circuits or other telecommunications services.

TSP, http://www.dhs.gov/telecommunications-service-priority-tsp

☐ **United States Computer Emergency Readiness Team (US-CERT) National Cyber Awareness System**

The National Cyber Awareness System offers a variety of information for users with varied technical expertise. A subscription to any or all of the National Cyber Awareness System products ensures that you have access to timely information about security topics and threats. Those with more technical interest can read Alerts, Current Activity, or Bulletins. Users looking for more general-interest pieces can read Tips.

US-CERT National Cyber Awareness System, https://www.us-cert.gov/ncas

Have an Actionable Plan in Place

☐ **Develop an Incident Response Plan**

There are numerous information sources, planning tools, and best practices you can use to create an incident response plan:

- ✓ *FDIC, Supervisory Insights, Incident Response Program,* https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin06/article01_incident.html
- ✓ *Federal Financial Institution Examination Council (FFIEC) Information Security Booklet, Incident Response Section, https://ithandbook.ffiec.gov/it-booklets/information-security/iii-security-operations/iiid-incident-response.aspx, and the full FFIEC Booklet library,* http://ithandbook.ffiec.gov/it-booklets/information-security/iii%20security-operations/iiid%20incident-response.aspx
- ✓ *U.S. Department of Commerce, National Institute of Standards and Technology, (NIST) – Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide,* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- ✓ *DHS (Department of Homeland Security) resources for home and businesses,* www.READY.gov
- ✓ *FEMA National Business Emergency Operations Center (NBEOC) which facilitates public/private information sharing when FEMA national level of coordination is activated https://www.fema.gov/nbeoc*

- ✓ *DHS Stop, Think, and Connect resources for business,* https://www.dhs.gov/publication/stopthinkconnect-small-business-resources
- ✓ *FEMA resiliency planning resources for home and businesses,* https://www.fema.gov/media-library/resources-documents/collections/344
- ✓ *U.S. CERT publications and alerts,* https://www.us-cert.gov/security-publications

☐ **Develop a Continuity of Operations Plan**

General guidance on continuity of operations planning—the development of plans to ensure that business-essential functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies—are available from FEMA.

https://www.fema.gov/continuity-operations

☐ **Identify Key Staff**

Identify those with primary responsibility for different 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*

Engage Legal Counsel

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

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

Test Plans to Identity Gaps

Conduct tests annually, at minimum, or more frequently, depending on changes in the operating environment. If possible, include your identified law enforcement agencies and/or emergency management contacts into the testing process.

Collect the Following Information for First Responders or Investigators

Cyber

- ✓ The physical or computer systems affected
- ✓ The apparent origin of the incident, intrusion, or attack
- ✓ Any remote servers to which compromised data were sent
- ✓ The identity of any other victim organizations, if such data is apparent in logged data

Natural, Technological, or Man-made

- ✓ Injuries or deaths
- ✓ Facility damage or destruction
- ✓ Third-party disruption: Any weapons or malware used in connection with the incident

Third-party Disruption

- ✓ The physical or computer systems affected
- ✓ The apparent origin of the incident, intrusion, or attack
- ✓ Any remote servers to which compromised data were sent
- ✓ The identity of any other victim organizations, if such data is apparent in logged data

Share Incident Information

Cyber

For cybersecurity incidents, the federal government has several different reporting mechanisms. No matter which agency is contacted first, information is shared with other agencies to provide an appropriate response.

- ✓ Contact the local FBI Office, Cywatch@ic.fbi.gov, (855-292-3937)
- ✓ Contact the local USSS Field Office, http://www.secretservice.gov/field_offices.shtml
- ✓ Contact the National Cybersecurity and Communications Integration Center, NCCIC@hq.dhs.gov, (888-282-0870)
- ✓ Contact FS-ISAC, SOC@fsisac.com, (877-612-2622, prompt 2). Crisis teams may engage; participate in any FS-ISAC calls
- ✓ 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 plan

Natural, Technological, or Man-made

- ✓ Participate in RPCfirst and register for email updates
- ✓ Contact local FEMA region
- ✓ Participate in your State's Office of Emergency Management business outreach office.
- ✓ Contact local business partnerships
- ✓ Contact trade association representatives; participate in trade association event calls.
- ✓ Contact FS-ISAC, SOC@fsisac.com, (877-612-2622, prompt 2). Crisis teams may engage; participate in any FS-ISAC calls
- ✓ Contact FFIEC and your regulatory representative to obtain mitigation instructions; communicate impact to critical business processes
- ✓ Implement employee/customer/external communications plan

Third-party Disruption

- ✓ Contact your third-party vendors 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 event calls
- ✓ Contact FS-ISAC, SOC@fsisac.com, (877-612-2622, prompt 2). Crisis teams may engage; participate in any FS-ISAC calls

File a Suspicious Activity Report (SAR) (Cyber)

Check 35q, "Unauthorized Electronic Intrusion" for activities or attempts to:

- ✓ Remove, steal, procure, or otherwise affect funds of the institution or the institution's customers;
- ✓ Remove, steal, procure, or otherwise affect critical information of the institution, including customer account information; and
- ✓ Damage, disable, or otherwise affect critical systems of the institution.

Since more than one type of suspicious activity may apply, the financial institution should check all boxes that apply when completing Items 29 through 38. In addition, financial institutions should provide a detailed description of the activity in the narrative section of the SAR.

For tips on filing SARs specific to account takeover activity, see the FIN-2011-A016 advisory (Dec. 2011), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2011-a016

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

Disaster Assistance

The Small Business Administration and the U.S. Department of Agriculture provide low-interest loans (Disaster and Economic Injury Loans) to businesses and individuals to repair or replace real estate, personal property, machinery and equipment, inventory, and business assets that have been damaged or destroyed in a federally declared disaster. https://www.sba.gov/funding-programs/disaster-assistance

Identify Lessons Learned

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

- ✓ Evaluate your bank'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 was appropriate.

- ✓ Prepare for a post-event examination, including incorporating the impact 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, particularly after a cybersecurity event.
  - Discuss the response to a physical event with community first responders.

State Bankers Association, American Bankers Association, and FS-ISAC Contacts

Georgia Bankers Association

Joe Brannen
President & CEO
jbrannen@gabankers.com
404-420-2026

David Oliver
SVP, Communications & Marketing
doliver@gabankers.com
404-522-1501

American Bankers Association

Paul Benda
Senior Vice President
ABA Cybersecurity Policy
pbenda@aba.com
202-663-5256

Heather Wyson-Constantine
Vice President, Risk Management
ABA Center for Payments and Cybersecurity Policy
hwyson@aba.com
202-663-7513

FS-ISAC

Susan Rogers
Business Resiliency, Director
srogers@fsisac.com
610-389-1271

Steven Estep
Business Resiliency, Manager
sestep@fsisac.com
651-767-2215

RPC*first*

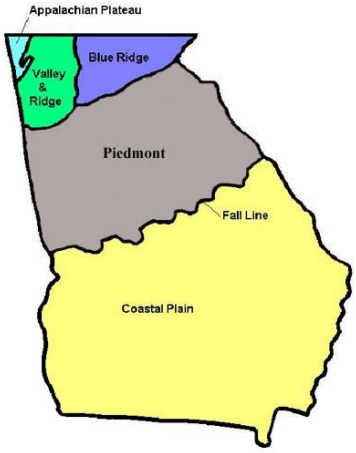
Brian Tishuk
RPC*first* Executive Director
info@rpcfirst.org

Robin Remines
RPC*first* Deputy Director
info@rpcfirst.org

Georgia Information and Incident Contacts

Regions: http://www.georgiaencyclopedia.org/articles/geography-environment/geographic-regions-georgia-overview

159 Counties in the State of Georgia



535 Municipalities: https://en.wikipedia.org/wiki/List_of_municipalities_in_Georgia_(U.S._state)

2017 Population Estimate: 10.4 million people
http://www.census.gov/quickfacts/table/PST045215/13

Governor's Office Key Point of Contact

Homer Bryson, Director Georgia Emergency Management and Homeland Security, 404-635-7008, Homer.bryson@gema.ga.gov

GA Government Directory: http://georgia.gov/agency-list

GEMHSA – Georgia Emergency Management & Homeland Security Agency

https://gema.georgia.gov/

Homer Bryson, Director Georgia Emergency Management and Homeland Security, 404-635-7008, Homer.bryson@gema.ga.gov

Georgia Emergency Management & Homeland Security Agency Area Offices – GEMHSA also has regional field offices that serve as the base of operations for local support.

Leadership: Statewide
Field Operations Director
GEMHSA P.O. BOX 12666
Chuck Ray, chuck.ray@gema.ga.gov

Area One: Northeast Georgia
GEMHSA-Cleveland Office: 1241 Helen Highway, Georgia 30528
Area One Coordinator: Don Strength, donald.strength@gema.ga.gov

Area Two: Southwest Georgia
GEMHSA - Valdosta Office: 1709 A Gornto Road, PMB #121, Valdosta, Georgia 31601
Area Two Coordinator: Frank Maneer, frank.maneer@gema.ga.gov

Area Three: East Central Georgia
GEMHSA – Blairsville Office, 46 Hughes Street, Suite A, Statesboro, Georgia 30512
Area Three Coordinator: Collin Hopf, collin.hopf@gema.ga.gov

Area Four: West Central Georgia
GEMHSA - LaGrange Office: P.O. Box 15, LaGrange, Georgia 30241
Area Four Coordinator: Jason Ritter, jason.ritter@gema.ga.gov

Area Five: Coastal Georgia
GEMHSA - Waycross Office: 3395 Harris Road, Suite 300, Waycross, Georgia 31503
Area Five Coordinator: Kristen Higgs, kristen.higgs@gema.ga.gov

Area Six: Northwest Georgia
GEMHSA Calhoun Office: 4543 Fairmount Hwy, Calhoun, Georgia 30701
Area Six Coordinator: Tim Reeve, tim.reeve@gema.ga.gov

Area Seven: Metro-Atlanta
GEMHSA - Marietta Office: P.O. Box 669112, Marietta, Georgia 30066
Area Seven Coordinator: Sheri Russo, sheri.russo@gema.ga.gov

Area Seven: South Central Georgia
GEMHSA - Douglas Office: 941 Mahogany Road, Douglas, Georgia 31533
Area Seven Coordinator: Diane Adams, diane.adams@gema.ga.gov

Georgia Emergency Operations Plan

The Georgia Emergency Operations Plan provides strategic guidance for the coordination and management of disasters and emergencies. This document is based on extensive planning and coordination between federal, state, local, private sector, and non-profit enterprises. It is designed to be in accordance with the National Response Framework and to support local emergency operations plans of all 159 counties in the state of Georgia.

https://gema.georgia.gov/plan-prepare

Georgia Emergency Communications

Georgia's radio and television stations serve as the primary means for providing emergency notifications to the public, whether the situation involves severe weather, civil defense or law enforcement emergencies, or missing persons. The Georgia Association of Broadcasters and the Georgia Emergency Management Agency work to operate and maintain the Georgia Emergency Alert System. In addition to the Georgia EAS, GEMHSA, in collaboration with various state and local public safety stakeholders, is working to coordinate the initial implementation of the FirstNet Program. FirstNet (First Responders Network) is a federal program that works to provide 4G wireless broadband capability to emergency responders.

http://gab.org/services/eas/
http://firstnet.gema.ga.gov/Pages/default.aspx

Georgia Fusion Centers

Primary fusion centers serve as the focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information and have additional responsibilities related to the coordination of critical operational capabilities across the statewide fusion process with other recognized fusion centers. Furthermore, primary centers are the highest priority for the allocation of available federal resources, including the deployment of personnel and connectivity with federal data systems.

National Fusion Center Association - https://nfcausa.org/

Fusion Centers
Georgia Information Sharing and Analysis Center, Atlanta, GA, 404-486-6420

http://www.dhs.gov/fusion-center-locations-and-contact-information

Georgia Homeland Security Office

Georgia Emergency Management and Homeland Security Agency: Homeland Security Division
https://gema.georgia.gov/what-we-do/homeland-security

Georgia Technology Authority
https://gta.georgia.gov/cyber-security

Georgia FBI Offices

FBI Atlanta
2635 Century Parkway NE
Suite 400
Atlanta, GA 30345
https://www.fbi.gov/contact-us/field-offices/atlanta
404-679-9000

Georgia Secret Service Offices

Albany
410 West Broad Avenue, #410
Albany, GA 31701
229-430-8442

DHS Critical Infrastructure Cyber Community (C3) Voluntary Program

The Critical Infrastructure Cyber Community (C3) Voluntary Program is a public-private partnership to help connect businesses; federal government agencies; academia; and state, local, tribal, and territorial government partners to DHS and other Federal government programs and resources that will assist their efforts in managing their cyber risks and using the NIST Cybersecurity Framework.

C3 Voluntary Program, www.dhs.gov/ccubedvp or www.us-cert.gov/ccubedvp
Getting Started Business, http://www.us-cert.gov/ccubedvp/getting-started-business