Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)
Cyber Information & Intelligence Sharing Initiative: Terms of Reference

1. Background

Cyber threat is borderless and the capabilities of the adversaries are constantly evolving, readily scalable and increasingly sophisticated, threatening to disrupt the interconnected global financial systems. Threat actors are highly motivated and can be persistent, agile, and use a variety of tactics, techniques and procedures (TTPs) to compromise systems, disrupt services, commit financial fraud, and expose or steal intellectual property and other sensitive information. To counter the threat and address the risk, financial infrastructures are required to also be dynamic and agile. Amongst other things, financial infrastructures should have effective cyber threat intelligence processes and actively participate in information and intelligence-sharing arrangements and collaborate with trusted stakeholders within the industry.

Cyber information and intelligence is any information that can help a financial infrastructure[1] identify, assess, monitor, defend against and respond to cyber threats. Examples of cyber information and intelligence include indicators of compromise (IOCs), such as system artefacts or observables associated with an attack, motives of threat actors, TTPs, security alerts, threat intelligence reports and recommended security tool configurations.

By exchanging cyber information and intelligence within a sharing community, financial infrastructures can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats they may face. Using this knowledge, members of the community can make threat-informed decisions regarding defensive capabilities, threat detection techniques and mitigation strategies. By correlating and analysing cyber information and intelligence from multiple sources, a financial infrastructure can also enrich existing information and make it more actionable (e.g. by sharing effective practical mitigations). This enrichment may be achieved by independently confirming the observations of other community members, and by improving the overall quality of the threat information. Financial infrastructures that receive and use this information impede the threat's ability to spread and subsequently raise their individual level of protection. Moreover, by impeding the potential contagion of such threats, the community acts in the ***public interest*** by supporting the safe and sound operation of the financial system as a whole.

[1] The term will be broadly used herein to include public and commercial entities operating FMIs, as well as critical service providers.

In light of the above, the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) members took the common position[2] that an information and intelligence sharing initiative among volunteering ECRB members should be established and that an ECRB Cyber Information and Intelligence Sharing Initiative (CIISI-EU) should be created.

These *CIISI-EU Terms of Reference* set out the high level framework for establishing and participating in CIISI-EU; articulate the core objectives for information sharing; and define the terms to enable the safe and effective information and intelligence sharing within the CIISI-EU Community.

In addition, more detailed information is set out in the '*CIISI-EU ECRB Community Rulebook*'[3].

2. CIISI-EU Objectives

The core objectives of CIISI-EU are:

1. To prevent, detect, respond and raise awareness of cybersecurity threats to ECRB members participating in CIISI-EU, thereby discharging a public interest responsibility;
2. To enable relevant and actionable intelligence sharing within CIISI-EU community, Law Enforcement (and potentially to wider ecosystem) to better protect the European financial institutions against cybersecurity threats;
3. To encourage active contribution and active participation within a 'trusted circle', rather than passive consumption or weak usage;
4. To synthesize and actively propagate the sharing of strategic intelligence in addition to operational TTPs and tactical IOCs indicators;
5. To continuously learn and evolve, as a collective, with regard to the process of analysing, developing and sharing cybersecurity intelligence.

3. CIISI-EU Overall Approach

Sharing across the CIISI-EU Community is based on a number of building blocks:

1. **Threat Intelligence Feeds**: CIISI-EU community members can keep their existing commercial / open source threat intelligence feeds. If information from these sources are relevant for the CIISI-EU Community, members can share them voluntarily and on a best efforts basis to the extent legally and contractually possible;
2. **Central Shared Platform**: CIISI-EU community members commit to using MISP as the standard for information sharing. At their own pace, each CIISI-EU member can

[2] https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/2019/20190628/2019-06-28_ECRB_summary.pdf

[3] The CIISI-EU ECRB Community Rulebook will be drafted by the CIISI-EU Community following agreement on these Terms of Reference. The Rulebook must be agreed upon by all members on a unanimous basis. The Rulebook will not be a legally binding document but a multilateral user description document, setting out how the CIISI-EU Community will operate the information and intelligence sharing network.

set up a MISP instance to connect to the central CIISI-EU MISP.[4] Each CIISI-EU member's MISP instance will synchronise with the other CIISI-EU members' MISP instances, and the collective will operate as a closed and trusted group;

3. **Intelligence Sharing**: CIISI-EU community members will elect what information or intelligence, as referred to in Section 4 of these Terms of Reference, is important enough to warrant disseminating onto the shared platform via their MISP instance;
4. **Strategic Analysis**: The third-party cyber threat intelligence provider[5] will have access to the centralised MISP platform and will add value through the synthesis of strategic analysis based on the collective tactical and operational intelligence on the shared MISP platform and based on their own knowledge of the cybersecurity threat landscape;
5. **Strategic Intelligence Reports**: The third-party cyber threat intelligence provider will produce strategic intelligence and bi-annual reports, focussed at Board level and written in business language, as well as other more frequent bespoke reports and threat dashboards;
6. **Third-party cyber threat intelligence provider Portal**: In addition to having access to the MISP platform, the CIISI-EU Community members will have access to the third-party cyber threat intelligence providers' own threat intelligence portal and interactive collaborative space;
7. **Alerting**: An alerting mechanism to the CIISI-EU Community will be provisioned via SMS text, e-mail distribution, or by using other collaborative tools, ensuring appropriate security and confidentiality requirements are met;
8. **Meetings / Calls**: In person TLP:AMBER[6] meetings and / or calls will be hosted regularly to establish and foster trust within the CIISI-EU Community, with the third-party cyber threat intelligence provider acting as the secretariat;
9. **Strategic Relationships:** The CIISI-EU Community will build strategic relationships with other information sharing communities to enrich the information and intelligence and to bridge communities. All strategic relationships must be agreed upon by all members of the CIISI-EU Community on a unanimous basis.

The provision of services from MISP and the third-party cyber threat intelligence provider will be bound by contractual terms between the CIISI-EU Community Members and the aforementioned service providers.

Further details on the processes and information and intelligence sharing protocols are set out in the *CIISI-EU ECRB Community Rulebook*. The Rulebook sets out the administrative policies, processes and procedures for the operation of CIISI-EU and includes rules on the composition of the CIISI-EU Community, changes to the composition, election of

[4] MISP (formerly known as Malware Information Sharing Platform) is an open source threat intelligence and sharing platform. It is a platform for sharing, storing and correlating Indicators of Compromises of targeted attacks but also threat intelligence such as threat actor information, financial fraud information and many more. A MISP instance is a mini-platform, set up at each member's institution, that will be connected to a centralised MISP platform accessible to all CIISI-EU members. This central MISP will be provided by the Computer Incident Response Centre in Luxembourg (CIRCL).

[5] The third-party cyber threat intelligence provider will be mandated by the CIISI-EU Community based on a procurement process and will provide dedicated threat intelligence services to the CIISI-EU Community.

[6] The information will be assumed to be TLP:AMBER and the source (identity of the providing organisation) be assumed to be TLP:RED.

representatives, meetings and telephone conference calls (place and time, language, chair, agenda, minutes) and decision making.

4. CIISI-EU Scope of Information to be Shared

The CIISI-EU Community will share Strategic[7], Tactical[8] and Operational[9] information and intelligence. As a combination, these three layers of information and intelligence will enable each CIISI-EU Community member to make the business and operational decisions appropriate to it. The scope is expected to encompass:

1. ***Indicators of Compromise (IOCs)*** – these are technical artefacts or observables[10] that suggest an attack is imminent or is currently underway or that a compromise may have already occurred. Indicators can be used to detect and defend against potential threats. Examples of indicators include the Internet Protocol (IP) address of a suspected command and control server, a suspicious Domain Name System (DNS) domain name, a Uniform Resource Locator (URL) that references malicious content, a file hash for a malicious executable, or the subject line text of a malicious email message.

2. ***Tactics, Techniques, and Procedures (TTPs)*** – these describe the behaviour of a threat actor. Tactics are high-level descriptions of behaviour, techniques are detailed descriptions of behaviour in the context of a tactic, and procedures are even lower-level, highly detailed descriptions in the context of a technique. TTPs could describe an actor's tendency to use a specific malware variant, order of operations, attack tool, delivery mechanism (e.g., phishing or watering hole attack), or exploit.

3. ***Security Alerts*** - also known as advisories, bulletins, and vulnerability notes - are brief, usually human readable, technical notifications regarding current vulnerabilities, exploits, and other security issues.

4. ***Threat Intelligence Reports*** – these are generally prose documents that describe TTPs, threat actors, campaigns, types of systems or information being targeted that provide greater situational awareness. Threat intelligence is threat information that has been aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for decision-making processes.

---

[7] Strategic information/intelligence refers to the contextual framework which shapes an adversary's operating environment and intended course of action. It is designed to explore the 'Who and Why' of an organisation's threat landscape.

[8] Tactical information/intelligence refers to visibility of the tools and hacking methodologies used by cyber adversaries to breach victim networks. High quality, actionable tactical information/intelligence gives a unique insight into hackers' methods/capabilities and forms the basis for understanding intent at an operator level. It is concerned with the 'How and What' of an attack.

[9] Operational information/intelligence involves trend analysis of adversary capabilities and attack methodologies. It is concerned with the 'When, Where and How' of an attack campaign and implies an understanding of adversarial skillset. Analysing an adversary's campaign history allows one to identify characteristic attack vectors and patterns of behaviour that can be used to proactively identify the likely precursors of an impending attack and defend against it.

[10] An observable is an event (benign or malicious) on a network or system.

5. ***Tool Configurations*** – these are recommendations for setting up and using tools (mechanisms) that support the automated collection, exchange, processing, analysis, and use of threat information. For example, tool configuration information could consist of instructions on how to install and use a rootkit detection and removal utility, or how to create and customize intrusion detection signatures, router access control lists (ACLs), firewall rules, or web filter configuration files.

6. ***Motives and goals of threat actors*** – these allow one to better understand the motives behind attacks. To predict potential future attacks, it is essential that infrastructures understand the motives, goals and campaigns being undertaken by a threat group, especially state actors or ideologically motivated groups.

More specific details of the types of information and intelligence to be shared are set out in the *CIISI-EU ECRB Community Rulebook*.

5. CIISI-EU Community Members

The 'CIISI-EU Community' is open to members of the ECRB, i.e. pan-European financial infrastructures, central banks (in their operational capacity), network providers, ENISA and EUROPOL. The third-party cyber threat intelligence provider is not a CIISI-EU Community member itself, but provides services to the CIISI-EU Community members, and therefore participates in the information and intelligence exchange.

Authorities in their capacity as regulators, overseers and/or supervisors are not part of the CIISI-EU Community and regulatory reporting on cyber incidents and data breaches are outside the scope of the intelligence sharing within the CIISI-EU Community. Central banks that are part of the CIISI-EU Community must ensure that an internal "Chinese Wall" separates its Security Operating Centre and its system operator function from the regulatory, oversight and supervisory functions it may have to the extent permitted by law.

The list of the CIISI-EU Community member institutions is shown in Appendix B.

6. CIISI-EU Secretariat

The CIISI-EU Community will be served by a CIISI-EU Secretariat. The CIISI-EU Secretariat will act as a liaison towards the CIISI-EU Community members and the third-party service providers. In agreement with the CIISI-EU Community members, the CIISI-EU Secretariat can delegate administrative tasks to the respective third-party service providers. The CIISI-EU Secretariat will rotate among the CIISI-EU Community members at agreed upon intervals.

7. CIISI-EU Community Membership - On/Off Boarding Process

Members are committed to participate in the CIISI-EU Community for an initial period of three years. Thereafter, CIISI-EU membership will automatically be re-affirmed on an annual basis unless a member wishes to withdraw its membership, which must be undertaken by written confirmation to the CIISI-EU Secretariat with a minimum of three months' notice

before the prescribed membership is due to be prolonged. In rare cases, the exclusion of an existing CIISI-EU member must be subject to a majority agreement by the other CIISI-EU members.

Requests for new membership, outside the existing CIISI-EU Community, needs to be sent to the CIISI-EU Secretariat and will be subject to an evaluation and voting process by the members. If there are no objections, the requesting party will enter a staging process for a period of one year, as a prospective member. During that period, the prospective member's participation, collaboration and overall activity will be evaluated by the collective CIISI-EU Community. At the end of that period, the prospective member has the option to decide whether or not to confirm its request for membership, and, provided the input is deemed satisfactory by the current full members of the CIISI-EU Community, there will be a proposal for full membership submitted to the CIISI-EU Community. If no objection from any CIISI-EU Community member is received, full membership will be granted.

More specific details about the on/off boarding and evaluation processes are set out in the *CIISI-EU ECRB Community Rulebook*.

8. CIISI-EU Member's Commitments

Without prejudice to applicable laws, each CIISI-EU member is expected to:

1. Adhere to the terms set out in this *CIISI-EU Terms of Reference* and in the *CIISI-EU ECRB Community Rulebook;*
2. Nominate a single point of contact (including a team, distribution list or group email account) within the member institution that acts as a central coordination point and focus for communications;
3. Maintain and share with the CIISI-EU Community a list of key contacts within the institution across all stakeholders, e.g. senior management, SOC, security operations, threat intelligence, etc.;
4. Adhere to the TLP intelligence sharing protocol referenced in Appendix A when sharing information;
5. For the monthly CIISI-EU Community telephone conference calls, participate on at least 8 of the calls per year;
6. For the in-person meetings, participate in discussions and provide materials / presentations on agreed upon topics of interest;
7. Actively use the central MISP sharing tool, to the extent possible, by sharing relevant intelligence, depending on significance;
8. Pay their financial obligations to MISP and to the third-party cyber threat intelligence provider in a timely manner; and
9. Ensure that the information and intelligence that it shares with the CIISI-EU Community as part of the intelligence sharing does not contain personal data or only personal data that is minimised to the maximum extent possible or is rendered pseudonymous. And ensure that the processing of data by it or on its behalf is

according to the respective national and European legal requirements, including, where relevant, GDPR, EUDPR and the EUROPOL Regulation[11] ("see Data Privacy").

Members that do not follow these terms may be asked to leave the CIISI-EU Community – see section '10. Complaint Process'.

9. Information Sharing Protocols

To ensure confidentiality and maintain the trust levels, all information and intelligence exchange will take place using secure communication channels between the CIISI-EU Community, which includes the third-party cyber threat intelligence provider. The following protocols should be observed:

1. Prior to sharing any information, all parties involved in the information sharing will ensure the confidentiality of the information shared during their cooperation;
2. Information and intelligence provided by members should be used only for the purpose and context intended by these Terms of Reference, and the TLP protocol in Appendix A will be adhered to;
3. Information should be stored and transmitted in an automated way as far as possible, through the MISP sharing platform;
4. By default, it is always assumed that information exchanged *without classification* is for the use only by members at level TLP:AMBER;
5. Information must not be shared with anyone outside of the community, including vendors, as per Appendix A, with the sole exception of the third-party cyber threat intelligence provider procured by the CIISI-EU Community; and
6. If there is a need for sharing outside the community, a query must be made to the originators detailing the intended dissemination. If the originators consent in writing, then the information can be shared to the external parties specified in the request to the originator.

Notwithstanding the above, a CIISI-EU Member may disclose the shared information to a competent regulatory, public or judicial authority having jurisdiction over it, provided it is legally obliged to do so either by law or pursuant to court order or other legal processes (in the latter cases of which, to the extent legally possible, the CIISI-EU Member shall give prior notice of the relevant disclosure order or demand to the originators, shall provide the originators with copies thereof and of the portion of the information disclosed and shall request that the information receives confidential treatment).

The CIISI-EU Community and its members will not create or develop (jointly or otherwise) any intellectual property rights under these Terms of Reference. Members do not licence, transfer, or otherwise grant any rights in their respective intellectual property rights by participating in the CIISI-EU Community and these Terms of Reference.

Appendix A contains the Traffic Light Protocol (TLP) for information sharing.

[11] Regulation (EU) 2016/679 (GDPR), Regulation (EU) 2018/1725 (EUDPR) and Regulation (EU) 2016/794 (Europol Regulation) respectively

10. Complaint Process

Each member shall abide by the membership rules, and undertakes to respect the confidentiality and integrity of the CIISI-EU Community, and of information and intelligence shared within the CIISI-EU Community.

If a member does not observe these rules, the other CIISI-EU Community members reserve the right to terminate its membership.

Termination will be effected by a motion from one member, supported by a simple majority vote of all members.

More specific details about complaints process and the implications of termination (e.g. removal of data, refund of funds for subsequent years, etc) are set out in the *CIISI-EU ECRB Community Rulebook*.

11. Anti-trust compliance

The CIISI-EU community must comply with all applicable competition law rules at all times. The members of the CIISI-EU community may potentially be regarded as competitors or potential competitors. Therefore they commit not to enter into any discussion, activity or conduct that may infringe any applicable competition law rules. For example, competitors shall not directly or indirectly discuss, communicate or exchange any commercially sensitive information, including non-public information relating to commercial strategy, pricing, costs and revenues.

More details on this are set out in Appendix C (Competition Law Compliance Reminder).

12. Liability

All information will be shared on a trust basis and in accordance with a mutually agreed criterion. However, if information shared by a member is factually incorrect, then the member shall not be held liable by other CIISI-EU Community members who may have taken action based on the shared information.

More generally, the CIISI-EU community members are not obliged to disclose information to the CIISI-EU community if such disclosure would result in an infringement of applicable laws and regulations.

13. Data privacy

Members of the CIISI-EU Community understand that in the course of processing the information stemming from CIISI-EU, it is possible that data directly or indirectly linked to a natural person (i.e. personal data) may be processed and as such:

1. Each member shall ensure that the processing of personal data is carried out according to the respective national and European legal requirements, including, where relevant, GDPR, EUDPR and the EUROPOL Regulation;
2. Each member should perform due diligence before sharing this type of information;
3. Each member is responsible to process personal data shared by another member in a lawful manner; and
4. Each member acknowledges that the purpose of processing personal data is to protect the public interest by enhancing the ability of the CIISI-EU Community members (which are as a collective of systemic importance to the EU) to protect and defend their Information Systems and shall not be used for any other purpose.

14. Financial obligations

Costs incurred for the provision of services from MISP and the third-party cyber threat intelligence provider will be borne by members of the CIISI-EU Community on an equal basis and as set out in the contractual terms by the providers. Exceptions can be agreed by the ECRB. Costs related to participation at the in-person meetings will be borne by each member itself.

The *CIISI-EU ECRB Community Rulebook* sets out in more detail the financial implications (including the policies and procedures) related to changes in the number of participants of the CIISI-EU Community.

15. Non-Binding Nature of the Terms of Reference

These Terms of Reference and related discussions are not legally binding and do not constitute terms capable of becoming a contract by acceptance. These Terms of Reference merely constitute a non-binding intention of the signatories. These Terms of Reference are not and shall not be construed in any way to create any binding or legally enforceable obligations on part of the signatories, including without limitation, the obligation to continue negotiations and/or discussions under these rules, nor is any signatory obliged to conduct negotiations and/or discussions in a pre-defined manner or to compensate any costs incurred by the CIISI-EU Community or any of the other signatories in connection with such negotiations and/or discussions.

Name of Entity: .....

Name of Signatory: .....

Position of Signatory: .....

Date of Signing: .....

Appendix A: Traffic Light Protocol (TLP) Information Sharing Protocol

The Traffic Light Protocol (TLP) used within the CIISI-EU Community has been adapted from the IS TLP version 1.1 as published by Trusted introducer at https://www.trusted-introducer.org/ISTLPv11.pdf and is being used to facilitate the information exchange within the CIISI-EU Community. Information will be shared orally in the telco/in-person meetings and through the use of the shared MISP platform. Each member may classify (or designate) each piece of information they provide with one of four information sharing levels, in accordance with their wishes for the handling of their information by other members.

It is the responsibility of the member offering the information to specify its sharing level and for all to respect the designated sharing levels of all information and intelligence offered. If the member offering the information does not designate a sharing level, the information will be assumed to be TLP:AMBER, and the source (identity of the providing organization) be assumed to be TLP:RED. If any member has any doubt whether information is TLP:RED, they must contact the person who offered it before taking any action on it. The four levels are:

RED: Non-disclosable information and restricted to members present at the telco or meeting only. If a document is received, then the document is solely for that individual and no other parties. Members must not disseminate the information outside of that exchange. TLP:RED information may be discussed during the telco/in-person meeting, where all members present have signed up to these rules. The meeting minutes will only mention the topic but no details will be shared in the minutes (they can be obtained on a bi-lateral basis). The use of TLP:RED should be limited as much as possible as it considerably restricts the possibility of acting upon the shared information. Indicators exchanged in a TLP:RED message will be considered TLP:AMBER unless they can be specifically attributed to a CIISI-EU Community member. In that case, they will be kept TLP:RED and the receiving party cannot share them within their organization. This will allow the receiving party to use the indicators that were shared to protect or defend itself. The rest of the message will remain TLP:RED.
AMBER: Limited disclosure and restricted to members of the CIISI-EU Community and those within their organizations (whether direct or affiliate's employees, consultants, contractors or outsource-staff working in the organization and affiliates, that do not have a conflict of interest with any CIISI-EU member or provider) who have an unequitable need to know in order to take action and may be used by the receiving party only to protect or defend itself or its affiliates.
GREEN: Information can be shared with other organizations, information exchanges or individuals in

the network security community at large, but not published or posted on the web. Information cannot be shared with vendors without prior approval by the source of the information.
WHITE: Information that is for public, unrestricted dissemination, publication, web-posting or broadcast. Any member may publish the information, subject to copyright.

Appendix B – Inaugural CIISI-EU Community Membership

To operationalise the sharing initiative, the inaugural CIISI-EU membership, as of February 2020, comprises the following institutions:

1. Banca d'Italia
2. Banco de Espana
3. Banque Centrale du Luxembourg
4. Banque de France
5. BME
6. CLS Bank International
7. Danmarks Nationalbank
8. De Nederlandsche Bank
9. Deutsche Börse Group
10. Deutsche Bundesbank
11. EBA Clearing
12. European Central Bank
13. ENISA
14. equensWorldline
15. European Central Counterparty N.V.
16. Euroclear
17. EUROPOL
18. Iberpay
19. Krajowy Depozyt Papierów Wartościowych / The Central Securities Depository of Poland
20. London Stock Exchange Group (on behalf of LCH SA and Monte Titoli)
21. Mastercard Europe SA.
22. Nasdaq Nordic (on behalf of Nasdaq Clearing and Nordic Exchanges)
23. Nationale Bank van België / Banque nationale de Belgique
24. SIA
25. STET
26. SWIFT
27. TARGET Services
28. Visa Europe

Appendix C – Competition Law Compliance Reminder

While it is appropriate to meet in order to discuss the Purpose (as set out in Section 2), it must be kept in mind that some Parties (i.e. CIISI-EU Members) may potentially be regarded as competitors or potential competitors and any action taken to exchange commercially sensitive information or prevent, restrict or distort competition between (potential) competitors can be a violation of competition laws, in particular Article 101 of the Treaty on the Functioning of the European Union.

Therefore, Parties who are (potential) competitors must refrain from sharing any commercially sensitive information, i.e. information which could potentially reduce strategic uncertainty in the market. Commercially sensitive information includes, inter alia, the following:

- prices and price components, price changes and any elements which might affect prices; profit margins;
- costs and cost strategies;
- fees charged from customers and discounts/rebates granted to customers;
- clients or groups of clients with whom the Participants have, or do not have, business relations;
- plans in relation to geographic or product markets;
- plans concerning the design, production, distribution or marketing of particular products; and
- corporate strategy and investment plans.