Mendoza Law, LLC

1000 University Ave., W. Suite 222
Saint Paul, MN 55104
651-330-8062 (Main)
www.mendozalawoffice.com

Anthony S. Mendoza, Esq.
Direct Dial: 651-340-8884
tony@mendozalawoffice.com

GUIDELINES RELEASED FOR ESTABLISHING CYBERTHREAT INFORMATION SHARING ORGANIZATIONS

New guidelines for the establishment of information sharing assistance organizations (ISAOs) were released by the ISAO Standards Organization (ISAO SO) on Friday, September 30, 2016. The ISAO SO, led by the University of Texas at San Antonio (UTSA) is a non-governmental organization established in October 2015 to facilitate the implementation of President Obama's Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing." The ISAO SO created working groups composed of over 160 industry, government and academic experts who led the development of the guidelines published Friday.

Four new guidelines were published:

ISAO 100-1: Introduction to Information Sharing and Analysis Organizations (ISAOs): This publication offers an overview of ISAOs. An ISAO is a voluntarily formed organization that analyzes and shares information related to cybersecurity risks and incidents between and among its membership. The ISAO SO envisions a cybersecurity information sharing ecosystem – a "white hat network" built on trust, shared values, and expectations. The 100-1 Publication describes the benefits that ISAOs can provide to their members, including:

- Providing cybersecurity threat information and operational practices to help ISAO members be more secure;
- Establishing and maintaining trust relationships among members by establishing a framework of common, shared values and expectations;
- Enhanced situational awareness and knowledge about how to protect against, detect, and react to cyber-attacks;
- Exchanging information and carrying out timely responses to cybersecurity incidents;
- Sharing non-incident information such as best practices, training opportunities, processes and procedures, and product information;
- Lowering costs and barriers to entry for cybersecurity information sharing.

Publication 100-1 also previews the full ISAO document series and the scope of future guidelines and standards.

ISAO 100-2: Guidelines for Establishing an Information Sharing and Analysis Organization: ISAO 100-2 guides readers through the most critical considerations to creating an effective organization, including:

- Importance of strategic planning prior to forming an ISAO, including considerations such as: defining the common purpose of the ISAO, how the

ISAO will improve the cybersecurity position of its members, the goals of the ISAO, what information the ISAO will share, the ISAO's role in the information sharing ecosystem, identifying partnerships and collaborations, defining the services and capabilities the ISAO will provide, defining membership criteria, development of methods to measure the effectiveness and thus the value delivered by the ISAO, operational planning, choice of entity, the appropriate governance model, development of a marketing plan, communications strategy, and financial model.

- Ways a new ISAO can establish and maintain a trusted community.
- Publication 100-2 also contains a valuable Appendix that provides a matrix of the different services and capabilities that an ISAO can provide.

An important emphasis of the new guidelines is that ISAOs can take a number of forms and roles. ISAOs can be formed across industry sectors. For example, entertainment related businesses may have a unique set of needs that might cause them to form an ISAO. Or, ISAOs can be formed on a geographic basis. ISAOs have been formed around the needs of particular states or regions, cutting across industry sectors.

In addition, ISAOs may start with rather modest or highly ambitious goals. Some ISAOs may start out with the goal of creating awareness about cybersecurity threats through sharing basic threat intelligence information. Other ISAOs may provide highly sophisticated real-time sharing of cyber-threat information. ISAOs can also start with modest goals that evolve to provide increasingly sophisticated services.

ISAO 300-1: Introduction to Information Sharing: This document describes a conceptual framework for information sharing concepts, the types of cybersecurity-related information an ISAO may want to share, ways an organization can facilitate information sharing, as well as privacy and security concerns to be considered.

ISAO 600-2: U.S. Government Relations, Programs, and Services: ISAO 600-2 addresses relevant federal laws and regulations regarding cybersecurity information sharing within the United States, as well as state and local perspectives. It also includes a comprehensive listing of available government resources to assist ISAOs and their members.

ISAO 600-2 also discusses the role the government plays within the information sharing ecosystem. Often threat information contains private data on individuals or competitively sensitive data, the disclosure of which can create liability for the disclosing party. ISAO 600-2 provides the legal framework around thorny questions regarding the sharing of threat intelligence with the government and liability protections afforded to organizations when doing so.

The publication of these four documents in just the beginning of an important movement to protect the nation from cybersecurity threats. The ISAO SO will be updating and expanding these

publications based on feedback received from the public. Moreover, the ISAO SO will be issuing additional guidelines. Seven sets of guidelines are anticipated around the following general topics:

ISAO 100 Series: Establishment and Operation of ISAOs
ISAO 200 Series: ISAO Services and Capabilities
ISAO 300 Series: Information Sharing
ISAO 400 Series: Privacy and Security
ISAO 500 Series: Analysis
ISAO 600 Series: Government Relations
ISAO 700 Series: Global Information Sharing

The guidelines as well as many other valuable resources related to cybersecurity can be found at the ISAO SO website: isao.org