# US Playbook Appendix
# FS-ISAC All-Hazards Framework

**Version 2019-1.5**

**Date: October 15, 2019**

**Classification: FS-ISAC TLP Green**

***FS-ISAC Traffic Light Protocol (TLP) GREEN*** *- Recipients may share* ***TLP GREEN*** *information with peers, trusted government and critical infrastructure partner organizations and services providers with whom they have a contractual relationship, but not via publicly accessible channels.*

## Table of Contents



### How Members Use the Playbook Appendix


| | |
|---|---|
| **Purpose of All-Hazards Framework** | Financial Services Information Sharing and Analysis Center (FS-ISAC), its members and financial services critical infrastructure strategic partners developed the voluntary *FS-ISAC All-Hazards Framework (the Framework)* to guide how the financial sector uses trusted information sharing to evaluate and respond to all-hazards events, share situational awareness, analysis, and coordinate with government and other partners. The overall goal is to enhance financial sector resiliency. This does not replace institution obligations to meet regulatory communication requirements. |
| **Definition of a crisis** | A "crisis" is defined as a large-scale disruption that impacts, or have the potential to impact, the security, stability, operations and/or reputation of the global financial services or other critical infrastructure sectors. FS-ISAC staff, financial institutions, association members and government partners discuss and assess the severity of threats and events to determine if they reach a "crisis" threshold. |
| **How FS-ISAC defers to and leverages others as "playbook runners"** | This US playbook explains FS-ISAC's role in crisis response and references other organizations that play important roles in crisis response. Depending on the event, FS-ISAC defers to and leverages the roles other organizations play in responding to crises, including the US capital markets and payments. FS-ISAC embraces a concept of leveraging others that serve as "playbook runners" while also ensuring that the information sharing needs of the broader financial sector are served. |
| **How FS-ISAC uses this US Playbook** | • Articulate the coordination activities within a country or region, critical sector or a specific event scenario.<br>• Identify the stakeholders who lead coordination and define how trusted information sharing global activities can be utilized by Playbook stakeholders. |
| **When does FS-ISAC use this US Playbook during a crisis?** | • Use during times of threat escalation and financial sector crisis events.<br>• Obtain assistance from the financial services sector and government incident response entities, even if the organization is not an FS-ISAC member.<br>• In recognition of the potential that a crisis impacts financial institutions and others outside of the US (and vice versa), this US Playbook may be supported by other Playbooks in other regions and countries and by FS-ISAC staff which is located in several key jurisdictions to support trusted member information sharing for Americas, EMEA and APAC. |

# I. FS-ISAC Crisis Information Sharing

## How Financial Institutions Report and Communicate Events

Individual financial institutions and their partners contribute to sector resilience by notifying emergency and government authorities whenever a physical or cyber-event disrupts their organization(s). In addition to notifying appropriate government and regulatory agencies, financial institutions are encouraged to contact FS-ISAC to assist in information sharing and analysis.

FS-ISAC uses the "Traffic Light Protocol" (TLP) system to label confidential and sensitive information for distribution across the industry as outlined in this Framework. The FS-ISAC Membership Guide defines the four-color designations used: Red, Amber, Green and White. A detailed description of these protocols can be found in Appendix A1.

## Reporting Events to FS-ISAC

The FS-ISAC provides a centralized hub for trusted voluntary information sharing and analysis. FS-ISAC members participate in trusted and anonymous communication channels with FS-ISAC and other financial institution. Financial Institutions and Sector Participants are encouraged to contact FS-ISAC and trusted communities to share event reporting anonymously or with attribution. There are several ways to contact FS-ISAC and include the following:

- **Contact FS-ISAC, 1 (877) 612-2622, prompt 2 or IncidentReporting@fsisac.com**
- **Share using trusted FS-ISAC group email addresses (listservs)**
- **Contact FS-ISAC Trusted Communities of Interest your company belongs to (see page 3).**

The FS-ISAC facilitates a trusted Media Response Team (MRT) community to determine whether public messaging during a crisis event is warranted and what that communication should convey. Members may contact the IncidentReporting@fsisac.com to request public messaging availability or to validate messaging with MRT members.

## Reasons to Contact FS-ISAC

To ask about an event or report an incident; with reference or anonymous request

To validate the facts of an event and request situational awareness or alerts

To inquire if public messaging for the event has been determined or to validate messaging

To ask for assistance with other critical infrastructure such as: electricity, communications, transportation, etc.

To request that FS-ISAC reach out to government or their global network for situational awareness and fact validation

To ask if FS-ISAC trusted communities are activated for the event; or ask questions of the peer community

# II. FS-ISAC Crisis Response Coordination

## FS-ISAC Crisis Coordination Communities

FS-ISAC members join trusted and global communities of interest to assess event threats and impact and then to collaborate on the response.

The FS-ISAC Playbook describes sector crisis response coordination activities facilitated by FS-ISAC and its members. Other organizations have playbooks and FS-ISAC defers to and coordinates with other playbook runners. Various sector Playbooks are identified in Appendix A1 – Financial Sector Playbook Inventory, US Government Resources and Templates. FS-ISAC Communities of Interest that engage during a crisis event include the following:

| | |
|---|---|
| **TIC** | **Threat Intelligence Committee** includes head of security, intelligence analysts and incident responders. |
| **BRC** | **Business Resiliency Committee** includes heads of business continuity, disaster recovery, physical security and operational risk management. |
| **MRT** | **Media Response Team** includes media relations, press officers, public affairs. |
| **CHEF** | **Clearing House and Exchange Forum** includes CISOs and senior level executives of clearinghouses and exchanges globally. |
| **CERG** | **Core Executive Response Group** includes key sector representatives, executive leadership of the FSSCC, FS-ISAC, Securities Industry, FSARC, Sheltered Harbor and TIC, BRC, CHEF and MRT Chair(s); US Treasury; expand as needed to respond to specific event. |
| **CMT** | **Crisis Management Teams:** Specialized experts will convene during a significant sector disruption to obtain situational awareness from participants in the event and produce alerts and instructions for all financial sector members. |

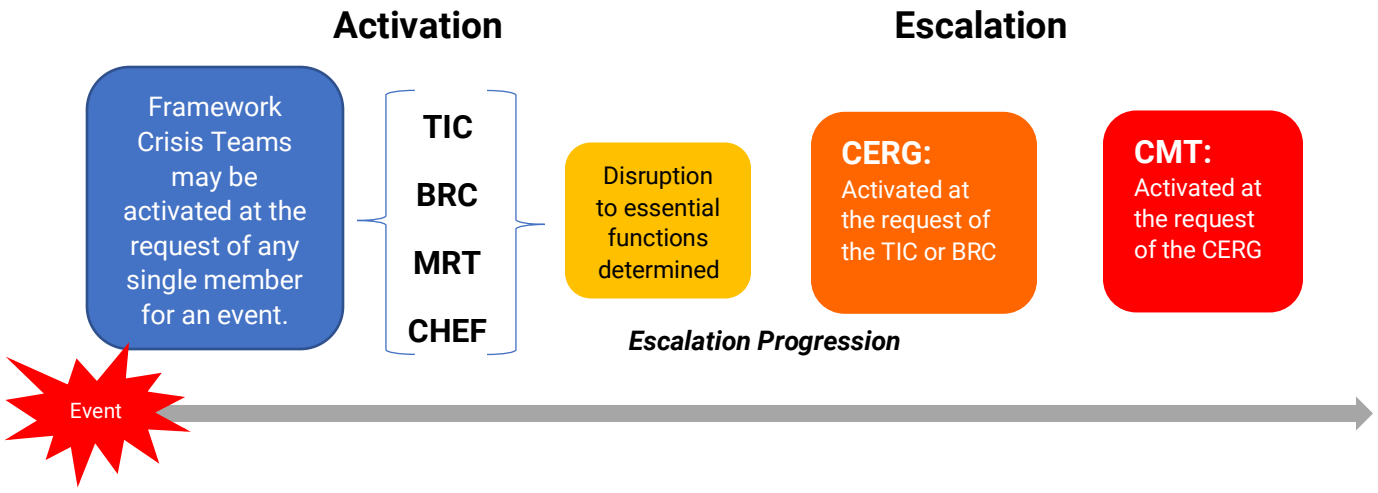
**FS-ISAC members lead communities of interest** including: Insurance, Community Banks, Credit Unions, Payment Processing, Compliance and Audit, EMEA and APAC, Mortgage and more.

**For financial sector stakeholders to contact any of these communities, contact FS-ISAC at IncidentReporting@fsisac.com or 1-877-612-2622, prompt 2**

## Activating Framework Crisis Teams

Activation of the *FS-ISAC All Hazards Framework* occurs when a member or partner requests the activation of one of the Crisis Coordination Communities. Any member may request activation of these groups. Escalation to the CERG and CMT will be determined following initial meetings by the TIC, BRC, MRT and CHEF. A visual representation of this process can be found in Appendix A2.

**Figure 1 – FS-ISAC Playbook Team Activation**

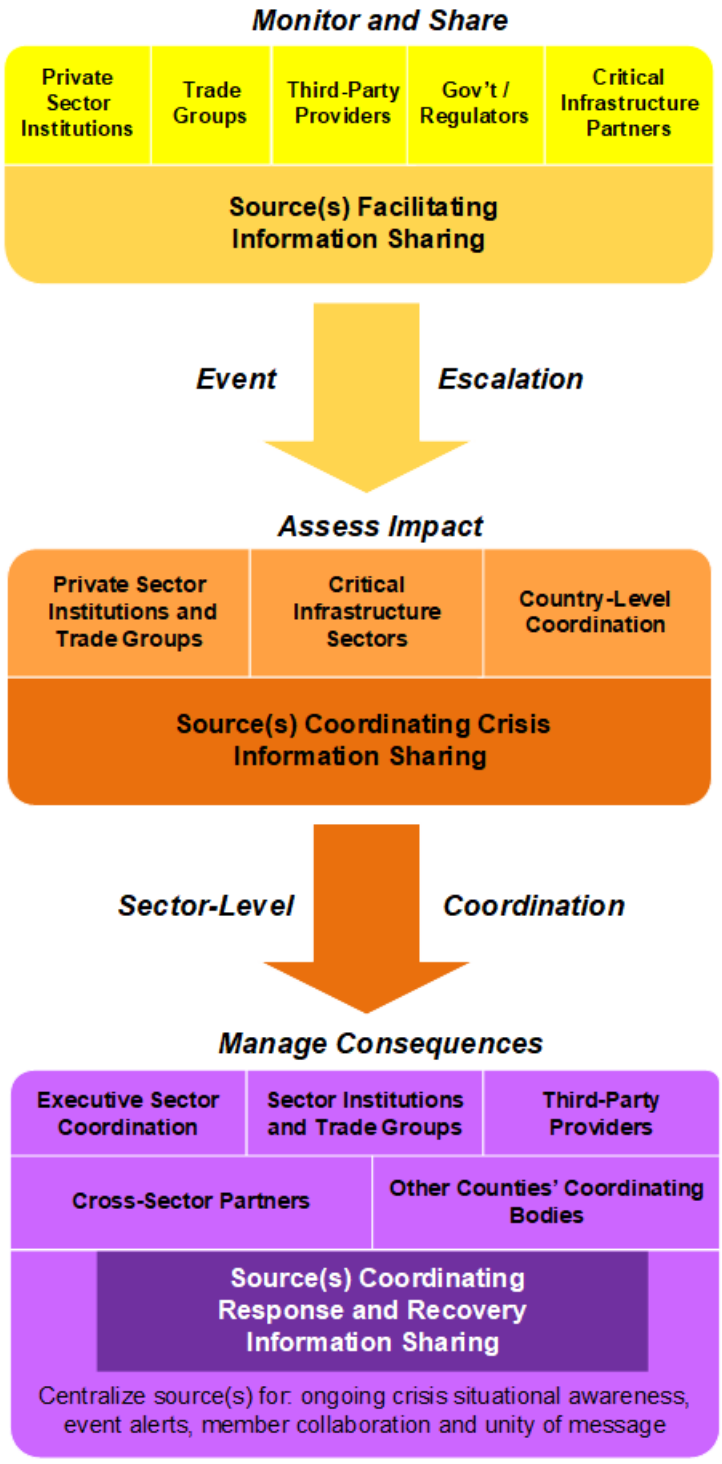



FS-ISAC members provide their crisis contact information to FS-ISAC and it is stored in the Critical Infrastructure Notification System (CINS). Depending on the urgency of the event, the FS-ISAC may use CINS to activate emergency call discussions and assemble financial sector crisis coordination teams. **FS-ISAC members may contact IncidentReporting@fsisac.com to request CINS activation.**

## Stages of FS-ISAC Crisis Response Information Sharing

Throughout all stages of an event FS-ISAC assists the sector by serving as a centralized hub of information sharing. Figure 2 below, represents the stages of information sharing during an event and the many parties which collaborate to protect the sector.

**Figure 2 – Stages of FS-ISAC Crisis Response Information Sharing and Activities**




### *Monitor and Share*

- FS-ISAC members communicate awareness of an event by emailing trusted member communities or contacting FS-ISAC Ops for anonymous sharing;
- FS-ISAC issues an alert early in the awareness process;
- FS-ISAC prepares event model to determine potential for disruption to the financial sector, including systemic disruption.

### *Assess Impact*

- Members activate the FS-ISAC All-Hazards Playbook crisis teams;
- CISOs and Resilience leaders collaborate through Regional and Global TIC and BRC; deliberate to change the cyber and physical threat levels; recommend content for FS-ISAC member alerts;
- Sector participates in:
  - Critical function impact assessment activities;
  - Trade group coordination efforts;
  - Country-level coordination;
  - Third-party impact and mitigation
- Media Response Team (MRT) directs FS-ISAC external messaging;
- FS-ISAC provides ongoing crisis alerts for situational awareness, mitigation instructions and more.

### *Manage Consequences*

- Sector executive coordination engages;
- FS-ISAC holds member crisis event calls;
- Sector participates in impact assessment, trade group. coordination, country-level and third-party efforts;
- Sector participates in systemic collaboration activities and financial critical function mitigation;
- Impacted organizations invited to join FS-ISAC trusted crisis calls; impacted non-members and third-party providers also invited;
- Tri-Sector Playbook activates to prioritize sector needs with electricity and communication sectors;
- FS-ISAC joins government critical infrastructure calls;
- FS-ISAC joins centralized crisis coordination calls, as invited, to provide situational awareness.

## Event Assessment and Changing Physical and Cyber Threat Levels

The BRC (for physical) and TIC (for cyber) assess the severity of a threat and determines the sector threat levels. Procedures for assessments are documented in Playbook resource guides: *Cyber Threat Advisory and Response Guide* and *FS Physical Threat Call Procedures and Guidelines*. The FS-ISAC uses a model to guide decision making.

**FS-ISAC Analysts and Intel Committees Guide Assessment**

**Cyber Threat Level (CTL)** – Reviewed bi-weekly during Threat Intel call; TIC engages during event escalation; recommends change of CTL, and messaging instructions for FS-ISAC member alerts.

**Physical Threat Level (PTL)** – FS-ISAC analysts prepare threat model; BRC engages during physical and/or business disruption event.

### Sector Impact Model Components

- ✓ **Likelihood:** that an incident occurs
- ✓ **Critical Financial Center:** impact to critical financial center
- ✓ **Critical Supporting Service:** critical sector supply chain disrupted
- ✓ **Member Impact Landscape:** number of members impacted
- ✓ **Dependent Sector:** disruption to critical infrastructure sectors
- ✓ **Risk Complexity:** identified potential for cascading disruption
- ✓ **Member Importance:** escalation by sector stakeholder or FS-ISAC member
- ✓ **National Importance:** impact to National Critical Functions
- ✓ **Systemic Risk:** identified through FSARC and other FS-ISAC sources


## III. Roles and Responsibilities of FS-ISAC Crisis Response Leaders

The financial services sector relies on several FS-ISAC committees and sector organizations to execute the resilience response framework. Depending on the type of event, there are certain financial sector associations authorized to coordinate crisis response and recovery operational routines on behalf of their membership. When the Financial Services Framework is activated, crisis teams perform activities to help coordinate sector response and recovery. These activities are outlined in the roles and responsibilities tables below.

| **FS-ISAC Sector Crisis Response**<br>Group includes: FS-ISAC Global Information Office, Operations and Incident Response Team (IRT) | |
|---|---|
| Respond<br>Recover | • Monitors and assesses cyber and physical threat information, facilitates information sharing, publishes alerts and engages BRC, TIC, CERG and Sheltered Harbor in threat escalation.<br>• Serves as a central point for reporting suspicious activity/event impact, monitoring thresholds, conducting surveys.<br>• Pushes information on cyber and physical incidents to the TIC, BRC, CHEF, Sheltered Harbor, FSARC and joins them in the decision to activate crisis team discussions and engage the CERG.<br>• Facilitates incident communications with CINS to engage sector communities of interest for crisis coordination calls.<br>• Facilitates RFIs (requests for information); communicates with other sectors, government and intel partners.<br>• Monitors the ongoing event and continues to push information on cyber and physical incidents to membership.<br>• Maintains communications with CERG, CMT and BRC and TIC co-chairs throughout incident response/recovery.<br>• Participates in government and cross-sector critical infrastructure, response and recovery activities.<br>**DECISIONS: None, this is a support role for members** |
| **Threat Intelligence Committee (TIC)**<br>Group includes: Head of Security, Intelligence analysts and incident responders | |
| Respond<br>Recover | • Serves as a trusted community of FS-ISAC members which facilitates the planning, direction, coordination, collection, analysis and dissemination of primarily cyberthreat intelligence by engaging with external stakeholders.<br>• Analyzes incident, determines if crisis escalation is required, collaborates with BRC and FSARC.<br>• Facilitates the decision to change the sector cyberthreat level and determine if crisis escalation is warranted.<br>• Provides technical mitigation and incident response guidance.<br>• Informs the CERG of the incident/suspicious activity, maintains communication with CERG, CMT, BRC, FSARC, NCCIC Liaisons and throughout incident response and recovery lifecycles.<br>• Provides communication guidance (incident facts, contingency actions and collaborates to reduce business impact).<br>**DECISIONS: Impact assessment; crisis escalation** |

| | |
|---|---|
| **Business Resiliency Committee (BRC)**<br>Group Includes: Heads of business continuity, disaster recovery, physical security and operational risk management | |
| Respond<br>Recover | • Serves as a trusted community of FS-ISAC members which collaborates to analyze business disruption caused by cyber, physical and systemic threats which may impact the global financial sector.<br>• Analyzes incident and determines if crisis escalation is required, collaborates with TIC, Securities Industry, FSARC and others.<br>• Facilitates decision to change the sector physical threat level; informs CERG and recommends Framework activation.<br>• Shares situational awareness of impact to CI essential functions, critical business and third-party vendors.<br>• Expands meetings, as needed, to include TIC, MRT and other FS-ISAC communities impacted by the crisis event.<br>• Contributes to Cross-Sector Playbook joint courses of actions, by escalating on behalf of members sector impact and mitigation priorities.<br>• Communicates with FS-ISAC global membership to obtain situational awareness for organizations who are leading crisis response and recovery.<br>• Provides communication guidance (e.g., incident facts and contingency actions) contributing to FS-ISAC alert communications to its global membership.<br>**DECISIONS: Impact assessment; crisis escalation** |
| **Media Response Team (MRT)**<br>Group Includes: Media relations, press officers, public affairs | |
| Respond<br>Recover | • Monitors media activity for stories that might significantly impact the reputation of the sector or may require an industry response.<br>• Verifies if a threat with the potential for large-scale disruption of the financial system is real (in coordination with the FS-ISAC's intelligence office, TIC and BRC).<br>• Serves as a coordinating hub among associations and large institutions in case a threat with the potential for large-scale disruption of the financial system has been validated.<br>• Develops and issues holding statements when this type of threat has been validated.<br>**DECISIONS: Validates threats and coordinates messaging** |
| **Core Executive Response Group (CERG)**<br>Group Includes: Key sector representatives, executive leadership of the FSSCC, FS-ISAC, Securities, FSARC, Sheltered Harbor and TIC, BRC, CHEF and MRT Chair(s); US Treasury; expand as needed to respond to a specific event | |
| Respond<br>Recover | • Gathers subject matter experts who participate in FS-ISAC and FSSCC resiliency mission, to determine event impact and significance to the financial sector.<br>• Provides a secondary leadership role during a market event, when Securities market committee is leading crisis response and recovery.<br>• Ensures that FS-ISAC members who are not Securities Industry members are incorporated into incident response.<br>• Determines CMT activation, team composition and incident commander, according to the nature of the threat.<br>• Assigns communication leader and defines authority for the crisis communications team.<br>• Represents the sector in critical infrastructure crisis activities.<br>• Oversees the CMT, to assist in crisis coordination and reconvenes the CERG to assist in policy decisioning.<br>• Uses the CERG activation plan, Appendix A3. **DECISIONS: Activates and composes the CMT** |
| **Crisis Management Teams (CMT)**<br>The CMT is led by CERG, Securities Industry or similar sector organizations; the specialized teams are identified dynamically during crisis event and in advance, during FSARC, FS-ISAC, Securities Industry or other specialized contingency playbook development. Includes subject matter experts to manage sector-level information sharing for a specific event | |
| Respond<br>Recover | • Coordinates status meeting of all aspects of crisis information sharing and collaborative response/recovery efforts.<br>• Interacts with critical external partners to obtain accurate situational awareness and resource support requirements.<br>• Develops and supports industry response and recovery, and activates incident response teams ("IRTs"), as needed.<br>• Solicits sector status via surveys through the FS-ISAC IAT; assesses and coordinates sector needs, (i.e.) waivers.<br>• As needed, specialized Technology CMT will be formed for impacted FI's to collaborate to mitigate cyber disruption.<br>• Uses the CMT activation plan, Appendix A4, as needed.<br>**DECISIONS: Partner collaboration; member calls/communication** |
| **Clearing House and Exchange Forum (CHEF)**<br>Group includes: CISOs and senior level executives of clearinghouses and exchanges globally | |
| Respond | • Engages when a crisis affects the securities industry; representative(s) from the CHEF will participate on the core executive response group (CERG) and crisis management team (CMT) and will coordinate communications and response with the markets and exchanges and Securities Industry as required.<br>• Analyzes cyber, physical and systemic threats that may impact the financial sector and facilitates collaborative planning with respect to sector business resilience, response and recovery capability.<br>• Provides technical mitigation, incident response and communication guidance (i.e., incident facts, contingency actions and collaborates to reduce business impact). **DECISIONS: Impact assessment; crisis escalation** |

| Financial Systemic Analysis and Resilience Center (FSARC) | |
|---|---|
| Respond | • Identifies systemic risk that threatens the stability of the broader financial sector.<br>• Serves as a point of escalation and internal review where key decisions are required as pertains to systemic risk mitigation and response.<br>• Identifies and analyzes incident to determine if the risk is systemic and if crisis escalation is required, collaborates with BRC and TIC.<br>• Assesses and coordinates activities mitigating cyber-based threats and systemic risks to the US financial system;<br>• Provides technical mitigation and incident response guidance.<br>• Recommends activation of the CERG.<br>• Collaborates with FS-ISAC in leading CMT coordination role and response. |
| Recover | • Participates in the CERG during incidents of systemic impact, and where FSARC Scenario and Response Guidelines and crisis coordination planning have been created.<br>• Collaborates with member firms to implement relevant action steps for compromised and non-compromised firms across the incident timeline.<br>**DECISIONS: Activates the CERG and collaborates with FS-ISAC in leading CMT for systemic event response** |
| **Sheltered Harbor (SH)**<br>Sheltered Harbor was created by the financial sector to protect retail customers (banking and brokerage), financial institutions, and enhance public confidence in the financial system in response to a catastrophic event, like a cyberattack, that causes critical systems—including backups—to fail; | |
| Respond | • Initiates Sheltered Harbor "Incident Management Process" in response to an early awareness "Heads-Up," sent to FS-ISAC Incident Reporting by Sheltered Harbor firm(s) experiencing an abnormal impact to its consumer services. |
| Recover | • Validates the "Heads-Up" and establishes an initial situational awareness exchange(s) among the FS-ISAC analyst, Sheltered Harbor staff and the firm issuing the "Heads-Up" to gather facts and any available indicators, using FS-ISAC capabilities.<br>• Assists impacted organizations and provides relevant information if other organizations are experiencing similar issues (while maintaining confidentiality of impacted parties).<br>• Depending on the situation information received and the extent of impacts being experienced in the sector, Sheltered Harbor and FS-ISAC Incident Reporting will determine if conditions exist for recomending crisis escalation to the BRC.<br>• In accordance with BRC responsibilities, will inform & recommend to CERG or CHEF escalation to FSCR Framework.<br>• Sheltered Habor staff assists impacted organization(s) and, with their approval, provides relevant information to other organizations.<br>• Coordinates and provides information to support impacted organization(s) as a firm decides whether to invoke, the firm's planned account data restoration process; and establishes contact, if requested, with other Sheltered Harbor firms that may assist an impacted firm.<br>**DECISIONS: Initiates its Incident Management Process and supports restoration efforts** |

## Roles and Responsibilities of Sector Stakeholders

Financial sector stakeholders lead crisis response coordination activities when critical functions of the sector are disrupted.

| Financial Services Sector Coordinating Council (FSSCC)<br>Private-sector firms and financial trade associations that coordinate sector needs and requirements | |
|---|---|
| Respond | • Serves on the Core Executive Response Group (CERG) and engages in crisis response, assessing impacts to the Sector and interfacing with the FBIIC as necessary. |
| Recover | • Coordinates Sector policy issues and requirements and will participate in developing strategic objectives derived from exercises and incident lessons learned.<br>**DECISIONS: Impact assessment; crisis escalation** |
| **Securities Industry and Financial Markets Association (SIFMA)** | |
| Respond | • Monitors the US equity, fixed income, cash and derivative markets for operational or technology incidents that could lead to a failure of market integrity. |
| Recover | • Activates a virtual Securities Industry Emergency Command Center; sits on CERG and assists in determining impacts to the sector.<br>• Serves as a central point for coordinating the exchange of information on incidents and issues identification and resolution for the securities industry.<br>• *Securities Industry Emergency Command Center*: Interfaces with exchanges, financial utilities, market participants, regulatory agencies, and NYC OEM to coordinate communications, situational awareness and response efforts.<br>• *Securities Industry Market Response Committee*: Coordinates and facilitates the decision-making process surrounding the opening and closing of US Fixed Income and Equity Markets.<br>**DECISIONS: US Equity Market and US Fixed Income Market - Open/Close Recommendation** |

| Payments Risk Committee (PRC) | |
|---|---|
| Respond<br>Recover | • Fosters enhancements to the safety and efficiency of financial market infrastructure, as a primary goal of the committee.<br>• Convenes PRC Emergency Conference Call Arrangement in response to events that could cause a significant disruption (e.g. operational, liquidity, etc.) to US PCS activities to share information among PRC call guide participants.<br>• Coordinates information sharing among members; the PRC will not manage incidents.<br>• Directs PRC participants to request an Emergency Conference Call Arrangement by contacting the FRBNY ex-officio members of the PRC,<br>• Created and maintains a day one playbook for the recovery of payments activity to provide a coordinated risk mitigation strategy and rapid response plan to help reduce the potential impact of an outage in the US payments market.<br>**DECISIONS: None, PRC is not a decision-making body** |

# IV. US Government Crisis Response Coordination*

**Private and Public-Sector Coordination of Crisis Incident Severity**
The US Department of the Treasury serves as the Sector-Specific Agency for the financial sector, as defined in Presidential Policy Directive 21 and provides a central point for voluntary crisis response collaboration. When a crisis event unfolds, the Treasury, working closely with other government agencies and the private sector, will seek to evaluate the consequences of an incident to the sector and more broadly so that all entities can communicate effectively, facilitating a coordinated response (Appendix A5 – US Government Crisis Level Definitions).

## US Government Crisis Response and Recovery Teams, Activities and Decisions

| Treasury (OCCIP) – US Department of Treasury, Office of Cybersecurity Critical Infrastructure Protection | |
|---|---|
| Respond | • Serves as a central liaison between public and private sector stakeholders for information sharing and facilitation of federal, state and local support and assistance, as appropriate.<br>• Consults, as appropriate, with the CERG to obtain information on threat and attack information.<br>• Provides FS-ISAC with timely and actionable all-source information on cyberthreats to the financial sector.<br>• Maintains situational awareness with DHS and other government agencies.<br>• Solicits information requirements from the sector.<br>• Responds to requests as part of a Request for Information (RFI) process.<br>• Serves as an observer to the BRC, CERG and CMT discussions and analysis.<br>**DECISIONS: Assess potential impact to the financial sector** |
| **Department of Homeland Security - Cybersecurity and Infrastructure Security Agency (CISA) and National Cybersecurity and Communications Integration Center (NCCIC)** | |
| Respond<br>Recover | • Conducts 24x7 threat and attack monitoring and identifies potential impacts of incidents on the sector.<br>• Maintains situational awareness, shares information (via sector alerts and advisories, analyst exchange, threat briefings) with the NCCIC Liaison, SOCs and financial services sector leadership as appropriate.<br>• Works with sector leadership to provide information to the sector and government partners on the incident, sector impact and suggested mitigation strategies.<br>• Provides incident response and threat hunting assistance upon request, pursuant to a Request for Technical Assistance.<br>**DECISIONS: Determine if the incident is of national-level significance and requires national-level coordination** |
| **CISA (NICC) – DHS National Infrastructure Coordinating Center** | |
| Respond<br>Recover | • The NICC maintains 24/7 situational awareness and crisis monitoring of critical infrastructure and shares threat information in order to reduce risk, prevent damage and enable rapid recovery of critical infrastructure assets from incidents caused by natural disasters, attacks, or other emergencies.<br>• Collect, maintain and share information about threats/hazards of concern to critical infrastructure, focused on natural hazards (acts of nature), Technological hazards (accidents or failure of systems and structures) and human-caused incidents (intentional actions of an adversary).<br>• Provides situational awareness for the Critical Infrastructure Key Resource (CIKR) community through: Private sector crisis management calls; situational reports; and processing of RFIs, as needed.<br>**DECISIONS: Determine if incident is of national-level significance and requires national-level coordination** |
| **CISA Physical Incident Management Support** | |
| Respond<br>Recover | • Serve as ESF Coordinator for ESF 2 and ESF 14 Coordinator.<br>• Leverage Protective Security Advisors to provide critical infrastructure expertise to state and local emergency operations centers.<br>• Develop analytic products and maps to help inform decision-making by CISA leadership, Federal partners, the interagency, and private sector partners.<br>• Staff CISA liaison position at the DHS National Operations Center and FEMA National Response Coordination Center. |

| Financial and Banking Information Infrastructure Committee (FBIIC) | |
|---|---|
| Respond<br>Recover | • Establishes and engages a mechanism for conducting rapid coordination of the financial sector regulators in the event of significant cyber or physical incidents impacting financial institutions or the financial services sector.<br>• Leads emergency conferences ensuring sharing among FBIIC members of timely and actionable incident information and provide a source of shared situational awareness of incidents as they unfold.<br>• Coordinates information exchange about incidents but does not manage incidents.<br>• Facilitates conferences which may be requested by members; necessity may be identified through a variety of sources, including members, law enforcement, the intelligence community, DHS or other private sector, government and international partners. **DECISIONS: Impact assessment, crisis activation** |
| **Federal Deposit Insurance Corporation (FDIC)** | |
| Respond<br>Recover | • Coordinates response activities with federal and state banking regulators to monitor the operational status of FDIC-insured financial institutions.<br>• Provides a conduit to facilitate requests for assistance (RFA) from FDIC-supervised financial institutions to the US Government through Treasury/FEMA.<br>• Provides regulatory relief guidance to help financial institutions and facilitate recovery in areas affected by a disaster.<br>• Establishes a disaster web page on fdic.gov and provides talking points for the FDIC Call Center to provide information to banks and bank customers affected by a disaster.<br>**DECISIONS: Coordinates monitoring, assesses impact, considers supervisory response and messaging** |
| **Federal Reserve System (FRS)** | |
| Respond<br>Recover | • Monitors incident response by supervised institutions.<br>• Exchanges situational awareness with FBIIC and Federal Financial Institutions Examination Council (FFIEC).<br>• Participates, as circumstances warrant, in Cyber UCGs convened in response to a significant cybersecurity incident.<br>• Coordinates with FFIEC, FBIIC and Cyber UCG to develop and implement a communications strategy, as necessary, regarding a significant cyber-incident.<br>**DECISIONS: Assess potential impact to sector and financial stability; consider supervisory, payments or policy response** |

# V. Trusted Cross-Sector and Global Stakeholders

FS-ISAC participates with cross sector and global stakeholders during crisis response to provide accurate situational awareness and escalation of member needs.

## Cross Sector and Global Situational Awareness Collaboration

| Tri-Sector Playbook<br>The Communication Coordination Council, Electricity Sub-Sector Coordinating Council and the FS-ISAC | |
|---|---|
| Response<br>Recover | • Collaborate across sectors during a time of a significant failure of critical infrastructure, to facilitate response and recovery, identify sector interdependencies and obtain priority support for their sector essential funcctions and members.<br>• Follow Cross-Sector Playbook activation thresholds to jointly validate crisis facts and develop joint courses of action in advance of meetings where sector executives and government to inform and prioritize decision making.<br>**DECISIONS: Recommend joint courses of action and recovery priorities** |
| **National Council of ISACs (NCI)** | |
| Respond<br>Recover | • Serves as a voluntary cross-sector body of ISACs and sector critical infrastructure and key resources (CIKR) that meet regularly to discuss issues of common interest primarily around operational matters.<br>• Engages in cross-sector information sharing among the sectors, as appropriate.<br>• Shares incident information and publishes RFIs to other NCI members through the NCI list server.<br>**DECISIONS: Identify and escalate events that affect or have an impact upon multiple sectors** |
| **Regional Partnership Council (RPC*first*)** | |
| Respond<br>Recover | • Serves as an umbrella organization established to foster collaboration among the regional partnerships that have formed across the US focusing on homeland security and emergency management issues with the public sector.<br>• Builds local and state crisis response partnerships and information sharing through coalitions in numerous states.<br>• Contacts the FIRST coalition located in impacted areas during a crisis. Coalitions will seek to provide or obtain daily incident information, obtain access to activated emergency operation centers during an emergency, and collaborate in learning more about evacuations, credentialing, and regional response.<br>• Utilizes relationships with local, county, and state govt., providing FS-ISAC network with crisis event ground truth.<br>**DECISIONS: Share information, member calls/communication** |

| Global Resilience Federation (GRF) | |
|---|---|
| Respond | • Serves as an infrastructure organization that facilitates development, maintenance and cross-sector sharing for nonprofit ISACs/ISAOs/CERTs and cultivates secure collaboration between multiple industries around the world.<br>• Establishes community crisis response partnerships through coordinating information sharing among GRF members and supported communities.<br>• Engages in crisis management and resilience activities to support the BRC during significant events;<br>• Coordinates development of response and recovery tasks and international and cross-sector outreach to enable rapid response and protection of community's critical assets.<br>• Facilitates situational awareness and updates to GRF members/supported communities through dedicated SOC staff.<br>**DECISIONS: Identify and escalate events that affect or have an impact upon multiple sectors** |
| Recover | |

# VI. Event Closure

## Event Closure & Playbook Improvement

After the crisis subsides, collaborative crisis response participants facilitates an after-action assessment to identify and coordinate evaluation of lessons learned, identifying areas of sector collaboration improvement and direction for revising of the *US Playbook appendix* as appropriate. Once the crisis ends, the crisis coordination teams return to steady-state responsibilities for cyber and physical threat information sharing. The CMT and CERG stand down and are closed. Improvements will be incorporated into the next revision of the US Playbook appendix.

# Appendix A1 – FS-ISAC Playbook Inventory, US Government Resources and Templates

Crisis resource guides, plans and references are used during a crisis event, as needed, to provide sector detail that supplements the *Financial Services Crisis Response Framework*.

| | FS-ISAC Playbook/Framework Inventory | Source | Last Update |
|---|---|---|---|
| Sector Playbooks/Frameworks | • TLP White **FS-ISAC All Hazards Framework** | FS-ISAC | Sep 2019 |
| | • TLP Green **US Playbook Appendix** | FS-ISAC | Sep 2019 |
| | • TLP Amber FS Communication Playbook | FS-ISAC | Nov 2016 |
| | • TLP Green FF Cyber and Physical Threat Call Procedures and Guidelines | FS-ISAC | Mar 2015 |
| | • TLP Amber **Tri-Sector Playbook** (financial, electricity, communication sectors) | FS-ISAC | Jan 2019 |
| | • TLP **Amber FSSCC** Reconnection Framework | FSSCC | Aug 2018 |
| | • TLP **Amber FSARC** Scenario and Response Guidelines | FSARC | May 2018 |
| | • TLP **Amber Securities Industry** BCP and Market Response Committees Overview | Securities Industry | Sep 2018 |
| | • TLP **Amber Sheltered Harbor** Incident Management Guide | | Jan 2019 |
| | • TLP **Amber Sheltered Harbor** Incident Communications Playbook | Sheltered Harbor | Jan 2019 |
| US Gov. Resources | • TLP White NCIRP, National Cyber Incident Response Plan | DHS | Dec 2016 |
| | • TLP White PPD-41 Cyber Incident Coordination | DHS | Jul 2016 |
| | • TLP White National Response Framework | DHS | May 2013 |
| | • TLP White PPD.8.National Preparedness Goal | DHS | Sep 2015 |
| | • TLP White Response Federal Interagency Operational Plan | DHS | Aug 2016 |
| | • TLP White Recovery Federal Interagency Operational Plan | DHS | Aug 2016 |
| | • TLP White Request for Technical Assistance | Treasury and FS-ISAC | |
| | • TLP Green Financial Services Sector Cybersecurity Enhanced Coordination Procedures | | Mar 2017 |

| Templates<br>Templates are used to create Country/Region Playbooks and event-specific plans. | Last Update |
|---|---|
| **TLP Green Playbook Appendix** is developed by financial sector leaders to articulate the coordination activities within a country or region, identify the stakeholders who lead coordination and define how trusted information sharing global activities can be utilized by Playbook stakeholders. | Jun. 2019 |
| **TLP Green Crisis Role and Responsibilities Table** defines the role and decisions made by key stakeholder groups and subject matter experts who will engage during an event. | Feb. 2016 |
| **TLP Green FS-ISAC Member Crisis Process Flow Template is a** walkthrough how FS-ISAC members and other sector teams coordinate crisis response information sharing. | Jul. 2016 |
| **TLP Red CERG Contact Roster** recommend sector leaders who will join the CERG escalation calls. | Feb. 2016 |
| **TLP Green CERG Event Specific Call Agenda meeting** outlining agenda based on customized Playbook and event | Mar. 2019 |
| **TLP Red CMT Contact Roster** recommend sector leaders and subject matter experts (SMEs) who will participate in CMT status meetings. May be used when specialized critical business process event Playbooks are developed. | Mar. 2019 |
| **TLP Amber Technology CMT Agenda meeting** outlining agenda based on customized Playbook and event. May be used during a crisis event to guide specialized technology or third-party provider crisis coordination calls. | Apr. 2019 |
| **TLP Green FS Quick Reference Guide Template p**rovides a one-page overview of the crisis team roles. | Feb. 2016 |
| **TLP Amber Map the Timeline of Coordinated Crisis Response** documents trusted stakeholder engagement. | Apr. 2019 |

## FS-ISAC Traffic Light Protocol

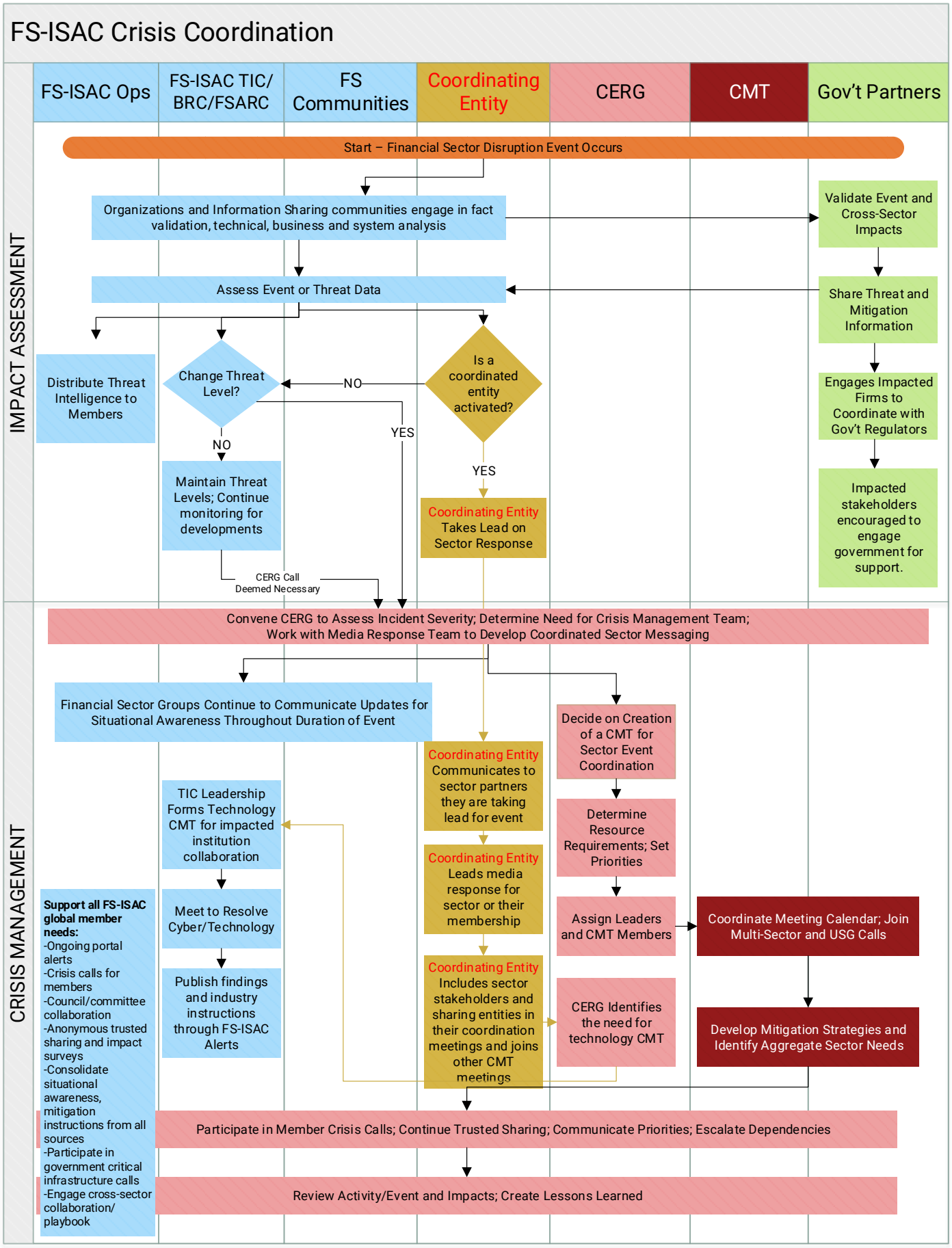
**(TLP) RED** – Recipients may not share TLP RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed

**(TLP) AMBER** – Recipients may only share **TLP AMBER** information with members of their own organization who need to know, and only as widely as necessary to act on that information.

**(TLP) GREEN –** Recipients may share TLP GREEN information with peers, trusted government and critical infrastructure partner organizations and services providers with whom they have a contractual relationship, but not via publicly accessible channels.

**(TLP) WHITE** – **TLP WHITE** information may be distributed without restriction, subject to copyright controls.

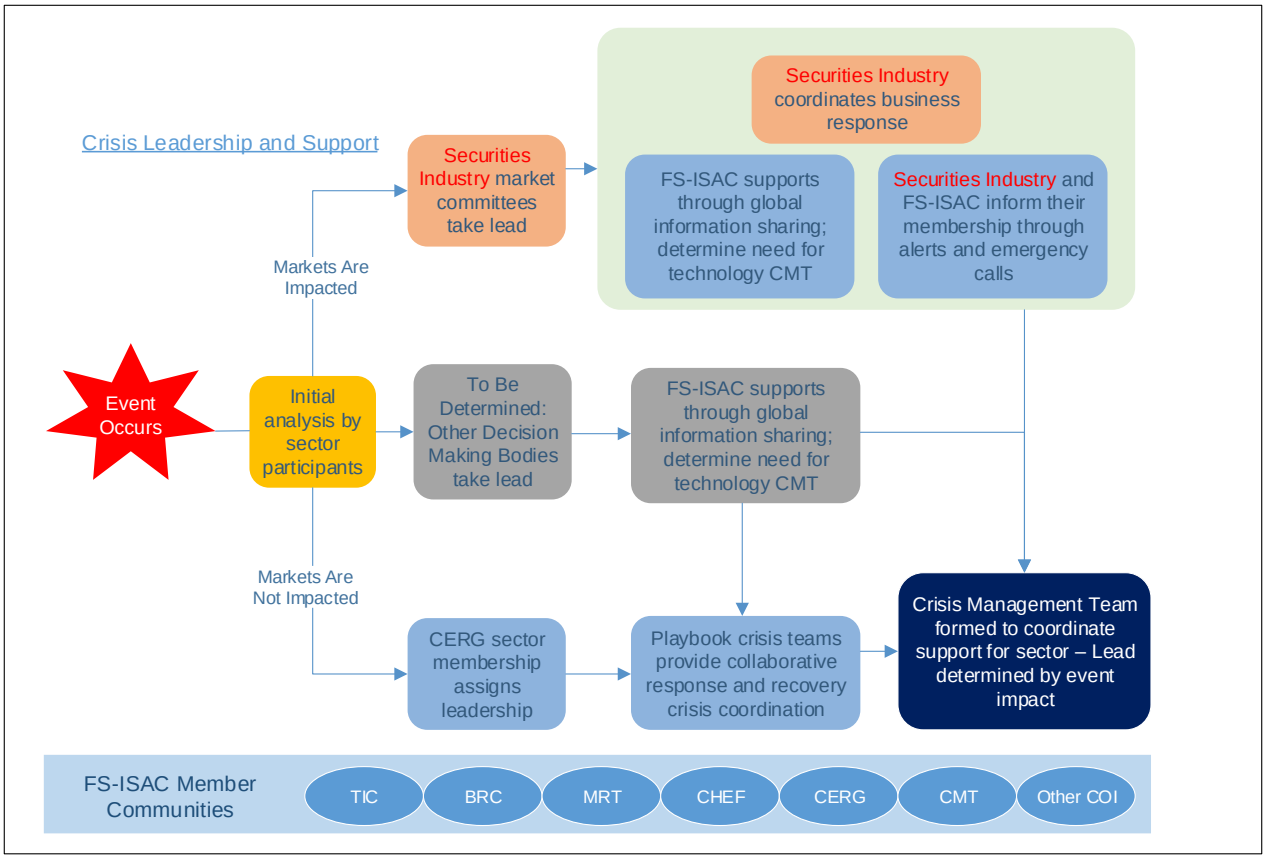
# Appendix A2 – FS-ISAC Event Response Coordination Process



# Appendix A3 – Core Executive Response Group (CERG) Activation Plan

The Core Executive Response Group brings information sharing leaders across the sector together to discuss event impact and significance to the financial sector. Additional experts join the CERG to determine if sector coordination is needed to mitigate immediate and ongoing threat. Securities Industry is a member of the CERG and plays a leading role during a market disruption event. If a market event is being led by Securities Industry, **the CERG identifies additional coordination activities needed to support the financial services stakeholders and FS-ISAC members**. A meeting of the CERG will be convened via conference call or Critical Infrastructure Notification System (CINS) ***CINS activation can be requested by contacting FS-ISAC IncidentReporting@fsisac.com or (877) 612-2622, prompt 2.***

**CERG Discusses Crisis Leadership**




## Sample CERG, BRC, TIC, CMT Crisis Assembly Meeting Agenda

| Agenda Item | Responsibility | Protocol |
|---|---|---|
| **Roll Call** | ➢ **FS-ISAC Crisis Response Lead** | Join call early |
| **Call Leader** | ➢ **FS-ISAC CEO. If not available: COO, Chief of Staff; FSSCC Chairman** | |
| **Situational Update** | ➢ Depending on event, situational awareness is begun by: **Securities Industry, FS-ISAC leadership, Trade org., FSARC or another TBD stakeholder** | Provide summary of event |
| | ➢ **NICCIC liaison, TIC, MRT, BRC** leaders report on event collaboration and priorities | Summarize critical issues |
| | ➢ **US Treasury** provides summary of government and industry collective actions | |
| | ➢ **Invited Stakeholders** join to contribute to collaborative response and recovery | |

## Actions of the CERG:

- ☐ Discuss impact to sector; identify the need for an event CMT; confirm leadership, meeting frequency and agenda.
- ☐ Designate a CMT and MRT leads for non-market impact events.
- ☐ Identify technology coordination taking place between impacted FI's. Confirm the need for Technology CMT.
- ☐ Engage third-party vendor to join in CMT situational awareness meetings.
- ☐ Identify the need for sector messaging, for non-market events. Provide instruction to FS-ISAC to support membership information sharing needs for all events.
- ☐ Request FS-ISAC Community polling to assist in financial sector impact and mitigation efforts.
- ☐ Identify critical needs, gaps for remediation; prioritize them.
- ☐ Identify issues for next meeting; assign task leads.
- ☐ Deconflict meetings taking place with other sector stakeholders or government; communicate logistics for next conference call.

# Appendix A4 – Crisis Management Team (CMT) Activation Plan

The Crisis Management Team (CMT) manages crisis information sharing, team coordination crisis support and recovery efforts. Crisis event subject matter experts engage to assist in sector mitigation, response and recovery.

## CMT Action Plan:

1. The CERG or other leading organization, will form the CMT and recommend subject matter experts needed to coordinate a sector response.
2. A meeting of the CMT will be convened via conference call or CINS to determine the consequences of the event and disruption to the sector. During the call, the main objectives will be to:
   a. Inform the other members of the team regarding details surrounding the incident;
   b. Determine what is unknown; identify sources needed to provide sector coordination and communication;
   c. Identify the leading financial sector trade groups, critical process and third-party organizations which are leading crisis response and recovery collaboration and coordination efforts within the sector. These organizations are invited to join the CMT to acknowledge their event leadership roles and align their respective framework activities, with CMT information sharing and crisis communication activities;
   d. Outline content for event executive brief and reporting;
   e. Outline and guide the event response plan;
   f. Deconflict overlap of crisis meetings; create an event meeting schedule for private and public coordination calls;
   g. Assign member survey activities; and
   h. Assign Crisis Media Response Team spokesperson and assist in building Crisis Media Response Team members for the event.
3. As needed, the CMT interacts with partners, third-parties, government and other sources to obtain accurate situational awareness and identify resource requirements and priorities.
4. CMT develops and supports industry response and recovery and activates specialized incident response teams as needed. These may include specialized technology teams or pre-defined systemic event disruption teams, such as those defined through FSARC contingency planning.
5. The CMT will continue to meet as required until the members determine the crisis is resolved.
6. Once the crisis is resolved a set of lessons learned will be generated specific to the communications process and procedures executed for the crisis.

## CMT Roles, Responsibilities

In the event of an industry-wide incident that requires cross-organizational coordination, the following roles will be assigned to facilitate the work of the Crisis Management Team.

| Operational Role | Responsibilities | Assignee |
|---|---|---|
| **CMT Leader** | Responsible for all aspects of an emergency response; including quickly developing incident objectives, managing all incident operations, application of resources as well as responsibility for all persons involved. Will set priorities and define the organization of the incident response teams and the overall actions to be taken. | **PRIMARY:** TIC Executive or BRC Co-Leader<br>**BACK-UP:** TIC Executive or BRC Co-Leader |
| **CISA Embedded Liaison** | Responsible for serving as a liaison to the NICC / NCCIC during an event/crisis. Provides a mechanism for incident management coordination among government and private sector stakeholders. Integrates information regarding infrastructure status, risk management and incident response and recovery operations. Supports comprehensive CIKR-focused situational awareness, impact assessments and courses of action. | **PRIMARY:** FS-ISAC Government Liaison<br>**BACK-UP:** FS-ISAC Government Liaison |
| **Communication Leader** | Responsible for coordinating, drafting and disseminating single flow of communications throughout the duration of an event. Specifically, responsible for drafting Sector-wide communications for approval of the Incident Commander and coordinates the development of any required surveys. | **PRIMARY:** Identified in Com Playbook<br>**BACK-UP:** Identified in Com Playbook |
| **Issue Identification/ Resolution** | Maintains the 'Big Picture' of the overall response and looks ahead to potential issues / roadblocks that are looming or not yet addressed. Recommend actions to mitigate results. | Subject Matter Experts for the event. |
| **Market Impact Coordination** | Responsible serving as the liaison with market committees. Supports comprehensive open/close market situational awareness, impact assessments and courses of action. | **PRIMARY:** Securities Industry<br>**BACK-UP:** Securities Industry |
| **Cross-Sector Coordination** | Responsible for mobilizing interaction with critical partners and agencies obtaining accurate situational awareness and resource requirements (to and from FS-ISAC). The voice of the coordinating council to enable priority response support based on established relationships. | **PRIMARY:** FS-ISAC Crisis Leader<br>**BACK-UP:** FS-ISAC Crisis Leader |
| **Impact Aggregation** | Responsible for compiling the degree/severity of impact with regards to the financial sector. Aggregates the initial assessment for 'worst-case' impact during early stages of a catastrophic event with limited access to ground-truth assessment. Compiles information from all available sources for vertical reporting. | **PRIMARY:** US Treasury, FSARC<br>**BACK-UP:** US Treasury, FSARC |
| **Scribe** | Responsible for documenting meeting attendance, minutes, task assignments and follow-up accounting. Aggregates in-situation lessons learned during course of an event. | FS-ISAC crisis response staff |

# Appendix A5 – US Government Crisis Definitions and Impact Tools

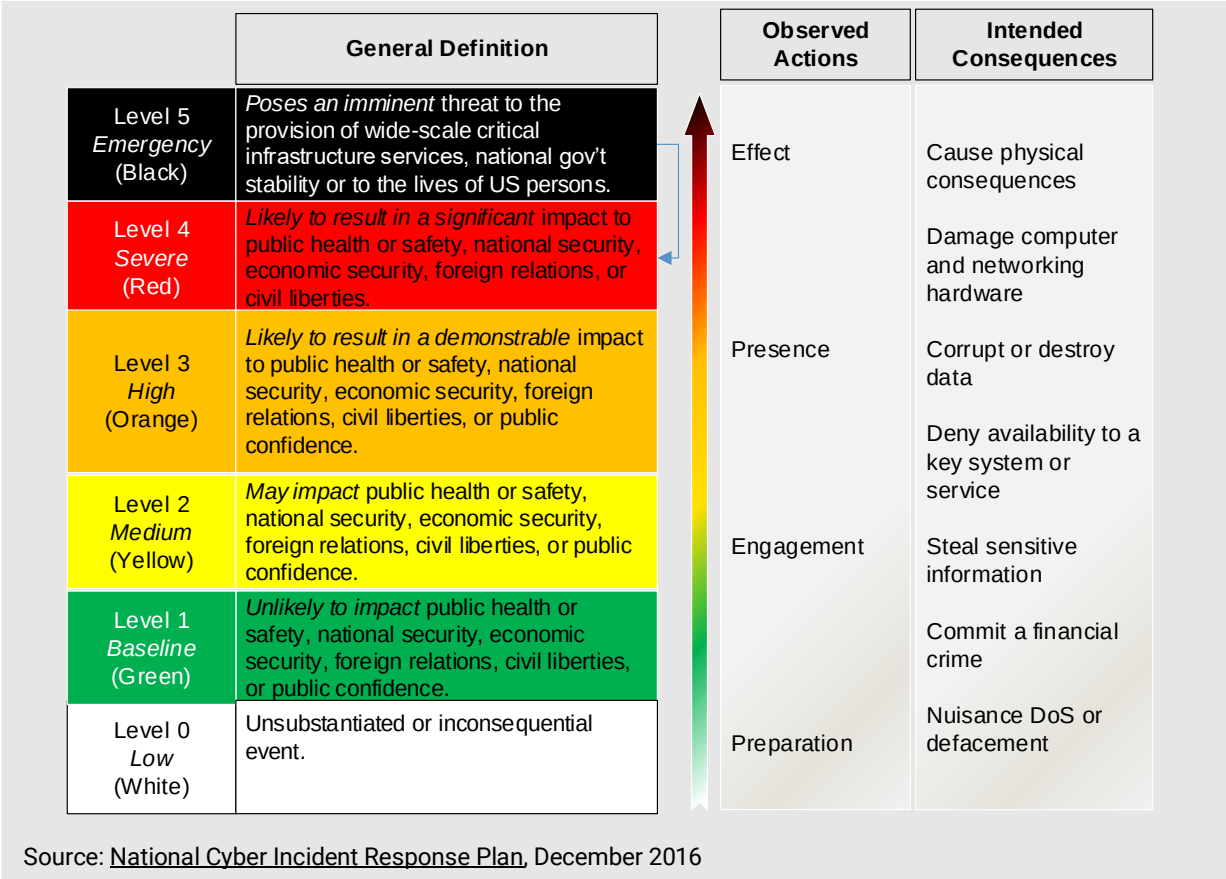
## Cyber Incident Definitions from PPD-41

The National Cyber Incident Response Plan describes the difference between a "cyber incident" and "significant cyber incident"; the NCIRP includes government response mechanisms for a significant cyber incident.

| Incident | Definition |
|---|---|
| Cyber Incident | An event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. |
| Significant Cyber Incident | A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. |

## US Government All-Hazards Severity Matrix

FS-ISAC coordinates with US Government agencies during a crisis. The US Government has a variety of policies and procedures that govern the response of regulators and other government agencies. The US Government uses the following matrix for defining the severity of a threat or incident which may drive actions that the US Government might take.




Source: National Cyber Incident Response Plan, December 2016

## NCCIC Cyber Incident Scoring System

The NCCIC Cyber Incident Scoring System is used by National Cybersecurity and Communications Integration Center personnel to evaluate risk severity and incident priority from a nationwide perspective.