Financial Services Information Sharing & Analysis Center FS-ISAC

Operating Rules
June, 2016

Contents

1.0 FS-ISAC History and Background

On July 15, 1996, the President of the United States signed executive order 13010 creating the President's Commission on Critical Infrastructure Protection (PCCIP). This commission was created to bring together the public and private sector to assess infrastructure vulnerabilities and develop assurance strategies for the future. The PCCIP identified the Banking and Finance Sector as one of eight critical infrastructures that require review and assurance strategies.

The commission advocated a strategy of "information sharing" in a "quantitative risk-assessment process". Through these processes the commission has developed policy and goals necessary to effect the recommendations of the commission.

On May 22, 1998, the President of the United States signed Presidential Decision Directive/NSC-63 (PDD-63), Critical Infrastructure Protection. This directive established government policy direction and national goals to address issues and recommendations made by the President's Commission on Critical Information Infrastructure Protection in their report completed in September 1997 (The Report of the President's Commission on Critical Infrastructure Protection, "Critical Foundations - Protecting America's Infrastructures", October 1997).

The PDD-63 recommended that within five years of the date of the PDD the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures, including Banking and Finance, from intentional acts that would significantly diminish the abilities of:

- The Federal Government to perform essential national security missions and to ensure the general public health and safety.
- State and local governments to maintain order and to deliver minimum essential public services.
- The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

The Banking and Finance Sector accepted as one of its objectives the establishment of a singular **Financial Services Information Sharing and Analysis Center (the "FS-ISAC").** *The FS-ISAC's mission is to help assure the resilience and continuity of the global financial services infrastructure and individual firms against intentional acts that could significantly impact the sector's ability to provide services critical to the orderly functioning of the global economy.* The FS-ISAC primary objective was and continues to be to disseminate and foster the sharing of relevant and actionable information among participants to ensure the continued public confidence in global financial services.

Since its formation in 1999, the FS-ISAC has experienced exponential growth in its membership and in the quantity, quality and value of the information shared. The FS-ISAC has established formal information sharing programs with various government agencies including the U.S.

Department of Treasury, Department of Homeland Security (DHS), Department of Defense, law enforcement (FBI, U.S. Secret Service, NYPD), intelligence agencies, and regulators. Cross-sector information exchange has also been formalized and integrated into the operating procedures of the FS-ISAC. The FS-ISAC and its members also partner with and collaborate on multiple information sharing initiatives and exercises within the sector and with other sectors.

The FS-ISAC Security Operations Center (SOC) monitors hundreds of open source websites and private sources of information for relevant and actionable cyber and physical threat, vulnerability and attack data. The most valuable source of information comes from the members themselves who share information either with attribution or anonymously through the secure portal. All FS-ISAC members are encouraged to share information to help protect the financial services sector and make it more resilient.

2.0 Overview

2.1 FS-ISAC (Financial Services Information Sharing & Analysis Center)

2.1(a) The FS-ISAC portal, database and information sharing tools are located in a secure facility. The FS-ISAC provides for authenticated and, when appropriate, anonymous and confidential input from its membership. It also shares and disseminates information associated with physical and cyber incidents, threats, vulnerabilities, and resolutions or solutions associated with the sector's critical infrastructures and technologies. The information is shared securely via the portal among members of the FS-ISAC, Inc. and CNOP participants within the financial services sector.

2.1(b) Terminology and Definitions:

1. Eligible firms may register as a Critical Notification Only Participant (CNOP) or subscribe as a fee paying member of the FS-ISAC. Fee paying members have access to the FS-ISAC portal and have privileges and benefits not offered to CNOP Participants. In this document *Participants will mean all eligible firms in the financial services sector (both CNOP firms and fee paying members) and Members will mean fee paying Basic, Core and above subscribers. Critical Notification Only Participants are those who register for Urgent and Crisis Alerts but do not pay a fee, do not have access to the FS-ISAC Portal, and are not considered Members. The CNOP category was created to enable the FS-ISAC to reach as many financial institutions as possible within the financial services sector during a major physical or cyber crisis or threat.*

2. *Primary Contact* is defined as the person in the Participant firm to whom all FS-ISAC notices, invoices (Basic, Core and above), and other information is delivered. The Primary Contact represents the Participant and attests to the FS-ISAC Board that its employees, agents and consultants who use the FS-ISAC will comply with the Operating Rules of the FS-ISAC and ensure strict confidentiality of FS-ISAC information. The Primary Contact is responsible for ensuring all Access Coordinators are current and have the need for credentials and have the appropriate authority to use the credentials issued by the FS-ISAC.

3. *Access Coordinators* are those employees, agents and contractors identified by the Primary Contact as authorized to have FS-ISAC credentials.

4. *Member Proprietary Information* means any information in any form voluntarily provided by the Participant to the FS-ISAC under these Operating Rules. The FS-ISAC will handle the information in accordance with these Operating Rules.

5. *FS-ISAC, Inc. Proprietary Information* means (i) any information in any form provided by the FS-ISAC to participants under these Operating Rules; and, (ii) any intellectual property defined and identified as such.

6. *Operator Proprietary Information* means all specifications, computer programs, upgrades, processes, know-how, and other intellectual property embedded in the FS-ISAC, except as defined and documented as belonging to the FS-ISAC, Inc.

7. The term *FS-ISAC website* or *website* means the public facing Internet website at www.fsisac.com.

8. *FS-ISAC Portal* or *Portal* refers to the Internet site that provides access to the private information that is exclusively available to FS-ISAC members after successful completion of the authentication process.

2.1(c) The database of information created is augmented by information provided by commercial, government and other sources of relevant information. Information submitted by the members will not be shared with non-members unless the member indicates it is permissible to share the submitted information to other specified groups such as law enforcement, Department of Homeland Security, other sectors, or with other affiliated entities that may enter into information sharing agreements with the FS-ISAC.

2.1(d) Members will be limited to regulated Banking and Financial Services companies and their service providers which provide critically important services to secure their networks and infrastructure and which meet the eligibility criteria established by FS-ISAC, Inc. as defined in Section 3.1,

2.1(e) Members will enroll by completing the appropriate FS-ISAC Subscriber Application, accepting the Subscriber Agreement and paying any applicable annual fee (for Basic, Core and above members) based on the organizations' requested level of service, identifying the Primary Contact, and identifying authorized access coordinators within their organization ("access coordinators"). Member organizations and their users of the FS-ISAC agree to abide by the Subscriber Agreement and the FS-ISAC Operating Rules.

2.1(f) There are eight levels of service:

NOTE: In order to qualify for CNOP or Basic membership, the financial services organization must be a depository financial institution (as defined by the Federal Reserve Act of 1916) and the organization must have less than one billion dollars in assets. All other membership levels are determined by either the value of the organization's assets, as in the case of depository financial institutions and brokerage firms, or by its revenues, as in the case of insurance companies, processors, associations, and other membership categories. Nonpublic investment firms that do not disclose revenues or assets may be assessed membership fees based on "assets under

management." The breakpoint for these different levels is determined by the FS-ISAC Board of Directors and is published on the FS-ISAC website.

1. ***CRITICAL NOTIFICATION ONLY PARTICIPANTS* (CNOP)** CNOP subscribers will receive only essential urgent and crisis alerts via email. A CNOP subscriber is not considered a member, has no access to the portal, and pays no membership fee. An institution can have only one CNOP email address.

2. ***BASIC MEMBERS***: Basic Members will receive urgent and crisis alerts via email, will be able to submit both anonymous and attributable information, and will be able to participate in industry surveys. Basic Members are able to access portal content except that which is provided by partners, such as NC4, CrimeDex, etc., and can participate in the TLS Registry and view the Member Contact Directory. Basic members are limited to one user ID per membership fee. Basic members may attend Member meetings for an additional fee.

3. ***CORE MEMBER***: Core Members will receive all services applicable to Basic Members, in addition to access to actionable alerts from partner and government and member sources, the ability to customize notification profiles, access to the 24x7 Watch Desk, and access to timely reports on industry trends and best practices. Firms can enroll up to four employees under Core membership. Core Members may attend Member meetings for an additional fee.

4. ***STANDARD MEMBER***: Standard Members will receive all services provided to Core Members and additional benefits including participation on threat conference calls. Standard Members have fewer portal accounts than Premier Members and must pay additional fees to attend the Member meetings.

5. ***PREMIER MEMBER***: Premier Members will receive all services provided to Standard Members and premium services including full portal functionality, a higher number of user IDs, the ability to participate on FS-ISAC committees and work groups, eligibility to serve on FS-ISAC governance bodies, and have no cost to attend the annual Member meetings, and additional benefits for paying an annual fee.

6. ***GOLD MEMBER***: Gold Members will receive all services provided to Premier Members, have a higher number of user IDs than Premier Members, have additional benefits outlined in their Member agreement, can attend some Board meetings, and receive other benefits for an additional annual fee.

7. ***PLATINUM MEMBER***: The Platinum Members will receive all services provided to Gold Members, have an unlimited number of user IDs, can attend some Board meetings, and have other benefits for an additional annual fee.

8. ***MANAGED SERVICES PROVIDER:*** The MSP Member will receive services provided to Standard Members. However, an MSP may not participate on FS-ISAC committees and work groups, or distribution lists where sensitive information is shared with attribution, except where a special need is recognized and participating members agree to invite the MSP to participate. The MSP Member will not have access to FS-ISAC RED content. The MSP Member will have two no-cost passes available for members of their security team to attend the Spring and Fall FS-ISAC conferences.

A complete description of the services available and minimum required membership levels is available on the FS-ISAC Website at www.fsisac.com.

2.1(g) The FS-ISAC, Inc. will be governed and managed under the processes and authorities established in the by-laws of the corporation. Generally, the board of directors is composed of elected representatives from the membership. The board will elect a chairman and the other officers of the company annually. The board will meet regularly to review and discuss matters pertaining to the company, to provide oversight over company matters, and to provide strategic direction to the management team. Daily management of the company is the responsibility of the President, who is also the chief executive officer of the company. Various standing committees, composed of representatives from the membership, exist and will meet regularly to provide strategic guidance, industry context and subject matter expertise, and direction.

2.1(h) A standing committee, the Threat Intelligence Committee (TIC), will be chartered to ensure that members have access to timely and relevant information pertaining to cybersecurity threats and incidents. The TIC will have primary oversight over cyber events affecting the sector, will coordinate actions during a crisis, and will be the primary control point for the Cyber Threat Alert Level for the sector.

2.1(i) A standing committee, the Business Resilience Committee, will be chartered to ensure that members have access to timely and relevant information pertaining to business continuity, disaster response and physical security services. The BRC will have primary oversight over physical events affecting the sector, will coordinate actions during a crisis, and will be the primary control point for the Physical Threat Alert Level for the sector.

2.2 Cornerstones of the FS-ISAC

The cornerstones of the FS-ISAC are the foundation upon which the member-elected Board of Directors select and manage trusted service providers to enable Financial Services Sector information sharing.

2.2(a) **Submission Anonymity**: Faith that submissions will pose no competitive threat and will be without attribution to the originating member if the submission is submitted anonymously.

2.2(b) **Authenticated Sharing of Information**: The FS-ISAC structure will allow certain information, such as events, incidents, threats, vulnerabilities, resolutions and solutions, to be shared in an authenticated, anonymous and private manner. Recipients of alerts are confident information is from an authorized and vetted source.

2.2(c) **Industry Owned and Operated**: Assurance that the database and input is owned by the Members, submitted to a private sector service provider, and managed by a professional staff and Chief Executive Officer that reports to the FS-ISAC Board of Directors. The FS-ISAC Board of Directors is in turn elected by the Membership.

2.2(d) **No Freedom of Information Act (FOIA) Access:** Control of the portal by the private sector ensures that the FS-ISAC database is not subject to Freedom of Information Act requests from the press or others that are not members of the FS-ISAC.

2.3 FS-ISAC Mission Statement

The FS-ISAC's mission is to help assure the resilience and continuity of the global financial services infrastructure and individual firms against intentional acts that could significantly impact the sector's ability to provide services critical to the orderly functioning of the global economy. This mission is accomplished by disseminating and sharing trusted and timely information to Members. This information increases sector-wide knowledge about physical and cyber security operating risks faced by the sector.

3.0 Participant Eligibility & Enrollment

3.1 FS-ISAC Participant Eligibility

3.1(a) Participants in the FS-ISAC will be limited to:

1. Regulated financial institutions and financial industry associations with a presence in the United States:
   - FDIC insured financial institutions;
   - NCUA federally insured credit unions;
   - FINRA licensed investment and brokerage firms;
   - Securities Investor Protection Corporation (SIPC) member firms;
   - Financial industry utilities such as clearing houses, exchanges, repositories, payment processors, and financial services bureaus/transfer agents, etc.;
   - Specialized United States or state licensed banking companies;
   - State licensed insurance companies;
   - An SEC or state registered investment advisor, investment manager, hedge fund or private equity firm;
   - CFTC registered firms or members of National Futures Association; or,
   - Financial services trade associations;

2. Regulated financial institutions or trade associations that do not have a presence in the United States which meet the following criteria:

   - Must be a regulated bank, credit union, insurance company, broker/dealer, payment processor, exchange, financial services utility, or recognized trade associations if their membership is comprised of financial services firms.
   - Cannot have its head office or have its primary business in a country on the OFAC list.
   - Cannot have its head office or have its primary business in a country that does not have laws targeting cybercrime or does not actively prosecute cyber criminals in their country.
   - Cannot have its head office or its primary business in a country that supports terrorist activities or corporate espionage against the U.S.

   Using the above criteria, the Board can approve specific countries where financial services organizations are headquartered. Other countries can be considered for inclusion on the list of approved countries pending Board approval of each new additional country.

   Any country on the approved list can be deleted if conditions change and the country no longer meets the criteria for membership. If the country is dropped from the approved list, the members from that country may have their membership terminated.

3. IT integrators, IT service providers, and security service providers to the industry which are relied upon by multiple financial institutions for IT or security services.

4. Other entities as may be determined by the Board of Directors of FS-ISAC, Inc. to be eligible for participation, which would be beneficial to the overall health of the financial services sector.

5. The Board, at its discretion, can deny membership to any applicant.

3.1(b) Other Requirements:

1. Participants:
   i. must be able to provide evidence of their good standing with all appropriate regulatory bodies or trade groups recognized by FS-ISAC.
   ii. Adhere to all applicable regulations and laws, including antitrust, privacy, and other relevant laws;
   iii. Adhere to strict standards for professional conduct;
   iv. Remain current with all financial obligations to FS-ISAC;
2. International applicants for membership must have their regulated status by their host country vetted and verified by the FS-ISAC staff.
3. Participants must immediately notify FS-ISAC if their eligibility status changes.
4. The FS-ISAC may conduct periodic member eligibility reviews to assure compliance.
   i. The FS-ISAC will conduct an annual review of the eligibility status of participating Managed Services Providers.

3.1(c) Participant Revocation: The FS-ISAC reserves the right to revoke participation in the FS-ISAC if the participants are found not to be compliant with the eligibility criteria, the Subscriber Agreement, timely payment of fees, or these Operating Rules.

3.1(d) FS-ISAC User Administration reviews the application and verifies the applicant through appropriate regulatory websites or other sources. For institutions or associations that do not have a U.S. presence, User Administration will verify the applicant is not on an OFAC sanctions list. For applications that User Administration cannot verify or if there are questions regarding eligibility, User Administration will contact the CEO for a decision. If User Administration has questions regarding membership level, User Administration will contact FS-ISAC Marketing for a decision.

3.2 Enrollment Process and Procedures

3.2(a) An organization wishing to become a participant in the FS-ISAC may obtain all relevant information including these Operating Rules and the Subscriber Agreement from www.fsisac.com. Subscriber Agreement acceptance and payment of the fees for the applicable

participation level may be made online at www.fsisac.com. Upon selecting the level of service desired the applicant will click on the "Join" button.

3.2(b) Critical Notification Only Participants and Basic and Core Members must use www.fsisac.com to apply for FS-ISAC membership. Applicants may use a credit card or use the self-invoice feature on the website. Standard and above applicants may use the website or a paper process for application or may call the designated contact shown on the website for assistance in the application process.

3.2(c) The FS-ISAC will use trusted third party sources to verify applicant eligibility based on the information provided in Exhibit A of the Subscriber Agreement. The primary Contact and Access Coordinator(s) identification must be completed.

The address for delivery of paper applications—**for Standard and above service levels only**—is:

FS-ISAC, Inc.
Attn: Membership Coordinator
12020 Sunrise Valley Dr
Suite 230
Reston, VA 20191

3.2(d) Upon receipt of a completed application (Subscriber Agreement and payment) and subsequent validation of eligibility by the FS-ISAC, participation will be enabled and notification will be sent.

3.2(e) Members will not be entitled to a refund of any fees.

4.0 Enrollment Material and Activation

4.1 FS-ISAC Activation

4.1(a) The FS-ISAC coordinator will contact the Primary Contact to activate the account once the application has been approved. The Primary Contact will receive the firm's access credentials and, in the case of Standard and above members, tokens.

4.1(b) Firms will have access to the features and benefits for the level of service selected. Detailed features and benefits for each service level may be found at www.fsisac.com under the Join Section.

4.2 User Hardware and Software Requirements

4.2(a) There are no special hardware or software requirements to use the database. A participant must have the capability to access the Internet using commonly supported browsers.

4.4 Portal Access Credentials

4.4(a) Access credentials are issued to the members' Access Coordinators. These are **not anonymous**. They will be allocated to individuals as determined by the participant and are tracked and monitored for use. Once authenticated, the user may submit an incident anonymously or with attribution by checking off the appropriate submission type. These credentials also allow access to the FS-ISAC databases and search engines. **It is the responsibility of the participants' Primary Contact to manage and maintain internal control and the current status of these credentials.**

4.4(b) Processes are established to initially set authentication credentials, reset authenticators, and reissue and invalidate authenticators when requested to by the Primary Coordinator or when suspicious access is attempted.

4.5 Credential Revocation Procedures

4.5(a) The Primary Contact may request replacement credentials from the FS-ISAC Help Desk toll-free at 1-877-612-2622 (prompt 2) or Outside U.S. at: +1 571-252-8517.

4.5(b) ***If a credential is rejected on three separate occasions it will be disabled without notice to the Primary Contact.*** It is the responsibility of the Primary Contact to ensure the FS-ISAC has current contact information for each Access Coordinator.

4.6 Unauthorized Use or Compromise of Credentials

4.6(a) ANY SUSPECTED COMPROMISE OR UNAUTHORIZED USE OF ANY CREDENTIAL MUST BE IMMEDIATELY REPORTED TO FS-ISAC SECURITY OPERATIONS CENTER (877-612-2622 or 571-252-8517 outside USA).

4.7 Failed Access Credentials

4.7(a) If any credentials become inoperative, the FS-ISAC User Administration (877-612-2622 or 571-252-8517 outside USA or admin@fsisac.com) must be contacted for instructions on how to receive a replacement and procedures for the return of the failed access credential(s) to the FS-ISAC operator.

4.8 Terminating Relationship

4.8(a) Upon termination of the Subscriber Agreement for any reason, access credentials to the FS-ISAC portal will be terminated.

5.0 Operations

5.1 Overview

5.1(a) The FS-ISAC has established a business relationship with a Service Provider to deliver the FS-ISAC portal services to the members and participants. The FS-ISAC and the service provider have a formal Service Level Agreement for the various services. Members may contact the FS-ISAC staff for details.

5.1(b) The FS-ISAC services, as determined by service level, and general overview of the operations follows:

1. The intent of the FS-ISAC is to:

- Utilize the sectors' vast resources (people, process, and technology) to aid the entire sector with situational awareness and advance warning of new physical and cyber security threats, incidents and challenges.

- Have an infrastructure that enables anonymity, if desired, and information dissemination and sharing via member and other trusted source submissions to the ISAC.

- Have a secure means to disseminate information when noteworthy events occur and as they evolve.

- Provide 24x7x365 service via a team of financial services industry analysts and security professionals within the FS-ISAC (the "Analysis Team") conducting research or intelligence gathering to alert the members of evolving or existing threats, incidents and vulnerabilities, support the development of content that is posted to the FS-ISAC database, advise on mitigation steps or best practices.

2. Members at all service levels have the capability to voluntarily and anonymously submit information to the database, which will be authenticated by the system as a submission from a current authorized participant. When a member chooses to submit information anonymously no one will know who submitted the information. FS-ISAC members will only know an authorized and vetted member submitted the data.

3. Information in the database will be available via secure, encrypted web-based connections only to currently authorized members at the appropriate service level. A team of analysts and security professionals within the FS-ISAC (the "Analysis Team") will assess each submission regarding the seriousness of the threat, vulnerability or attack and to identify patterns. When appropriate, end users will be notified, by electronic page, e-mail or other member designated alert-mechanism that an Urgent or Crisis situation exists and will be advised how to obtain additional information. A user profile will allow filtering of notifications for Basic

and above members to receive advisement only when a relevant issue arises. The profile is user driven and is used to ensure only meaningful alerts are delivered. In many cases, a Crisis Conference call will be initiated within a short time for Basic and above members when a Crisis Alert is issued.

5.1(c) Information Dissemination Categories: Information to be disseminated will generally fall into categories as defined in Section 5 of these Operating Rules and may be disseminated to pre-defined groups of users with special interests, for example payment processors, business continuity staff, etc.

5.1(d) Information Sources: Information will be contributed by members submitting anonymously or with attribution. Other sources, to be monitored by the FS-ISAC analysis team, will include: commercial firms, federal, state, or local government and law enforcement agencies, technology providers, security providers and other reliable sources.

5.1(e) Information Analysis: Submitted or obtained incident information will be analyzed by financial services sector experts to determine technical validity, indications of a broader problem, trends, etc. and results will be disseminated to participants via the FS-ISAC.

5.1(f) User Updates: Members may be requested to update resolutions or solutions to previously identified incidents or vulnerabilities based on the tracking number which is used to identify the event—not the user firm submitting the data. This information is available via the Lookup Database.

5.1(g) Sanitizing of Submitted Information: Participants are solely responsible for ensuring that submissions intended to be anonymous are submitted without identifying information. However, all incident information submitted to the FS-ISAC undergoes a two-step sanitization process to make best efforts to assure there is no reference to a specific company. The first step is an automated process of keyword search and removal. The second step is a manual review of the submitted information by the FS-ISAC analysis team.

5.2 Submission of Information to the FS-ISAC

5.2(a) The goal of the FS-ISAC is to permit members to voluntarily share information about physical and cyber incidents, threats, vulnerabilities, resolutions, and solutions. Submitting this information will allow the FS-ISAC to determine if this report is potentially harmful to the sector or potentially part of a larger event occurring across the infrastructure.

5.2(b) Through the collaborative sharing of this information and when combined with solutions/resolutions to such threats, incidents or vulnerabilities, the entities in the banking and finance sector are all better prepared to protect their individual infrastructures. This sharing of information is expected to be very beneficial for preparedness, protection, and crisis management.

5.2(c) The following definitions are offered as guidance to participants for categorizing and classifying information being considered for submission:

1. Incidents:

- Physical or cyber security breaches or incidents experienced of a new evolving nature, or ones that clearly go beyond daily norms or appear to have broader consequences, or correlate to incidents reported by others or correlate to specific threat information received.
- Physical or cyber security breaches or incidents which are having a significant impact on operations (e.g. Denial of Service attacks, attacks on integrity, bomb threats) or are of a recurring or persistent and insidious nature.
- Security breaches or incidents related to criminal activities (e.g. fraud or extortion or espionage).
- Once analyzed, these incidents will be made available in the FS-ISAC database. Incidents will be classified as to the nature of their severity.

2. Threats:

- Specific physical or cyber threats to any component or entity in the sector – Knowledge uncovered of threats against other sectors or entities.
- Any cyber or physical extortion threats.
- Details of "hacker" or "nation state" or "criminal" information, which pose a threat to our infrastructure or systems
- Threat information or indicators received from other credible sources.

3. Vulnerabilities:

- Items reported by organizations such as US-CERT, FIRST, DHS, etc., by another ISAC, or vendor security bulletins considered to be of operational importance to the general banking and finance infrastructure because of its architecture, operational procedures, or knowledge of historical exploitation of vulnerabilities of similar nature.
- Reports of and/or validation of vulnerability hoaxes being perpetrated.
- Operational vulnerabilities experienced with various vendor or service providers, which could impact the sector broadly (e.g. cryptographic exploits, authentication technology exploits).
- Results of the investigation of vulnerabilities or the validation of specific vulnerabilities within systems.

4. Resolutions/Solutions:

- The goal of participants providing Resolutions/Solutions is to help other organizations deal with similar incidents. Resolutions to specific incidents will be posted to the FS-ISAC database. Participants are requested to submit and update resolutions of incidents they report; these postings may be done anonymously. Submitted resolutions will not be checked for technical

accuracy by the FS-ISAC analysis team. Resolutions can be a single activity such as apprehension of an individual causing the incident or a combination of events such as implementation of new processes or controls or reconfiguration of key equipment.

- Participants should provide any practical knowledge uncovered when working to address specific vulnerabilities or threats that have a broader application to the sector (e.g. effectiveness of various methods or practices for dealing with e-mail borne virus or trojan horse programs). These can be categorized into two categories: technical solutions or process/business solutions.

5.3 Government/Law Enforcement Information, Via NCCIC Liaison

5.3(a) Information may be accepted and authenticated as coming from the U.S. or other governments, government agencies, state or local governments, or law enforcement agencies regarding incidents, threats, and vulnerabilities.

5.3(b) The FS-ISAC provides data on specific events or incidents to appropriate government and law enforcement agencies, and private sector partners such as other ISACS, when there is potential benefit to the financial sector and only with the consent of the member providing the information. Information is shared without attribution to the incident originator. It can help to provide an overall, general threat landscape of the financial sector to government and private-sector partners.

5.4 Member Submission Modes

5.4(a) Attributable: Members may submit attributable information by using the attributable submission option on the database, or sending to e-mail address iat@FSISAC.com, fax (877-612-2822 or telephone 877-612-2622 or +1 571-252-8517 outside USA). Attributable communications will be authenticated by the access coordinator's password.

5.4(b) Anonymous:

Web – Members may submit information anonymously by using the anonymous submission form on the portal. A user will log into the FS-ISAC portal and will complete the reporting page and submit it for analysis.

E-Mail – Using anonymous credentials, an e-mail of the data may be sent to the FS-ISAC e-mail address iat@FSISAC.com.

5.5 Criticality Classification of Advisories

5.5(a) Advisories issued by the FS-ISAC will be assigned a Severity, Urgency and Credibility score, each of which will be measured on a 1-5 scale. In addition, Threat and Vulnerability advisories are assigned a Risk score, which will be based on the Severity, Urgency, and Credibility scores.

5.5(b) Severity. Severity is scored on the following scale:

1. Informational
2. Minimal Impact
3. Moderate Impact
4. Significant Impact
5. Major business disruption

The following criteria are used to determine the Severity:

- What's the impact for a financial services firm?
- How widespread is the impact to the financial services sector likely to be?
- Is there exploit code/POC, Metasploit
- Is the affected product widely used in the FS sector?
- CVSS Score
- The type of vulnerability (DoS, XSS, Security Bypass, Remote Code Execution, etc)

5.5(c) Urgency. Urgency is scored on the following scale:

1. Informational
2. Action recommended
3. Action highly recommended
4. Take action asap
5. Take immediate action

The following criteria are used to determine the Urgency:

- How soon are we anticipating impact?
- Is there recommended action?
- Are there existing patches/mitigation?
- What is the impact if action is not taken?

5.5(d) Credibility. Credibility is scored on the following scale:

1. Unknown
2. Suspect
3. Single Source
4. Multiple Sources
5. Verified

The following criteria are used to determine the Credibility:

- Is the information available through multiple, independent sources?
- Are there multiple, conflicting reports?
- Has the vendor acknowledged the issue?

5.5(e) Risk. Risk is scored on the following scale:

1-7: Normal

8-9: Urgent
10: Crisis

Risk reflects the overall risk presented to the financial sector. Typically, Risk= Severity + Urgency. Risk may be downgraded based on low Credibility.

5.6 Traffic Light Protocol

5.6(a) All information submitted, processed, stored, archived, or disposed of will be classified and handled in accordance with its classification.

5.6(b) Information will be classified using the *Traffic Light Protocol (TLP), d*efined as:

Color	When should it be used?	How may it be shared?
RED	Sources may use TLP RED when the information's audience must be tightly controlled, because misuse of the information could lead to impacts on a party's privacy, reputation, or operations. The source must specify a target audience to which distribution is restricted.	Recipients may not share TLP RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use TLP AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP AMBER information with staff in their own organization who need to know, or with service providers to mitigate risks to the member's organization if the providers are contractually obligated to protect the confidentiality of the information. TLP AMBER information can be shared with those parties specified above only as widely as necessary to act on the information.
GREEN	Sources may use TLP GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community.	Recipients may share TLP GREEN information with peers, trusted government and critical infrastructure partner organizations, and service providers with whom they have a contractual relationship, who have a need-to-know but not via publicly accessible channels.
WHITE	Sources may use TLP WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	TLP WHITE information may be distributed without restriction, subject to copyright controls.

5.6(c) If no marking is specified, the information shall be treated as FS-ISAC Confidential Information (TLP: Amber).

5.6(d) Information classified as Green, Yellow, or Red must be disclosed, transported, stored, transmitted, and disposed of in a safe and secure manner using controls appropriate to the level

of classification. These controls include, but are not limited to, encryption, shredding, securely erasing, and degaussing of media.

5.7 Alert Subject Line Formats

5.7(a) To facilitate the automated parsing and forwarding of FS-ISAC alerts, the email "Subject" line in FS-ISAC alerts sent to the membership uses the following format**:**
[Alert_Type][Criticality]: [Alert_Title]

5.7(b) The ***Alert_Type*** is a 3-letter abbreviation for the alert type, as follows:

- Announcements: **ANC**
- Cyber Vulnerabilities: **CYV**
- Cyber Threats: **CYT**
- Cyber Incidents: **CYI**
- Collective Intelligence: **COI**
- Physical Threats: **PHT**
- Physical Incidents: **PHI**
- CISCP Reports: **CIS**

5.7(c) The ***Criticality*** is the "criticality" value for the corresponding alert type (for Collective Intelligence, no criticality value will be included). The Exact format of the Criticality field for each Alert Type is as follows:

- Announcements: Priority is a number, 1-10. 8-10 is high priority.
- Cyber Vulnerabilities: Risk is a number, 1-10. 8-9 is Urgent, 10 is Crisis.
- Cyber Threats: Risk is a number, 1-10. 8-9 is Urgent, 10 is Crisis.
- Cyber Incidents: Severity is a number followed by a description, as follows:
  - 1- Informational
  - 2- Minimal Impact
  - 3- Moderate Impact
  - 4- Significant Impact
  - 5- Major Business Disruption

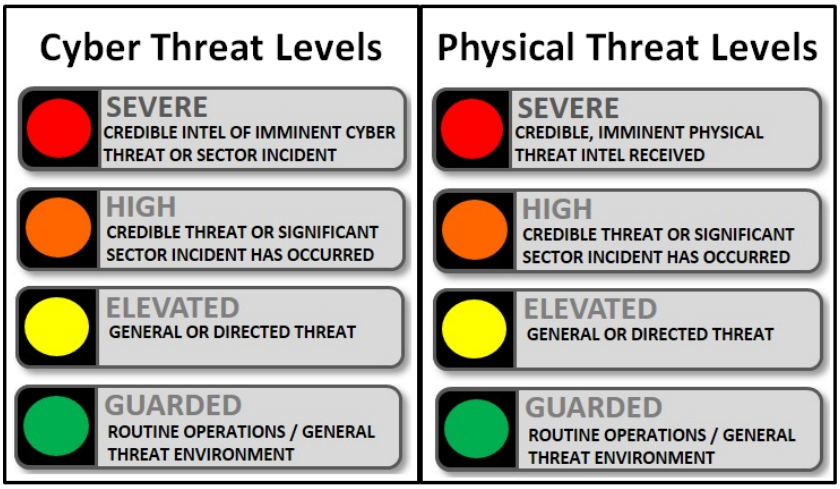
- Collective Intelligence: There is no Criticality metric for Collective Intelligence. This will be blank (no value).
- Physical Threats: Risk is a number, 1-10. 8-9 is Urgent, 10 is Crisis.
- Physical Incidents: Severity is a number followed by a description, as follows:
  - 1 - Informational
  - 2 - Minimal Impact
  - 3 - Moderate Impact
  - 4 - Significant Impact
  - 5 - Major Business Disruption

5.7(d) The ***Alert Title*** is the contents of the "Title" field in the alert.

5.8 Security Threat Level

5.8(a) The FS-ISAC will maintain a "Financial Services Sector Cyber Threat Advisory" and a "Financial Services Sector Physical Threat Advisory" to indicate the degree of threat to the sector.

5.8(b) Threat to the sector will be rated against the scale:



5.8(c) The FS-ISAC portal will indicate the threat levels at all times.

5.8(d) The Cyber Threat Level will be reviewed during the biweekly "Threat Intel" call, with input from the Threat Intelligence Committee. The Threat Intelligence Committee (TIC) can also convene a call to review and set the threat level outside of the normal bi-weekly protocol if the situation warrants. The FS-ISAC Service Provider will adjust the website to reflect any decisions made during the weekly call to change the level.

5.8(e) The Physical Threat Level will be maintained in conjunction with procedures to be established by the Business Resilience Committee.

5.9 Crisis Management Calls

5.9(a) If a cyber or physical emergency occurs, the FS-ISAC Threat Intelligence Committee or the Business Resilience Committee, respectively, will meet and determine if there is need for an emergency call. On the call, Members will receive a current status and, where practical, be able to converse with the appropriate vendor, government agencies, and Members to answer questions and discuss solutions/next steps.

5.9(b) Crisis calls will be held to determine the status, countermeasures, and response information related to ongoing security breaches or incidents being coordinated across the sector.

5.9(c) Crisis conference calls will continue on a cycle determined by the respective Committee Chair and the FS-ISAC ALL-HAZARDS CRISIS RESPONSE Playbook until the Crisis is resolved.

5.9(d) Crisis coordination, escalation, and risk mitigation will continue in accordance with the FS-ISAC ALL-HAZARDS CRISIS RESPONSE Playbook until the Crisis is resolved.

6.0 Analysis and Retrieval of Database Information

6.1 Analysis

6.1(a) The FS-ISAC analysis team will review all information submitted to the FS-ISAC 24 hours a day 7 days a week. Based on the analysis, the FS-ISAC may determine a "Crisis" notification should be made to the members. This means an incident may be upgraded or downgraded based on other factors determined by the analyst.

6.1(b) Data arriving at the FS-ISAC undergoes an authentication process to ensure it came from an authorized member. Anonymous submissions are reviewed and sanitized of any information that may have mistakenly been included that could allow it to be attributed to a specific member. The FS-ISAC analysis team will exercise best efforts but are not responsible if a member fails to remove all identifying information. Upon completion of the review process, the data will be posted to the FS-ISAC database within the timeframes established for each classification.

6.1c) Data may be provided by members during discussions that may take place in committees, for example the Threat Intelligence Committee, and special interest groups supported by list servers maintained by the Security Operations Center. The FS-ISAC analysis team will monitor these discussions and will categorize and post the results of the discussions, in accordance with the established information classification and handling rules, to the FS-ISAC database.

6.1(d) Upon completion of a submission, the FS-ISAC will automatically assign a tracking number. **This number is unique to the incident and is not associated with the submitting member.** The FS-ISAC will post to the portal the "tracking number" so that the submitter has positive acknowledgement the submission has been posted. The FS-ISAC may also identify by "tracking number" on the portal a specific submission with any problems or missing information. The responsible submitter should correct and resubmit the information.

6.1(e) Participants will be notified of **"Crisis"** and **"Urgent" Alert Notification** information through the alert-mechanism(s) specified by each Member access coordinator (i.e., by pager, e-mail, cell phone) or as defined by the level of service.

6.2 Retrieving "Crisis" and "Urgent" Alert Information

6.2(a) Members receiving "Crisis" or "Urgent" alert notifications must access the FS-ISAC portal for specific information relating to these notifications using their **Access Credentials** to log into the portal and authenticate themselves. CNOP Subscribers will receive "Crisis" or "Urgent" alerts via a mail list. Members may not use anonymous credentials to retrieve information.

6.3 Retrieval of Information and Searching the FS-ISAC Database

6.3(a) Standard and above members may regularly search and retrieve information from the FS-ISAC database by using their **Access Credentials** to log into the FS-ISAC portal and authenticate themselves.

7.0 FS-ISAC System Security Monitoring

7.1 Monitoring and Testing

7.1(a) The FS-ISAC systems are actively monitored 24 hours a day, 7 days a week. The FS-ISAC operator will use reasonable efforts to notify participants of the status of the system through the alert-mechanism specified by each participant access coordinator (i.e., by pager, e-mail, digital cell phone).

7.1(b) The FS-ISAC will use a third party on at least an annual basis to complete a formal, documented penetration test of the web portal. Results of this test will be delivered to the FS-ISAC Board of Directors and be available to members on a request basis.

8.0 Help Desk Policy and Procedures

8.1 User Support Procedures

8.1(a) CNOP, Basic Participants and Core Members must contact the FS-ISAC via email for Help Desk activities at admin@FSISAC.com.

8.2(b) Standard and above members may contact Help Desk personnel to assist with any FS-ISAC problems by calling 877-612-2622, or +1 571-252-8517 outside USA. Alternatively, Standard and above members may send an e-mail to admin@FSISAC.com.

9.0 Antitrust/Competition Provisions

9.1 Policy

9.1(a) The FS-ISAC, Inc., its Board of Directors, and its Members will comply with all laws and regulations governing antitrust and anticompetitive practices. FS-ISAC officers, directors, staff, and members must not engage in any conduct that may constitute violation of these laws, including but not limited to price fixing, group boycotts, or allocations of markets among organizations or institutions.

9.1(b) To assure compliance with this policy:

1. FS-ISAC Members are prohibited from discussing any company-specific, competitively sensitive information, including terms, sales, conditions, pricing, or future plans, related to their firms or other firms, including vendors or service providers they engage;
2. The FS-ISAC portal and its forums are not to serve as a conduit for discussions or negotiations between or among vendors, manufacturers or security service providers with respect to any participant or group of participants;
3. Neither the FS-ISAC staff, officers, and directors nor its Members, committees, and committee chairs are to recommend in any FS-ISAC-sponsored exchange or forum in favor of or against the coordinated boycott or adoption of any company or product or service of particular manufacturers or vendors;
4. Each FS-ISAC Member will determine the effect of the exchanged information on its individual purchasing and related decisions;
5. Any breach of these guidelines will be reviewed by the Board of Directors of the FS-ISAC and may result in termination of the organization's FS-ISAC membership and forfeiture of remaining annual membership fees.
6. Committee chairs, directors or staff will designate a responsible party to publish and disseminate minutes of Board committee and association meetings.

9.2 Vendor Discussion Policy

In addition to modifying the antitrust provisions, the Board established a policy that permits the sharing of positive or negative views concerning products, services, or vendors. However, such sharing must be professional and courteous. The vendor community is vital to the mission of the association, as well as often being a direct and valuable supporter of the FS-ISAC.

While information should flow freely, those sharing such views should be mindful of appropriate etiquette and focus on providing factual information. Tone and the sheer number of comments should be taken into account.

10.0 Code of Conduct for Officers and Directors

10.1 Code of Conduct

10.1(a) A Code of Conduct will apply to FS-ISAC directors and officers to provide guidance to help them recognize and deal with ethical issues; provide mechanisms to report unethical conduct; and to help foster a culture of honesty and accountability.

10.2 Obligations under the Code of Conduct

10.2(a) Directors and officers are responsible for the stewardship of FS-ISAC, assuring that it continues to have the critical capabilities needed to achieve its objectives.

10.2(b) Directors and officers have fiduciary duties to FS-ISAC, including the duties of care, obedience, and loyalty, and are obligated as a matter of corporate law to act in good faith to promote the best interests of FS-ISAC, including undivided loyalty to FS-ISAC. Directors and officers under this Code are obligated to:

1. Act honestly, in good faith and in the best interests of FS-ISAC, including but not limited to furthering the FS-ISAC mission and activities above those of other companies or organizations;
2. Follow guidelines established by the Board regarding how it will govern and conduct itself;
3. Refrain from speaking as an individual on behalf of the Board unless authorized to do so;
4. Appropriately avoid actual or apparent conflicts of interest.

10.2(c) Directors and officers are obligated to treat as confidential discussions at Board or committee meetings, including expressions of opinion and discussions. Board and committee decisions should be kept confidential until publicly disclosed by FS-ISAC. Confidentiality extends to, but is not limited to, all disclosures of trade secrets, proprietary know-how, financial information or other confidential information made to any director of officer.

10.3 Code of Conduct Compliance

10.3(a) The Chair of the Board should immediately be notified of any legal process from third parties calling for disclosure of any information received by a director in his or her role as a director or committee member.

10.3(b) Directors and officers must communicate any suspected violations of the Code promptly to the Chair of the Board. Suspected violations will be investigated by the Board or by a person or persons designated by the Board, and appropriate action will be taken in the event of any violations of this Code.

11.0 Confidentiality

11.1 Confidentiality Requirement

11.1(a) Directors, officers, staff and members may have access to or receive from the FS-ISAC, its members, or affiliated partners certain trade secrets and other information pertaining to the disclosing party or its employees, customers and suppliers.

1.1(b) Confidential information may be disclosed by an FS-ISAC alert or notification. Confidential information may also be disclosed at member meetings, committee meetings, and meetings held by various working groups of the FS-ISAC that may be constituted.

11.1(c) Directors, officers, staff and members agree that all such Confidential information obtained shall be considered confidential and proprietary to the disclosing party.

11.1(d) As stipulated in Section 5.5, Traffic Light Protocol, all information is classified as Confidential (Amber) by default unless specifically classified otherwise.

11.1(e) Staff and contractors are required to execute a confidentiality agreement as a condition of employment. Members, including directors and officers, are bound by the terms of the Subscriber Agreement.

11.1(f) Parties in possession of Confidential Information may be requested to disclose Confidential Information to law enforcement, a government authority or other third party, pursuant to subpoena or other legal order. To the extent allowed by law, the disclosing party will use reasonable and customary efforts to provide FS-ISAC with advance notice of such disclosure to allow FS-ISAC and impacted parties to seek an appropriate protective order or other relief to prohibit or limit such disclosure.

11.2 Confidentiality Agreement

11.2(a) Recipients of Confidential Information will be obligated to:

1. Protect and preserve the confidential and proprietary nature of all Confidential Information;

2. Not disclose, give, sell or otherwise transfer or make available, directly or indirectly, any Confidential Information to any third party for any purpose, except as expressly permitted in writing by the FS-ISAC and the disclosing party;

3. Not use, or make any records or copies of, the Confidential Information, except as needed in order to provide specific services in the conduct of their duties, or as required

by law or regulations, or as needed to use the information effectively to mitigate risk in their respective organizations;

4. Limit the dissemination of the Confidential Information to those with the need to know the Confidential Information, provided that such individuals are obligated to maintain the confidential and proprietary nature of the Confidential Information;

5. Return all Confidential Information and any copies thereof as soon as it is no longer needed or immediately upon the disclosing party's request, to the extent permitted by law and regulatory retention requirements;

6. Notify the FS-ISAC immediately of any loss or misplacement of Confidential Information, and

7. Comply with any reasonable security procedures designated in the Confidentiality Agreement as may be prescribed by the FS-ISAC for protection of the Confidential Information.

12.0 Soltra Membership Service*

12.1 Scope Of Section

12.1(a) FS-ISAC and Soltra have agreed that, to facilitate deployment of the Soltra Offerings to FS-ISAC members, FS-ISAC is authorized to act as a Sponsoring Organization for Soltra.

12.1(b) As a Sponsoring Organization for Soltra, FS-ISAC makes available Soltra Membership as an optional service to FS-ISAC members.

12.1(c) This Section applies to those FS-ISAC members who have opted to become Soltra Members through FS-ISAC, as a Sponsoring Organization for Soltra, and have been approved by Soltra for Soltra Membership.

12.2 Application of Soltra Operating Rules

12.2(a) Soltra Membership is governed by the Soltra Operating Rules, as amended by Soltra from time to time (the "Soltra Operating Rules").

12.2(b) A FS-ISAC member who has received notice from FS-ISAC that it has been approved for Soltra Membership, as of the date of such notice, shall be a Soltra Member, shall be deemed to have agreed to the Soltra Operating Rules, and shall be subject to and bound by the Soltra Operating Rules as if such FS-ISAC member had entered into an agreement directly with Soltra for Soltra Membership.

12.2(c) In the event of a conflict between the Soltra Operating Rules and the FS-ISAC Operating Rules involving the Soltra Offerings, such conflict shall be governed by the Soltra Operating Rules. In the event of a conflict between the Soltra Operating Rules and the FS-ISAC Operating Rules not involving the Soltra Offerings, such conflict shall be governed by the FS-ISAC Operating Rules.

12.2(d) The current version of the Soltra Operating Rules can be found at www.soltra.com/memberapp.

12.3 Invoices

12.3(a) FS-ISAC shall invoice the FS-ISAC member for the Soltra fee associated with the member's Soltra Membership.

12.3(b) The FS-ISAC member shall remit payment to FS-ISAC in accordance with the terms and conditions specified on such invoice.

12.4 Access To FS-ISAC Content

12.4(a) Only FS-ISAC members are permitted to access FS-ISAC content, for example the Cyber Threat Repository, and can do so via any of the Soltra Offerings.

12.5 Definitions

12.5(a) For purposes of this Section, the terms "Soltra", "Soltra Offerings", "Sponsoring Organization", "Soltra Member" and "Soltra Membership" shall have the meanings ascribed to such terms in the Soltra Operating Rules.

*The FS-ISAC's Soltra Membership Service is an optional service offered by FS-ISAC to FS-ISAC members which enables FS-ISAC members to become Soltra Members through FS-ISAC (that is, without executing a Soltra Membership agreement directly with Soltra). The FS-ISAC's Soltra Membership Service is available only to FS-ISAC members.

13.0 Rules Modification and Precedence

13.1 Modification of Rules Approvals

13.1(a) From time to time these Operating Rules and the Subscription Agreement may be modified with the approval of the Board of Directors. E-mail notifications to current participants will be provided at that time. All changes will be highlighted and/or annotated for applicability.