Solicitation for a Discussion on an ISAO Certification Model

Purpose of ISAO Certifications

In 2015, the Information Sharing and Analysis Organization (ISAO) Standards Organization (SO) was formed to support the objectives of Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing.* The ISAO SO has set out to create the conditions for a deep, broad, and rich network of information-sharing organizations. Its goal is to foster the development and adoption of mechanisms for the timely sharing and analysis of cybersecurity information to elevate the security of our nation. As the number of ISAOs grows from dozens to hundreds, a clear understanding of an ISAO's services and capabilities will be essential to promote the growth of trust that is essential to facilitate the rapid propagation of time-critical information throughout the ecosystem. One potential mechanism for promoting a scalable and sustainable information-sharing environment is a voluntary certification process. The certification is a validation to prospective members and to others in the ecosystem that an ISAO provides a specific set of capabilities and services.

The purpose of establishing certifications is to promote rapidly scalable growth within a strong and healthy sharing community. To that end, certification requirements must not create a significant barrier to entry for newly forming ISAOs, nor jeopardize the viability of currently functioning, healthy ISAOs. Voluntary certifications should promote a more rapid development of trust between an ISAO and its members, from ISAO to ISAO, and between an ISAO and the government. Certification also should provide an understanding of what can be expected by members of the ISAO.

Certification Types

There are two types of certifications: self-certification and third-party certification. The information-sharing community may create additional certifications to address future requirements as foundational, additional, and unique services and capabilities are further defined (and, possibly at some point, associated service levels).

Self-Certification

An ISAO can become a *self-certified ISAO* by completing the ISAO SO Self-Certification form and submitting it to the ISAO SO to be recorded in the Database of Self-Certified ISAOs.

When an ISAO self-certifies, it is publicly affirming that it performs the five foundational services and capabilities identified in ISAO 100-2 and ISAO 200-1:

- Collect information
- Analyze information
- Disseminate information to members
- Facilitate member sharing
- Survey members.

Self-certification can be asserted with or without reference to specific means, methods, or technologies that an ISAO employs, and it may or may not identify a specific level of services and capabilities provided

to its members. It is acknowledged that self-certification will not by itself engender a great deal of trust in an ISAO, but it does present a public statement that the ISAO provides the specified services in some fashion. It also is a first step for emerging ISAOs that may not be ready for third-party certification but want to work toward it.

Third-Party Certification

The certification process is initiated when the ISAO makes a request to an ISAO certifying body (CB) to become a "certified ISAO." Using certification procedures published by the ISAO SO, the CB will conduct a demonstrative review of the specific means, methods, and technologies employed by the ISAO and will further validate that the ISAO provides the five foundational services.

ISAOs may also choose to develop additional or unique services and capabilities to better serve their members. None of these are required for the foundational certification, but the ISAO may wish to have the additional or unique services and capabilities certified along with the five foundational services and capabilities. The following are examples of additional and unique services and capabilities taken from ISAO 100-2, *Guidelines for Establishing an Information Sharing and Analysis Organization*:

- Host a secure online discussion for member-to-member collaboration
- Collect and disseminate mitigation information and resources
- Collect and disseminate response and recovery information and resources
- Host a secure online document repository for sharing information with members
- Participate in automated indicator sharing
- Provide vendor vulnerability notifications
- Provide a reach-back service whereby members can consult subject matter experts
- Form committees, working groups, or special communities of interest among members
- Facilitate mutual aid among members
- Provide managed security services (security operations center)
- Provide access to a library of adversary tactics, techniques, and procedures
- Offer test-bed access by members for malware analysis.

An ISAO is responsible for maintaining its services and capabilities consistent with its certification. The ISAO can choose at any time to withdraw a certification. (Note: this document should ultimately also address the process by which certifications can be reviewed or revoked by the ISAO SO or an ISAO CB.)

Accreditation of Third-Party Certifying Bodies

To ensure the consistency, quality, and value of these and future certifications, the ISAO SO will accredit third-party certifying bodies through an open and transparent process. (Note: specific accreditation requirements have not yet been defined.) The CB will need to be reaccredited every 2 years. The ISAO SO will maintain a published list of all CBs.

Definitions

Additional services and capabilities: Enhanced services (beyond foundational services and capabilities) designed to address the specific needs of an ISAO's members.

Capability: A business process or task that is used to support the ISAO.

Cyber-threat information: Any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor. Major types of threat information include indicators, security alerts, threat intelligence reports, tool configurations, and tactics, techniques, and procedures.

Federal government: All U.S. government agencies.

Foundational services and capabilities: These are generally considered baseline services for most ISAOs but are established based on the needs of the members. They might include using a standard method to send and receive cyber-threat intelligence, vetting members (a trust capability), and storing cybersecurity information, to name a few**.**

Service: A business process or task that is offered to support an ISAO's members.

State, local, tribal, and territorial governments: Government entities that are not the federal government.

Unique services and capabilities: Specialized functions or activities developed or adopted by the organization to meet its particular needs or opportunities. Unique services are those that are not otherwise identified as "foundational" or "additional." An ISAO electively creates and applies unique services. These might include understanding effective firewall settings, growing mentor-protégé opportunities, and instituting listserv mechanisms.