NGO-ISAC OPERATING RULES
v2022.02.24

1. OVERVIEW

1.1 The Non-Governmental Organization Information Sharing & Analysis Center ("NGO-ISAC") operates to support information sharing, best practice guidance, and collaboration among U.S.-based non-governmental entities with respect to cyber and NGO-infrastructure readiness and response efforts, including, but not limited to, disseminating early warnings of physical and cyber system threats, sharing security incident information between non-governmental entities, providing trends and other analysis for security planning, and distributing current proven security practices and suggestions.

1.2 These Operating Rules provide outline the terms of participation in NGO-ISAC, and set forth governance and security measures to protect the integrity of the organization and participants. There are two types of "Participants" in NGO-ISAC:

(a) "Members" are qualifying organizations that participate in the products and services available to NGO-ISAC participants. Membership is limited to non-governmental entities organized under the laws of and operating out of the United States. For purposes of these Operating Rules, Member includes the employees of the Member that are granted access to the pursuant to the Member Agreement.

(b) "Partners" are individuals or entities who have entered into a Partner Agreement with NGO-ISAC to provide information and/or services to NGO-ISAC and/or its Members, and/or utilize Data shared by the NGO-ISAC to better secure its Members and the greater internet community, with appropriate privacy and security protections of Member Data

1.3 Members and Partners must apply to be participants and, once approved, must enter into Member Agreements and Partner Agreements, respectively, with NGO-ISAC (collectively, the "Participant Agreements"), which incorporate by reference these Operating Rules.

2. OPERATIONS

2.1.1 The NGO-ISAC will be operated and supported by the staff of the NGO-ISAC

focused on enhancing the cyber security readiness and response of public and private sector entities, with a particular focus on non-governmental and critical infrastructure. The intent of NGO-ISAC is to:

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

(b) Enable the sharing and dissemination of Participant and other trusted source submissions to NGO-ISAC on current threats and security incidents.

(c) Provide immediate information related to major or crisis-level incidents related to the industry to Members.

2.2 Information Sharing.

(a) NGO-ISAC maintains relationships with other sources who provide reports that can be disseminated to the membership, including that from government cyber security agencies, trade associations, CERTs or other entity. When possible, attribution to these external sources will be provided in the alert.

(b) Participants also have the capability to voluntarily submit threat or incident information to NGO-ISAC, through Slack channels (or other similar online communication technologies that may be adopted by NGO-ISAC), shared document forums, and email communications. Sharing of intelligence can occur direct to the NGO-ISAC team or via the member email lists. All alerts published are provided without attribution to the originator to protect their identity unless the originator provides explicit approval to attribute the information to them. Any information provided by Members is provided in good faith, without any warranty or representation by the Member or NGO-ISAC.

(c) Information on cyber threats and incidents should relate to what is experienced by the Participant organization, a third-party provider to the organization or sector or critical infrastructure that the sector depends on. Open source intelligence (i.e. publicly available information found on the internet) is suited for general discussion and does not count as Participant submissions unless the Participant can tie the information to internal events or incidents at their firm.

2.3. Separate from threat sharing, members can also use Slack channels, shared document forums, and email to chat/discuss about a variety of topics. This may be publicly available threat information, advice on security technology or processes, fraud topics, business continuity topics, cross-sector incidents or other items.

2.4 NGO-ISAC maintains formal and informal information sharing relationships with

government cyber security centers, law enforcement and national CERTs. In all relationships, NGO-ISAC strictly follow the TLP handling guidance and never provides information to these partners without the explicit permission of the originator. Attribution is also not provided from Member sources.

2.5 NGO-ISAC has established business relationships with external service providers, including Partners, to deliver certain NGO-ISAC products and services to the Member participants. These products and services are provided subject to the third-party provider's terms and conditions.

2.6 In addition to sharing information though online and written forums, NGO-ISAC shares information with Participants through periodic webcasts and in-person events.

3. DATA PROTECTION

3.1 "Data" is any information shared by either NGO-ISAC or any Participant in accordance with these Operating Rules.

3.2 NGO-ISAC and each Participant acknowledge that the protection of shared Data is essential to the security of both Participants and the mission of the NGO-ISAC. The intent of the Data protection terms are to:

(a) Enable Participants to make disclosures of Data to NGO-ISAC while still maintaining rights in, and control over, the Data; and

(b) Set common information sharing protocols that will determine the extent to which Data can be shared with others.

Except as set forth in Section 4, unless a Participant designates in writing that the Data in question cannot be shared or that such sharing is subject to stated restrictions, all Data provided by Members may be shared with NGO-ISAC's Partners (including, without limitation, all NGO-ISAC partners as listed on member site), and may be shared with other NGO-ISAC Participants provided that the Data is anonymized and not attributable to any Member

3.3 Reports containing Data.

(a) As part of its NGO-ISAC information sharing efforts, the NGO-ISAC may prepare written reports that include or are based on TLP Red Data shared by a Participant. For such reports, the TLP Red Data will be anonymized and Participant shall be provided a period of time to review such reports, papers, or other writings and has the right to review to correct factual inaccuracies and make recommendations and comments to the content of the report.

(b) NGO-ISAC and Participants agree to work together in good faith to reach

mutually agreed upon language for the report; if the parties are unable to reach agreement on an issue, the Participant has the right to edit out its Data.

3.4 Data Retraction.

(a) A Participant can retract Data sent to NGO-ISAC upon written notice. If a Participant retracts any Data it sent to the NGO-ISAC, then, upon notification by the Participant, the NGO-ISAC will delete such Data and all copies thereof, and as applicable, notify other NGO-ISAC Participants to delete the Data.

(b) Upon receiving such notification, NGO-ISAC Participants will delete such information and all copies thereof within 7 days.

(c) If an NGO-ISAC Participant is unable to delete the Data based on applicable law, then that Participant will continue to maintain the confidentiality of the Data consistent with the TLP designation assigned to the Data.

3.5 Data Requests.

(a) If any third party makes a demand for any Data, the NGO-ISAC or any other Participant receiving such a demand shall, if legally permitted, promptly forward such request to the Participant who shared the Data, if known (and otherwise to NGO-ISAC), and consult and cooperate with that Participant or NGO-ISAC and make reasonable efforts, consistent with applicable law and the applicable TLP designation, to protect the confidentiality of the Data.

(b) The Participant sharing the Data will, as needed, and if legally permitted, have the opportunity to seek judicial or other appropriate avenues of redress to prevent any release of such Data.

3.6 Other Data Designations. NGO-ISAC and Participants acknowledge that certain Data may also be designated with a notice of patent, copyright, trade secret or other proprietary right and NGO-ISAC and Participant each agree not to remove, alter or obscure any such designation without the prior written authorization of the party sharing the Data. Nothing in these Operating Rules conveys any rights or ownership in the Data to NGO-ISAC or other Participants, apart from the right to use the Data as provided herein. Each Participant shall maintain ownership of its Data.

4. TRAFFIC LIGHT PROTOCOL (TLP)

4.1 All information submitted, processed, stored, archived, or disposed of is classified under TLP and handled in accordance with its classification as defined here.

(a) RED. Sources may use RED when the audience for the information 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 RED information with any parties outside of the original recipients.

(b) AMBER. Recipients may only share TLP AMBER information with staff in their own organization who need to know, or with service providers to mitigate risks to the Member's organization if the providers are contractually obligated to protect the confidentiality of the information. TLP AMBER information can be shared with those parties specified above only as widely as necessary to act on the information.

(c) GREEN. Sources may use GREEN when the information is useful for the awareness of all member organizations as well as peers within the broader community. Recipients may share GREEN information with peers, trusted government and critical infrastructure partner organizations and service providers with whom they have a contractual relationship, but not through publicly accessible channels.

(d) WHITE. Sources may use WHITE when the information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. WHITE information may be distributed without restriction, subject to copyright controls.

4.2 If no marking is specified, the information shall default to TLP AMBER.

4.3 Information classified as RED, AMBER, GREEN 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. NGO-ISAC SYSTEM SECURITY

5.1 Information Security Program

NGO-ISAC maintains an Information Security Program that at a minimum provides: (i) an organizational structure and appropriate security controls to protect Member and corporate information; (ii) employee and contractor controls including communication of applicable policies, security awareness, and disciplinary processes; (iii) data and system security controls including access and authorization, logging and monitoring and vulnerability management; and (iv) incident response procedures.

6. CONFIDENTIALITY

6.1 Confidentiality Information

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

(b) Confidential information may be disclosed by an NGO-ISAC alert or notification. Confidential information may also be disclosed at member, committee and other meetings of members that may be constituted.

(c) Directors, officers, staff of NGO-ISAC and Participants agree that all such Confidential information obtained shall be considered confidential and proprietary to the disclosing party.

(d) As stipulated in Section 4.3, Traffic Light Protocol, all information is classified as Confidential AMBER by default unless specifically classified otherwise.

(e) 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 NGO-ISAC with advance notice of such disclosure to allow NGO-ISAC and impacted parties to seek an appropriate protective order or other relief to prohibit or limit such disclosure.

6.2 Confidentiality Agreement. Recipients of Confidential information are obligated to:

(a) Protect and preserve the confidential and proprietary nature of all Confidential Information.

(b) 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 NGO-ISAC and the disclosing party.

(c) 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.

(d) 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.

(e) 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.

(f) Notify the NGO-ISAC immediately of any loss or misplacement of Confidential information, and

(g) Comply with any other reasonable security procedures prescribed by the NGO-ISAC for protection of the Confidential information.

7. RULES MODIFICATION

7.1 From time to time these Operating Rules and the Member Agreement may be modified with the approval of the Board of Directors. Notifications to current Members will be provided at that time via electronic means.

8. HELP DESK POLICY AND PROCEDURES

8.1 Users of NGO-ISAC's products and services can find assistance either by contacting membership@ngoisac.org or via Slack in the #membership-questions-and-management