MedISAO Vulnerability Submission Handling Procedure

Purpose

This process is designed to meet the needs of ISAO members in the medical device development community. The process take into account different privacy levels so that MedISAO may respect member Intellectual property while still providing the necessary sharing duties of an ISAO. This procedure may be updated in the future as new use cases and modes are discovered.

Privacy Level

All submitted vulnerability or threat information must be accompanied by a privacy level in the format of the Traffic Light Protocol (TLP) (https://www.first.org/tlp).

For Reference, the TLP levels are:

1. **TLP:RED** = Not for disclosure, restricted to participants only.
   Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
2. **TLP:AMBER** = Limited disclosure, restricted to participants' organizations.
   Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
3. **TLP:GREEN** = Limited disclosure, restricted to the community.
   Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
4. **TLP:WHITE** = Disclosure is not limited.
   Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

If submitted information is labeled as **TLP:RED** and also labeled as Protected Critical Infrastructure Information (PCII) , then the information will be electronically submitted to DHS as PCII. All submissions labeled as **TLP:RED** will be kept strictly confidential with MedISAO, and every 30 days, will be reviewed by MedISAO and the information submitter to determine if the privacy level can be lowered. The intent is that after a sufficient amount of time, the information may be shared with the broader community. All submissions labeled **TLP:AMBER** will be shared with members who have an active NDA signed within MedISAO, but not outside membership. All members of MedISAO should be up to date on the TLP protocol, and respect the labeling. **TLP:GREEN** submissions will be shared with the broader ISAO community, but not published on any public facing pages. **TLP:WHITE** submissions will be shared with the broader ISAO community and may be published publically.

Encryption and Security

All data in the database of submission information will be encrypted using MedISAO's public PGP key. Access to the private version of the key will be limited to the MedISAO director and designated analysts. All submissions will only be accepted over a secured TLS http connection (i.e. modern HTTPS) or via e-mail already encrypted with MedISAO's public PGP key.

Coordinated Disclosure

If the submission originated from a 3rd party, and not from the manufacturer or creator of the device or product that the submission concerns, MedISAO will attempt to submit the information through the Coordinated Disclosure Policy of the manufacturer. If the manufacturer has not set up a Coordinated Disclosure policy, MedISAO will attempt to submit the information through the manufacture's complaint handling process. If a 3rd party submits information to MedISAO labeled with the **TLP:RED or TLP:AMBER** privacy level, MedISAO will attempt the contact the submitter of the information to clarify intention. MedISAO may, at it's sole discretion, choose to submit the information to the Manufacturer's Coordinated Disclosure Program regardless of TLP privacy designation.