Government Relations Considerations

Draft Document—Request For Comment

SWG G 6—2016 v0.2

ISAO Standards Organization
Standards Working Group 6: Government Relations
Mike Echols, Chair
David Weinstein, Vice-Chair

May 2, 2016

Table of Contents

Revision Updates

Item	Version	Description	Date
1	0.1	Initial document: Products and Services	April 5, 2016
2	0.1.2	Update: Role of Government and State and Local	April 19, 2016
3	0.2	Update: Regulation and finalize draft	May 2 2016

EXECUTIVE SUMMARY

The objective of Standards Working Group 6, Government Relations, and this guide is to identify preliminary matters of policy and principles, state and local government perspectives, and relevant federal regulations. Developing trust between the government and ISAOs is a major consideration for all parties. This working group also addresses considerations for ISAO interaction with the intelligence community, law enforcement agencies, U.S. regulatory agencies, the Department of Homeland Security, and other government departments and agencies.

The purposes of this voluntary ISAO Standards Organization (SO) guide are to:

- Assist ISAOs, both new and existing, with information relevant to their operation and federal, state, local, and tribal governments.
- Outline the scope, strategy, and outputs concerning the Role of Government Subgroup.
- Address issues and considerations from the perspective of state and local governments.
- Provide an overview of relevant federal regulations.

This is the first complete draft of this voluntary guide on scope, strategy, and outputs concerning the role of government. This draft is intended to be a starting point and will be updated continuously through public input and working group research.

SCOPE, STRATEGY, AND OUTPUTS CONCERNING THE ROLE OF GOVERNMENT

The Role of Government Subgroup of Standards Working Group 6, Government Relations, has conducted its initial review of the tasks that it has been charged to perform as part of the ISAO SO efforts to issue guidance to existing and emerging ISAOs. The first report of the Role of Government Subgroup provides a consensus view concerning the scope, strategy, and outputs related to the role in which government agencies should participate in ISAO efforts nationally.

PRELIMINARY MATTERS

The subgroup identified six fundamental issues that were necessary to resolve before exploring other issues:

- What voice should serve as the driver for issue spotting and analysis?
- What broad functional categories should serve as a framework for analysis?
- What principles should guide our analysis of the legitimacy of government participation?
- How does the subgroup develop role of government issues for consideration?
- To what extent should mechanisms be created to resolve disputes at the federal, state, and local level between governmental and private-sector entities—for example, in the context of law enforcement investigations?
- Does the subgroup effort need extended continuity, given the dynamic nature of its charge? If continuity is recommended, what mechanisms are needed to ensure a viable and meaningful feedback and issue resolution loop?

WHAT VOICE?

By consensus, the subgroup believes that its voice should be that of the private sector and the non-federal levels of government. Information sharing, cross-sector partnering, and regional capacity building are part of the national approach to improved cybersecurity that has been promulgated at a national level (such as via executive orders and federal law). The approach that led to establishment of the ISAO SO originated from the White House. Lacking in the emergence of the ISAO initiative to date, however, are meaningful inputs from the private sector and non-federal levels of government. To achieve national adoption of the ISAO approach to improved cybersecurity, the subgroup believes that other views besides those of the federal government are essential to achieving success.

It is understood by the subgroup that this pathway is primarily to ensure dialogue and collaboration. The voice of the federal government will help to ensure that the voluntary standards for ISAOs reflect all levels of appropriate considerations

and take into account the equities of all participants in the public-private partnership.

WHAT CATEGORIES?

By consensus, the subgroup slightly reframed the scope suggested by the ISAO SO, preferring instead to focus on the roles of government with respect to the enablement, collaboration, and support for ISAOs. The subgroup's analysis will focus on these participation functions in its analysis, assessing these categories for federal, state, and local government.

WHAT PRINCIPLES?

By consensus, the subgroup agreed to an initial list of roles that are generally accepted as government functions in society (assessed at each level). The purpose of the list is for use as a measure of the legitimacy of government involvement in functions identified for analysis. The generally accepted roles are:

- National security and defense
- International relations and diplomacy
- Public safety and preparedness
- Administration of justice
- Governance and legislation
- Economic stability
- Critical infrastructure
- Social welfare
- Education
- Law enforcement.

The subgroup conducted online research and used the expertise of its Core Development Team to produce this list. The subgroup anticipates that this list will continue to evolve and increase in specificity as use cases trigger deeper analysis. In terms of establishing a framework for assessing the legitimacy of a government role, the subgroup believes that this list is useful.

WHAT PROCESS FOR ISSUE DEVELOPMENT?

The subgroup divided into liaison and production sections. Liaison staff perform outreach and coordination with other working groups and subgroups. The organizing and standards development work of these other groups is likely to generate concrete role of government issues. The liaison structure will facilitate issue spotting and introduction to the Role of Government Subgroup for analysis and production of consensus views, recommendations, and best practices. The subgroup will also develop its own issues, which may range from strategic issues

to concrete issues developed from the experiences of the Core Development Team.

WHAT POLICIES OR MECHANISMS MIGHT BE CREATED FOR RESOLVING DISPUTES?

Especially, but not only, in the area of law enforcement, disputes will arise concerning the desire for government entities at all levels to obtain information from private-sector entities whose potential cooperation might be conflicted by various privacy interests. While the safety and security components of the role of government are clear enough, can the government's role be amplified to involve mechanisms short of judicial proceedings that involve ongoing conventions between government and ISAOs or groups of ISAOs?

WHAT PERMANENT CONTINUITY?

By consensus, the subgroup's initial view is that role of government issues will continue to emerge as society adopts and implements the ISAO approach. Therefore the subgroup anticipates a future recommendation that outlines the need for permanence and offers a proposed model that enables continuity and meaningful contributions to a dynamic ISAO ecosystem.

ISSUES TO ADDRESS FROM THE STATE AND LOCAL GOVERNMENT PERSPECTIVE

TRUST RELATIONSHIP

Effective information sharing requires a trust relationship among those who share and receive information. Specific concerns related to government entities include the following:

- Governmental entities should feel safe to share and receive sensitive cyber threat and vulnerability information without fear of public disclosure via state sunshine or freedom of information laws.
- Governmental entities must balance citizen privacy concerns with effective information sharing policies and practices.
- Private entities may not want to share sensitive threat and vulnerability information with governmental entities if there is a fear of governmental regulation based on the information received.
- It should be assumed that the relevance of cyber threat and vulnerability information extends outside of a formal information sharing environment—that is, entities external to the ISAO could benefit from the information being shared. There should to be a mechanism to ensure that such an entity is able to receive sensitive cyber threat and vulnerability information upon request.

- Governmental entities should be assured that the receipt of cyber threat and vulnerability information does not create affirmative duties for which they could be held liable.
- Care and consideration should be given to the quality, timeliness, and relevance of information that states and localities share with ISAOs.

RECOMMENDATIONS

The greatest barrier to sharing cyber threat and vulnerability information with state governments is state disclosure laws. Critical infrastructure and cyber disclosure exemption laws would streamline the sharing of information between private entities and government to set a pathway so that cybersecurity information sharing is more proactive rather than reactive. This could facilitate and encourage the private sector to participate and collaborate with states more regularly. Several states have begun to address this issue via state legislation, creating such exemptions for critical infrastructure and cyber security information. It is recommended that states undertake the development of such exemptions to enable more effective collaboration and ultimately build trust between states and private sector entities.

Some key themes, principals, and language found in successful state legislation effectively address these exemptions.

- A definition for critical infrastructure information and exclusion from disclosure under state freedom of information or sunshine laws. Critical infrastructure information may defined using:
  - The federal definition of critical infrastructure information found within 6 United States Code (U.S.C.) § 131.
  - Language defining public utility systems such as oil, electric, gas, sewer, water, or wastewater sectors.
  - More specific language pertaining to a specific sector such as critical energy infrastructure.
- A definition of security information, which may include physical or cyber-related data. Examples of types of security information include:
  - Cybersecurity plans, assessments, and operational manuals
  - Technical or diagnostic records that, if disclosed, could reveal the location or operational details of sensitive systems
  - Information not lawfully available to the public regarding specific cybersecurity threats or vulnerabilities
  - Information that identifies, or provides means of identifying, a person who could, as a result of the disclosure, become a victim of a cybersecurity incident, or that would disclose a person's cybersecurity plans or

practices, procedures, methods, results, or organizational structure, hardware, or software.

EXISTING CAPABILITIES AND PROGRAMS

States may also look to existing capabilities and programs that support broader information sharing between local, state, federal, and private-sector stakeholders. These capabilities include but are not limited to those discussed below.

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII) PROGRAM

Formed as a result of the passage of the Critical Infrastructure Act in 2002, the Protected Critical Infrastructure Information (PCII) program affords protections to information provided by the private sector to the federal government. These protections include exemption from the federal Freedom of Information Act (FOIA), state and local disclosure laws, regulatory action, and civil litigation. Although DHS manages the PCII program at the federal level, states are encouraged to maintain their own programs in order to provide access to PCII protected information for state and local authorities with a need to know. States can implement PCII programs to more effectively share information with the private sector and build trust by protecting the information from regulators and the public.

FUSION CENTERS

Fusion centers were formed as a result of the terrorist attacks on September 11, 2001, and serve as a means of collecting, analyzing, and disseminating information that pertains to terrorism and organized crime activities. They exist in most states and are already integrated into local, state, and regional homeland security initiatives. Though fusion centers have varying levels of maturity with respect to cyber analytical capability, they have already established themselves within the critical infrastructure community as a means of sharing information on physical threats and are poised as an effective mechanism to share cyber threat information across sectors and disciplines. As states look to interface with and/or develop ISAOs, fusion centers may serve as a key capability in this effort.

MEMORANDUMS OF UNDERSTANDING OR AGREEMENT

States and localities should also consider the use of Memorandums of Understanding or Agreement (MOUs or MOAs) as a formal means of forging partnerships with public and private stakeholders and to foster information sharing. Although a PCII like assists in protecting information that the private sector shares with government, it also precludes other private-sector entities from accessing that information. States and localities that seek to form or support ISAOs might wish to use an MOU or MOA to allow for broader distribution of information under certain conditions.

OVERVIEW OF FEDERAL REGULATIONS FOR ISAO CONSIDERATIONS

FEDERAL STATUTES RELATED TO INFORMATION SHARING

ISAOs may wish to consider a number of existing federal statutes when establishing policies and procedures for sharing of information, including those discussed below.

CYBERSECURITY INFORMATION SHARING ACT OF 2015

On December 18, 2015, President Obama signed into law the Cybersecurity Information Sharing Act of 2015 (CISA), which is designed to increase cybersecurity information sharing between the private sector and the federal government. CISA provides various protections to non-federal entities that share cyber threat indicators or defensive measures with the federal government. The DHS Automated Indicator Sharing (AIS) initiative is the principal mechanism for such sharing. Sharing information with DHS through AIS or other DHS mechanisms in accordance with CISA provides the submitter with certain liability protections.

DHS has released guidance to assist private-sector and non-federal entities that share cyber threat indicators with the federal government. DHS has also released interim policies and procedures relating to the receipt and use of cyber threat indicators by federal entities, interim guidelines relating to privacy and civil liberties in connection with the exchange of those indicators, and guidance to federal agencies on sharing cyber-related information in the government's possession.

The PCII program enhances voluntary information sharing between infrastructure owners and operators and the government by providing a level of protection to facilities submitting information authorized as PCII to DHS. This better enables DHS to work directly with infrastructure owners and operators to identify vulnerabilities, mitigation strategies, and protective measures. If the information submitted to DHS satisfies the requirements of the CII Act, it is protected from:

- FOIA
- State, tribal, and local disclosure laws
- Use in regulatory actions
- Use in civil litigation.

PCII protections mean that homeland security partners, including ISAOs, can be confident that sharing their information with the government will not expose

sensitive or proprietary data. In fact, the PCII final rule specifically discusses the protections afforded to information provided to DHS by ISAOs. See 71 Federal Register 52262 et seq.

For more information on the PCII program, see: https://www.dhs.gov/protected-critical-infrastructure-information-pcii-program.

To view the guidance documents and learn more about AIS and the sharing of cyber threat indicators, see: www.us-cert.gov/ais.

CRITICAL INFRASTRUCTURE INFORMATION ACT OF 2002/PROTECTED CRITICAL INFRASTRUCTURE INFORMATION PROGRAM

The Critical Infrastructure Information (CII) Act of 2002 was established to facilitate DHS's ability to collaborate effectively to protect America's critical infrastructure. It authorized DHS to accept information relating to critical infrastructure from the public; owners and operators of critical infrastructure; and state, local, and tribal governmental entities, while limiting public disclosure of that sensitive information under FOIA, 5 U.S.C. § 552, and other laws, rules, and processes. To implement the CII Act, DHS established the PCII program, 6 Code of Federal Regulations (CFR) Part 29.

THE FREEDOM OF INFORMATION ACT

The Freedom of Information Act, 5 U.S.C. § 552, generally provides that any person has the right to request access to federal agency records or information except to the extent that the records are protected from disclosure. Records may be protected from disclosure under one of nine exemptions contained in the law:

- Classified information for national defense or foreign policy
- Internal personnel rules and practices
- Information that is exempt under other laws
- Trade secrets and confidential business information
- Interagency or intra-agency memoranda or letters that are protected by legal privileges
- Personnel and medical files
- Law enforcement records or information
- Information concerning bank supervision
- Geological and geophysical information.

Congress also provided special protection in the FOIA for three narrow categories of law enforcement and national security records. The provisions protecting those records are known as "exclusions." The first exclusion protects

the existence of an ongoing criminal law enforcement investigation when the subject of the investigation is unaware that it is pending and disclosure could reasonably be expected to interfere with enforcement proceedings. The second exclusion is limited to criminal law enforcement agencies and protects the existence of informant records when the informant's status has not been officially confirmed. The third exclusion is limited to the FBI and protects the existence of foreign intelligence or counterintelligence, or international terrorism records when the existence of such records is classified. Records falling within an exclusion are not subject to the requirements of the FOIA.

For more information on FOIA, see: www.foia.gov or https://www.justice.gov/oip/foia-resources.

THE PRIVACY ACT

The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A "system of records" is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of 12 statutory exceptions. The Privacy Act also provides individuals with a way to seek access to and amend their records, and sets forth various agency record-keeping requirements.

For more information on the Privacy Act, see: https://www.justice.gov/opcl/privacy-act-1974.

FEDERAL CYBERSECURITY REGULATIONS WITH AN INFORMATION SHARING NEXUS

A small number of existing or proposed federal regulations concerning cybersecurity touch on cybersecurity information sharing that ISAOs may wish to consider when establishing policies and procedures. They include those discussed below.

CHEMICAL FACILITY ANTI-TERRORISM STANDARD

Under the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, high-risk chemical facilities must develop and submit to DHS for approval site security plans that, among other things, include the facility's cybersecurity measures. While CFATS-covered facilities have flexibility in establishing a security posture that is tailored to their unique characteristics, DHS expects such

facilities to include in their security plans a description of their approach to addressing cybersecurity incidents, including the reporting of such incidents to US-CERT (www.us-cert.gov).

For more information on the CFATS cybersecurity requirements, including reporting of cybersecurity incidents, see https://www.dhs.gov/cfats-risk-based-performance-standards, and download a copy of the CFATS Risk-Based Performance Standards Guidance Document.

POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES

Recognizing the growing importance of cybersecurity for medical devices and the potential public health risks that could result from inadequate post-market cybersecurity management, the U.S. Food and Drug Administration (FDA) on January 22, 2016, issued "Postmarket Management of Cybersecurity in Medical Devices (Draft Guidance)." A can be found at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf. The guidance states that FDA views voluntary participation in an ISAO to be a "critical component of a medical device manufacturer's proactive post-market cybersecurity plan," and it strongly recommends that device manufacturers participate in a cybersecurity ISAO (Draft Guidance, pp. 7, 12).

The guidance also includes recommendations with regard to reporting actions taken by device manufacturers to address identified cybersecurity vulnerabilities. Generally, actions to address controlled risks will not require reporting under FDA's regulations, and FDA does not intend to enforce reporting requirements under 21 CFR part 806 if several conditions are met, one of them being that the manufacturer is a participating member of an ISAO.