Operating Rules

1.0 FS-ISAC History and Background

1.1 FS-ISAC (Financial Services Information Sharing & Analysis Center

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 affect 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 (FS-ISAC).** *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.* 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, FS-ISAC has experienced exponential growth in its membership and in the quantity, quality and value of the information shared. FS-ISAC has established formal information sharing programs with various government agencies.

Cross-sector information exchange has also been formalized and integrated into the operating procedures of FS-ISAC. FS-ISAC and its members also partner with and collaborate on multiple information sharing initiatives and exercises within the sector and with other sectors.

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) FS-ISAC portal, database and information sharing tools are located in a secure facility. 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 FS-ISAC, Inc. and CNOP participants within the financial services sector

2.1(b) Terminology and Definitions:

- Eligible firms may register as a Critical Notification Only Participant (CNOP) or subscribe as a fee paying member of FS-ISAC. Fee paying members have access to 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 FS-ISAC Portal, and are not considered Members. The CNOP category was created to enable FS-ISAC to reach as many financial institutions as possible within the financial services sector during a major physical or cyber crisis or threat.*

- *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 FS-ISAC Board that its employees, agents and consultants who use FS-ISAC will comply with the Operating Rules of 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 FS-ISAC.
- *Access Coordinators* are those employees, agents and contractors identified by the Primary Contact as authorized to have FS-ISAC credentials.
- *Member Proprietary Information* means any information in any form voluntarily provided by the Participant to FS-ISAC under these Operating Rules. FS-ISAC will handle the information in accordance with these Operating Rules.
- *FS-ISAC, Inc. Proprietary Information* means (i) any information in any form provided by FS-ISAC to participants under these Operating Rules; and, (ii) any intellectual property defined and identified as such.
- *Operator Proprietary Information* means all specifications, computer programs, upgrades, processes, know-how, and other intellectual property embedded in FS-ISAC, except as defined and documented as belonging to FS-ISAC, Inc.
- The term *FS-ISAC website* or *website* means the public facing Internet website at www.fsisac.com.
- *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 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 FS-ISAC agree to abide by the Subscriber Agreement and 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 FS-ISAC Board of Directors and is published on fs-isac website.

- *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.
- *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.
- *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.
- *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.
- *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.

- *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.
- *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.
- *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 FS-ISAC website at fsisac.com.

2.1(g) 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 FS-ISAC

The cornerstones of 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**: 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 FS-ISAC Board of Directors. 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 FS-ISAC database is not subject to Freedom of Information Act requests from the press or others that are not members of FS-ISAC.

2.3 FS-ISAC Mission Statement

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 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 US

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.ITintegrators, 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. 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 FS-ISAC staff.
3.Participants must immediately notify FS-ISAC if their eligibility status changes.
4.FS-ISAC may conduct periodic member eligibility reviews to assure compliance.
FS-ISAC will conduct an annual review of the eligibility status of participating Managed Services Providers.

3.1(c) Participant Revocation: FS-ISAC reserves the right to revoke participation in 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 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) 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 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

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, and processors.

4.1(a) 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.

4.4 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 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 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 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, 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 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) FS-ISAC has established a business relationship with a Service Provider to deliver FS-ISAC portal services to the members and participants. FS-ISAC and the service provider have a formal Service Level Agreement for the various services. Members may contact FS-ISAC staff for details.
5.1(b) FS-ISAC services, as determined by service level, and a general overview of the operations follows:

1. The intent of 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 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 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 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 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 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 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 FS-ISAC analysis team.

5.2 Submission of Information to FS-ISAC

5.2(a) The goal of 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 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 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 FS-ISAC database. Participants are requested to submit an update resolution of incidents they report; these postings may be done anonymously. Submitted resolutions will not be checked for technical accuracy by 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

5.3Government/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) 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 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 FS-ISAC e-mail address iat@FSISAC.com.
Any efforts to re-identify the identity of a submitter of an anonymous submission is prohibited, unless required by law or to prevent fraud.

5.5 Criticality Classification of Advisories

5.5(a) Advisories issued by 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 an impact?
- Is there a 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:

Color	When should it be used?	How may it be shared?
RED	Sources may use FS-ISAC 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 FS-ISAC RED information with any parties outside of the original recipients.
AMBER	Sources may use FS-ISAC 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 FS-ISAC AMBER information with other FS-ISAC Members, 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. FS-ISAC AMBER information can be shared with those parties specified above only as widely as necessary to act on the information.
GREEN	Sources may use FS-ISAC GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community.	Recipients may share FS-ISAC GREEN information with peers, trusted government and critical infrastructure partner organizations, and service providers with whom they have a contractual relationship, but not via publicly accessible channels.
WHITE	Sources may use FS-ISAC WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	FS-ISAC WHITE information may be distributed without restriction, subject to copyright controls.

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, d*efined as:
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:

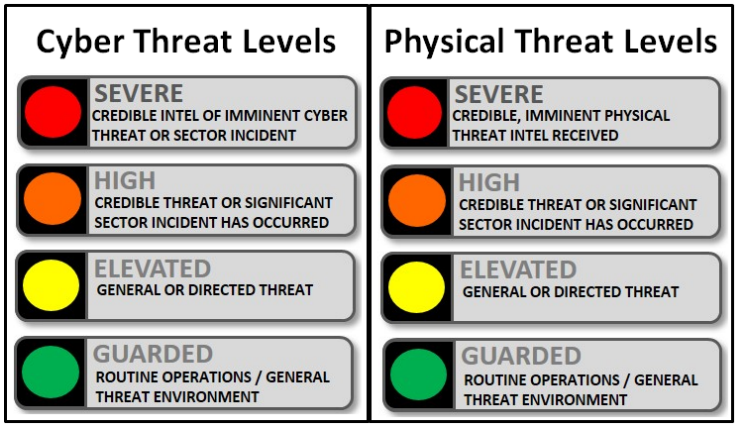
- Announcements: Priority is a number, 1-10. 8-10 is high priority.
- Cyber Vulnerabilities: Risk is a number, 1-10. 8-9 is Urgent, 10 is Crisis.
- Cyber Threats: Risk is a number, 1-10. 8-9 is Urgent, 10 is Crisis.
- Cyber Incidents: Severity is a number followed by a description, as follows:
  1. Informational
  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) 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) 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. 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, 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 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 FS-ISAC ALL-HAZARDS CRISIS RESPONSE Playbook until the Crisis is resolved.
5.9(e) Each Member shall make available to FS-ISAC the contact information of a person designated by that Member to handle or receive information concerning Crisis Management matters

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.
(c) 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 e-mail or 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 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 e-mail or 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:

i. 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;
ii. 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;
iii. 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;

iv. Each FS-ISAC Member will determine the effect of the exchanged information on its individual purchasing and related decisions;
v. 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.
vi. 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 Personal Data Protection

12.1 Members as Data Controllers; FS-ISAC as Data Processor

12.1(a) Section 12 applies to personal data shared between Members in the context of threat intelligence sharing only, whether shared both through the Portal and via FS-ISAC's email systems, ("**Threat Personal Data**").
12.1(b) Threat Personal Data may be subject to Data Protection Laws, including GDPR. The Threat Personal Data is shared by the Members through FS-ISAC in a manner that allows each Member and FS-ISAC a degree of control over the purpose of the sharing of information and the means of such processing by FS-ISAC and the Members engaged in information sharing. When processing Threat Personal Data, each of its Members shall be acting in the capacity as a data controller. When processing Threat Personal Data on behalf of the Members in accordance with these Operating Rules, FS-ISAC shall act in the capacity as a processor for the purposes of Data Protection Laws. However, FS-ISAC and the Members acknowledge that FS-ISAC will, in addition, act in its own capacity as a controller when processing Threat Personal Data for its own purposes.
12.1(c) The Members and FS-ISAC hereby agree and acknowledge that: (i) the processing of Threat Personal Data is necessary for their respective legitimate interests in protecting and securing their networks and information systems, particularly from unlawful or malicious actions, and to preserve the security of the banking and financial services offered by Members to their customers; (ii) in assessing such legitimate interests, the Members and FS-ISAC have taken account of Recital 49 of GDPR and consider that the sharing of Threat Personal Data is strictly necessary and proportionate for the purposes of achieving and maintaining the security of Members' networks and systems; and (iii) the Members and FS-ISAC consider that their respective legitimate interests as described in this Section 13.1(c), and the legitimate interests of relevant third parties, provide a lawful basis for them to process Threat Personal Data, to the extent this is required by Data Protection Laws.

12.1(d) To the fullest extent permissible by applicable law, each Member and FS-ISAC (when acting as a controller), as applicable, shall be responsible for responding to enquiries from, or providing required notifications to, Data Subjects. However, each Member shall reasonably assist and cooperate with FS-ISAC and the other Members to the extent reasonably necessary to help FS-ISAC's or any Members meet its obligations hereunder.
12.1(e) Where applicable, the data exporter shall notify in writing the data importer of any registration by the data exporter with any data protection or supervisory authority.
12.1(f) Subject to the requirements of this Section 13, each Member shall comply with all Data Protection Laws applicable to its sharing and use of Threat Personal Data. Each Member acknowledges that FS-ISAC will share Threat Personal Data with third parties (including government organizations and other ISACs) as it deems necessary and / or appropriate.

12.1(g) Each Member shall, taking into account the nature of the Threat Personal Data being processed, implement appropriate technical and organizational measures (including, without limitation, the secure encryption of Threat Personal Data) to ensure that Threat Personal Data is processed securely in accordance with the requirements of Data Protection Laws and these Operating Rules.
12.1(h) A Member shall hold harmless and defend FS-ISAC against any claims or actions made or brought against FS-ISAC by a third party, whether a private or government entity, and shall indemnify FS-ISAC for any damages or liability (including reasonable attorney's fees and costs of compliance with any orders), in each case solely to the extent arising out of (i) any breach by the Member of its obligations under Section 12 of these Operating Rules, including the applicable obligations under the Standard Contractual Clauses, (ii) such Member's violation of any applicable Data Protection Laws relating to its interactions with FS-ISAC, or (iii) a Personal Data Breach involving a Member relating to its interactions with FS-ISAC and which was not caused by FS-ISAC's breach of its obligations under Section 12 of these Operating Rules, including the applicable obligations under the Standard Contractual Clauses or FS-ISAC's violation of any applicable Data Protection Laws.
12.1(i) Each Member shall designate an appropriate contact person in connection with personal data protection matters and make that person's contact information available to FS-ISAC, and shall procure that each such contact person will reasonably cooperate in good faith with FS-ISAC and other Members in relation to the provisions of Section 13 of these Operating Rules.
12.1(j) Each Member warrants and represents that it has the authority to provide, and shall provide, contact information for such Member to be included in FS-ISAC's Member directory.

12.2 FS-ISAC Processing Threat Personal Data on Behalf of Members

12.2(a) To the extent FS-ISAC processes any Threat Personal Data as processor for a Member, FS- ISAC shall:

a. process such Threat Personal Data (i) only in accordance with the Members written instructions from time to time (including those set out in these Operating Rules or other agreement between the Member and FS-ISAC), unless it is otherwise required by applicable law (in which case, unless such law prohibits such notification on important grounds of public interest, FS-ISAC shall notify the Member of the relevant legal requirement before processing the Threat Personal Data), and (ii) only for the duration specified in these Operating Rules;
b. ensure that those of its personnel who have access to such Threat Personal Data are committed to binding obligations of confidentiality when processing such Threat Personal Data;
c. taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing) implement and maintain technical and organizational measures and procedures to ensure an appropriate level of security for such Threat Personal Data, including protecting such Threat Personal Data against the risks of accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, dissemination or access;
d. inform the Member without undue delay upon becoming aware of such Threat Personal Data (while within FS-ISAC's or its subcontractors' possession or control) being subject to a Personal Data Breach;
e. take such steps as are reasonably required to assist the Member in ensuring compliance with its obligations under Articles 32 to 36 (inclusive) of GDPR (if applicable);
f. provide the Member with its co-operation and assistance in relation to any request made by a data subject to exercise its rights under the Data Protection Laws in relation to that persons Threat Personal Data.
g. except for Threat Personal Data of which FS-ISAC is also a data controller and except as required by law or in order to defend any actual or possible legal claims, take reasonable steps to return or irretrievably delete Threat Personal Data, and not make any further use of such Threat Personal Data, as set out in this Section 13;
h. provide to the Member and any DP Regulator all information and assistance reasonably necessary to demonstrate compliance with the obligations in this Section 13.2 and/or the Data Protection Laws;
i. permit the Member or its representatives to access any relevant premises, personnel or records of FS-ISAC on reasonable notice to audit and otherwise verify compliance with this Section 13.2, subject to the following requirements:
j. the Member may perform such audits no more than once per year (or more frequently if required by Data Protection Laws) and all audits shall be at the Member's sole cost and expense; and

k. following receipt of such notice, the Member and FS-ISAC shall agree in writing the full details and scope of the requested audit, provided that in all cases: (i) the audit shall be subject to FS-ISAC's audit, security and other related policies and procedures; and (ii) FS-ISAC shall be entitled to impose additional confidentiality and security obligations as it may reasonably require.

12.2(b) The Member generally agrees that FS-ISAC may engage third party providers including any advisers, contractors, or auditors to process Threat Personal Data ("Sub-Processors"), and that:

a. if FS-ISAC engages a new Sub-Processor ("New Sub-Processor"), FS-ISAC shall inform Members of the engagement and a Member shall have an opportunity to object to the engagement of such New Sub-Processor by notifying FS-ISAC within 3 Business Days, provided that such objection must be on reasonable, substantial grounds, directly related to such New Sub- Processor's ability to comply with substantially similar obligations to those set out in this clause;

b. FS-ISAC shall ensure that its contract with each Sub-Processor shall impose obligations on that Sub-Processor that are materially equivalent to the obligations to which FS-ISAC is subject to under this Section 13.2; and

c. any sub-contracting or transfer of Threat Personal Data pursuant to this Section 13.2 shall not relieve FS-ISAC of any of its liabilities, responsibilities and obligations to the Member under this Section 13.2 and FS-ISAC shall remain liable for the acts and omissions of its Sub-Processor.

12.2(c) The provisions of this Section 13.2 shall not apply where FS-ISAC processes Personal Data as a controller.

12.3 Mechanism for Transfer Outside of EEA

12.2(a) Save for any transfers of Threat Personal Data made to (i) countries as to whom the European Commission has determined that the data protection laws are adequate, or (ii) organizations that have self-certified under the EU-U.S. Privacy Shield or any equivalent approved mechanism, all transfers of Threat Personal Data outside of the EEA made:

i. by Members to FS-ISAC, shall be made pursuant to the terms of the Standard Contractual Clauses attached as **Attachment A** (Controller to processor Standard Contractual Clauses as approved by the European Commission in Commission Decision 2010/87/EU, dated 5 February 2010); and

ii. by Members to Members (whether via FS-ISAC as a processor or otherwise) or by FS- ISAC as a controller to Members, shall be made pursuant to the terms of the Standard Contractual Clauses attached as **Attachment B** (Controller to controller Standard Contractual Clauses as approved by the European Commission in Commission Decision C(2004)5721).

12.2(b) To the extent applicable, acceptance of these Operating Rules constitutes and shall be deemed to mean acceptance, execution, and delivery of the Standard Contractual Clauses attached as **Attachment A and B**, by FS-ISAC and its Members, in the manner and in their respective capacities as follows:

	CAPACITY		
DATA SOURCE	**Sharing Member**	**FS-ISAC**	**Receiving Member**
Data shared by member located in EEA with FS-ISAC	Data exporter	Data importer	N/A
Data forwarded by FS-ISAC to members (Portal access and email listerver distribution)	N/A	Data exporter	Data importer

By way of example, if a Member located in the EEA submits Threat Personal Data through the Portal or by email, as to that Threat Personal Data, that Member is a controller and bound as a "data exporter" by the terms of the relevant Standard Contractual Clauses. As to that information, FS-ISAC is bound as a "data importer" by the terms of relevant the Standard Contractual Clauses. (The relevant Standard Contractual Clauses will be those at Attachment A to the extent FS-ISAC acts a processor for the Member, and those at Attachment B to the extent FS-ISAC acts as a controller.)

When FS-ISAC shares that information with its Members – via Portal or email distribution – as to that sharing, FS-ISAC is doing so as a processor on behalf of the Sharing Member, who is a controller and bound as a "data exporter" by the terms of the Standard Contractual Clauses at Attachment B. A Member receiving that information is also a controller and bound as a "data importer" by the terms of the Standard Contractual Clauses at Attachment B.

12.4 Conflicts

12.4(a) In the event of any inconsistency, contradiction, or conflict between the terms of this Section 13 and any terms or conditions in the Subscription Agreement, the terms of this Section 13 shall prevail and govern.

12.5 Definitions

12.5(a) For the purposes of this Section 13, the following terms shall have the following meanings:

(i) ″Data Protection Laws″ means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of personal data including: (i) GDPR; (ii) any laws or regulations ratifying, implementing, adopting, supplementing or replacing the GDPR; and (iii) any laws and regulations implementing or made pursuant to EU Directive 2002/58/EC (as amended by EU Directive 2009/136/EC); in each case, as updated, amended or replaced from time to time.

ii. ″DP Regulator″ means any governmental or regulatory body or authority with responsibility for monitoring or enforcing compliance with the Data Protection Laws.

iii. ″GDPR″ means the EU General Data Protection Regulation 2016/679;

iv. ″Sharing Member″ means a Member who shares Threat Personal Data with FS-ISAC and other Members;

v. ″Receiving Member″ means a Member who receives Threat Personal Data from FS-ISAC or other Members in the context of Members' threat information sharing activities;

vi. ″Threat Personal Data″ has the meaning given to that term in Section 13.1(a); and

vii. the terms, ″controller″, ″Data Subject″, ″Personal Data″, ″Personal Data Breach″, ″processor″, ″processing″ and ″supervisory authority″ shall have the meanings set out in the GDPR.

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.

Attachment A – Standard Contractual Clauses (Controller to Processor)

Standard contractual clauses for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Data transfer agreement between the entity deemed the "data exporter" under the Operating Rules, hereinafter "data exporter"
And The entity deemed the "data importer" under the Operating Rules, hereinafter "data importer"
each a "party"; together "the parties".

Have agreed on the following contractual clauses (the clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1.Definitions

For the purposes of the clauses:

a. 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

b. 'the data exporter' means the controller who transfers the personal data;

c. 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

d. 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the clauses and the terms of the written subcontract;

e. 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
f. 'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer
The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the clauses.

3. Third-party beneficiary clause

1. The data subject can enforce against the data exporter this clause, clause 4(b) to (i), clause 5(a) to (e), and (g) to (j), clause 6.1 and 6.2, clause 7, clause 8.2, and clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this clause, clause 5(a) to (e) and (g), clause 6, clause 7, clause 8.2, and clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this clause, clause 5(a) to (e) and (g), clause 6, clause 7, clause 8.2, and clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.
5. Obligations of the data exporter the data exporter agrees and warrants:

a. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
b. that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the clauses;
c. that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;
d. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
e. that it will ensure compliance with the security measures; that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
f. to forward any notification received from the data importer or any sub-processor pursuant to clause 5(b) and clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
g. to make available to the data subjects upon request a copy of the clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the clauses, unless the clauses or the contract contain commercial information, in which case it may remove such commercial information;
h. that, in the event of sub-processing, the processing activity is carried out in accordance with clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the clauses; and

i. that it will ensure compliance with clause 4(a) to (i)

6. Obligations of the data importer the data importer agrees and warrants:

a. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
b. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
c. that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred; that it will promptly notify the data exporter about:

i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
ii. any accidental or unauthorized access; and
iii any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

d. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred; at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
e. to make available to the data subject upon request a copy of the clauses, or any existing contract for sub-processing, unless the clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter; that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent; that the processing services by the sub-processor will be carried out in accordance with clause 11; to send promptly a copy of any sub-processor agreement it concludes under the clauses to the data exporter.

7. Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in clause 3 or in clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with clause 6.1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in clause 3 or in clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in clauses 6.1 and 6.2, arising out of a breach by the sub-processor of any of their obligations referred to in clause 3 or in clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the clauses.

8. Mediation and jurisdiction

The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the clauses, the data importer will accept the decision of the data subject:

a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
b. to refer the dispute to the courts in the Member State in which the data exporter is established. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

9. Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to clause 8.2. In such a case the data exporter shall be entitled to take the measures foreseen in clause 5(b).

10. Governing law These clauses shall be governed by the law of the country in which the data exporter is established.

11. Variation of the contract the parties undertake not to vary or modify the clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the clause.

12. Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in clause 6.2 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in clause 11.1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of sub-processing agreements concluded under the clauses and notified by the data importer pursuant to clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

13. Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in clause 12.1.

Dated: As of the date of the latest amendment to the Operating Rules.

FOR DATA IMPORTERFOR DATA EXPORTER

Executed pursuant to the terms of Section 13. Executed pursuant to the terms of Section 13.

Appendix 1 - To the Standard Contractual Clauses

(To be completed by the parties)
Data subjects
The personal data transferred concern the following categories of data subjects: (1) individuals whose personal data is involved with a cybersecurity threat (including: victims of fraud (or other crimes) who have had their personal data stolen by a third party; and threat actors committing fraud (or other crimes)); and (2) individuals who submit threat intelligence information on a non- anonymous basis.
Purposes of the transfer(s)
The transfer is made for the following purposes: threat intelligence sharing to 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.
Categories of data
The personal data transferred concern the following categories of data: (1) names and contact information of individuals who submit threat intelligence information on a non-anonymous basis; (2) IP addressees; (3) device identifiers; (4) email addresses;
(5) domain names and Uniform Resource Locators (URLs); (6) social network account identifiers; (7) financial account identifiers;

a. other personal information used by a threat actor to hide his/her identity.

Recipients
The personal data transferred may be disclosed only to the following recipients or categories of recipients: FS-ISAC members in accordance with the Operating Rules.
Sensitive data (if appropriate)
The personal data transferred concern the following categories of sensitive data: None.
Data protection registration information of data exporter (where applicable): To the extent applicable, such information is submitted separately, in writing, by the data exporter to the data importer, in accordance with the Operating Rules.
Additional useful information (storage limits and other relevant information): This paragraph applies only if the data importer is a Member. Unless otherwise required by applicable law, including by regulatory requirements or necessary for statute of limitation purposes, all personal data that is (a) received by a Member through the Portal and downloaded, copied, or distributed outside of the Portal or (b) received by a Member by email through the threat intelligence listserver, shall be deleted by the data importer within forty-five (45) days of receipt.
Contact points for data protection enquiries: Each data importer and each data exporter hereunder shall provide to the other, in writing, contact information for data protection enquiries.

Appendix 2 – To the Standard Contractual Clauses

This Appendix forms part of the clauses and must be completed and signed by the parties.
Description of the technical and organizational security measures implemented by the data importer in accordance with clauses **Error! Reference source not found.** and **Error! Reference source not found.** (or document/legislation attached):
Information sharing is a critical part to the defense and protection of critical infrastructure. This Executive Summary gives a high-level overview of the Information Security program for FS-ISAC.
FS-ISAC operates from offices in Reston, Virginia, United States; Singapore, Singapore; and London, United Kingdom. FS- ISAC incorporates a defense-in-depth philosophy influenced by the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) and industry best practices to help develop processes and security controls focused on five core elements of Identify, Protect, Detect, Respond, and Recover.
Identify: FS-ISAC manages an Information Protection Policy outlining guidance for key areas for its security and risk program. Additionally, FS-ISAC leadership regularly convenes an Executive Security Steering Committee to review risks, control recommendations, and evaluate additional security enhancements to protect against new attack vectors.
Furthermore, the Security & Risk Committee (SRC) of the Board of Directors provides oversight for the security program on an ongoing basis. FS-ISAC conducts regular risk assessments and vulnerability scanning. FS-ISAC also conducts security awareness training for all

workforce on a regular basis. As one of the world's premier information sharing organizations for cyber and physical threats, FS-ISAC staff regularly monitor, participate in sharing, and act on relevant cyber threat information shared amongst its membership.
Protect: FS-ISAC deploys a defense-in-depth security strategy using a variety of preventive, detective, and corrective security controls to protect its most sensitive assets and data. In collaboration with trusted partners, FS-ISAC's critical systems are segmented and protected from online attacks through strategically placed intrusion detection and prevention systems, access control systems, advanced firewalls, anti-phishing/spear phishing technology, social engineering prevention technology, malware detection technology, and security policy enforcement technology. Logical access to systems is secured through multi-factor authentication and developer access to production systems is restricted. Critical systems are backed up to ensure continuity.
Detect: FS-ISAC's Information Security team partners with Managed Service Providers (MSPs) to monitor FS-ISAC's networks using state-of-the-art logging and alerting capabilities.
Respond: FS-ISAC maintains an Incident Response playbook to help manage incidents within the enterprise that is routinely reviewed and tested. Incident Response and Forensic specialist are on retainer when needed to assist FS-ISAC staff with containment, investigation, and analysis of a major incident.
Recover: FS-ISAC maintains an inventory of critical assets to aid in recovery of affected systems. FS-ISAC also conducts after-incident assessments to incorporate lessons-learned into existing processes.

Attachment B - Standard Contractual Clauses (Controller to Controller)

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers
Data transfer agreement between the entity deemed the "data exporter" under the Operating Rules, hereinafter "data exporter "and the entity deemed the "data importer" under the Operating Rules, hereinafter "data importer" each a "party"; together "the parties".
Definitions
For the purposes of the clauses:

a. "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);
b. "the data exporter" shall mean the controller who transfers the personal data;
c. "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;
d. "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.
Obligations of the data exporter

The data exporter warrants and undertakes that:

a. The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.
b. It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.
c. It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.
d. It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.
e. It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

I. **Obligations of the data importer**

The data importer warrants and undertakes that:

a. It will have in place appropriate technical and organizational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

b. It will have in place procedures so that any third party it authorizes to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorized or required by law or regulation to have access to the personal data.

c. It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

d. It will process the personal data for purposes described in Annex B and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

e. It will identify to the data exporter a contact point within its organization authorized to respond to enquiries concerning processing of the personal data and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

f. At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g. Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h. It will process the personal data, at its option, in accordance with:

i. the data protection laws of the country in which the data exporter is established, or

ii. the relevant provisions1 of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorization or decision and is based in a country to which such an authorization or decision pertains, but is not covered by such authorization or decision for the purposes of the transfer(s) of the personal data2, or

iii. the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: Option iii.
Initials of data importer: This section is hereby deemed initialed by each Member that is (a) located outside of the European Economic Area (EEA) in a country without a determination by the European Commission as having adequate data protection laws and (b) is not self-certified under the U.S. Privacy Shield (or equivalent approved mechanism for the transfer of personal data outside of the EEA).

I. It will not disclose or transfer the personal data to a third-party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

II. the third-party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

III. the third-party data controller becomes a signatory to these clauses, or another data transfer agreement approved by a competent authority in the EU, or

IV. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

V. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

II. **Liability and third-party rights**

a. Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

1 "Relevant provisions" means those provisions of any authorization or decision except for the enforcement provisions of any authorization or decision (which shall be governed by these clauses).
2 However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.

b. The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

III. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

IV. Resolution of disputes with data subjects or the authority

a. In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b. The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c. Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

V. Termination

a. In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b. In the event that:

i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

iii. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.
Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred

VI. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.
Dated: As of the date of the latest amendment to the Operating Rules.

FOR DATA IMPORTERFOR DATA EXPORTER

Executed pursuant to the terms of Section 13. Executed pursuant to the terms of Section 13.

Appendix 1 – Data Processing Principles

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorized by the data subject.
2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.
4. Security and confidentiality: Technical and organizational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organization holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organizations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organization may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.
6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.
7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.
8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:
   a. I. Such decisions are made by the data importer in entering into or performing a contract with the data subject, and
   ii. The data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.
   Or

b. where otherwise provided by the law of the data exporter.

Appendix 2 - Description of the Transfer

(To be completed by the parties)

Data subjects

The personal data transferred concern the following categories of data subjects: (1) individuals whose personal data is involved with a cybersecurity threat (including: victims of fraud (or other crimes) who have had their personal data stolen by a third party; and threat actors committing fraud (or other crimes)); (2) individuals who submit threat intelligence information on a non- anonymous basis.

Purposes of the transfer(s)

The transfer is made for the following purposes: threat intelligence sharing to 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.

Categories of data

The personal data transferred concern the following categories of data: (1) names and contact information of individuals who submit threat intelligence information on a non-anonymous basis; (2) IP addresses; (3) device identifiers; (4) email addresses; (5) domain names and Uniform Resource Locators (URLs); (6) social network account identifiers; (7) financial account identifiers; (8) other personal information used by a threat actor to hide his/her identity.

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients: FS-ISAC members in accordance with the Operating Rules.

Sensitive data (if appropriate)

The personal data transferred concern the following categories of sensitive data: None.

Data protection registration information of data exporter (where applicable): To the extent applicable, such information is submitted separately, in writing, by the data exporter to the data importer, in accordance with the Operating Rules.

Additional useful information (storage limits and other relevant information): This paragraph applies only if the data importer is a Member. Unless otherwise required by applicable law, including by regulatory requirements or necessary for statute of limitation purposes, all personal data that is (a) received by a Member through the Portal and downloaded, copied, or distributed outside of the Portal or (b) received by a Member by email through the threat intelligence listserver, shall be deleted by the data importer within forty-five (45) days of receipt.

Contact points for data protection enquiries: Each data importer and each data exporter hereunder shall provide to the other, in writing, contact information for data protection enquiries.