MITRE TECHNICAL REPORT

The Role of a Framework of Legal Instruments in the Establishment of Effective International Regional Cyber Information Sharing

Considerations for Founders and Organizers

MICHAEL A. AISENBERG, ESQ.
International Operations
The MITRE Corporation
McLean, Virginia
October, 2012

ABSTRACT

This Report provides advice and direction to support the development of organizations, and capabilities within organizations for the collection and sharing of Cyber Information, especially information about threats, risks, vulnerabilities, attacks, as well as defenses to service disruptions, intrusions and other exploits against electronic information networks and other network-supported critical infrastructures.

The purpose of Cyber Information Sharing is to enable timely access to actionable information about ongoing cyber attacks, to permit present and potential targets to defend against and recover from exploits lodged against their critical networks.

The material addresses the initial phases of development of International Regional Cyber Information Sharing entities, and highlights key decisions which organizers face on the nature of the Information Sharing entity, associated necessary legal framework instruments, and their utility for particular aspects of an organization's expected activities.

The Report provides specific guidance to organizers - nations and other sponsoring parties - in the selection of an operating form for the Cyber Information Sharing entity, and provides a basis for decisions regarding the appropriate legal framework instruments to employ and the essential contents of those instruments, summarizing the characteristics and benefits of the various available instruments.

TABLE OF CONTENTS

I. Executive Summary

This Report is directed at a community of nations, organizations and industries engaged in the development and use of information and communications technology (ICT) to support national objectives, including defense, intelligence, government services, operation and management of critical civilian infrastructures and other commercial and industrial operations.

The Report is an element of documentation supporting a process being undertaken by MITRE to foster organizations or discrete capabilities within and among this audience for the specific purpose of enhancing the security and viability of these critical information technology networks and related assets. Once established, these new entities will support the cyber security objectives of sponsoring nations by making available to them timely actionable information regarding threats or imminent attacks against these networks. This process is widely referred to as cyber information sharing (CIS). Timeliness and actionability are the essential characteristics of "useful information" about "cyber threats".

This document supports the creation of these national organizations and mechanisms by enabling their establishment in a manner consistent with international legal requirements. Cyber information sharing is being conducted around the world in various organizational forms, including "Centers of Excellence", "Emergency Response Teams" or similarly styled "centers" as the operational home [locus/venue] of activities managing the exchange of "actionable" information regarding cyber threats, vulnerabilities, and actual attacks. Centers are hosted and sponsored through a variety of existing structures such as multinational bodies of governments on global, regional or local bases (United Nations, Asia-Pacific Economic Council, Gulf States Cooperation Council, Caribbean Basin Initiative, North American Free Trade Area), individual nation states (e.g., United States [U.S.] Computer Emergency Readiness Team [CERT]), entities based on agreements between sovereigns and resident industries (e.g., Abu Dhabi Security Information Center), or among industries within a single nation or group of nations (e.g., Financial Services [FS] Information Sharing and Analysis Center [ISAC]). Information Sharing Entities may be "permanent" with physical facilities, ad hoc, relying on sponsors' existing resources, or virtual, with no permanent home and operating with contributed resources from sponsoring participants.

Importantly, legal and policy frameworks support the legitimacy of organizations, and thereby sustain their longevity, especially those created by multiple nations. Frameworks define the scope of an entity's activities, criteria for participation, and specific roles of members. Framework documents can provide specific guidance on such matters as expected activities of the organization including detailed operational aspects of the organization. Framework documents frequently can provide for dispute resolution and other actions to sustain the viability of an organization.

This Report provides advice on the nature of framework instruments, their utility for particular aspects of an Information Sharing organization's expected activities, and selection of particular organizational form appropriate to various proposed courses of conduct. It is meant to guide nations and other sponsoring entities in the selection of an operating form for the Cyber Information Sharing entity, and to provide a basis for derivative decisions regarding the appropriate legal framework instruments to employ and the essential contents of those instruments.

The Report concludes by making several summary Recommendations to guide International Regional Cyber Information Sharing (IRCIS) Organizers, including one of overarching importance. In the development of a Cyber Information Sharing Activity, two decisions and two documents reflecting them are essential: organizers must determine what entities will be members of their IRCIS activity, and then execute an appropriate agreement setting out that agreement; organizers must also determine the form they wish the IRCIS activity to take from among several options, and develop operating rules that specify that form, as well as roles and responsibilities of participants.

II. Predicates for Cyber Information Sharing & the Creation of Regional Cyber Information Sharing Capabilities

It approaches "cliché" status to say that "without good information, there can be no effective defense against attacks against computer systems supporting critical infrastructures." The fact that this proposition is widely accepted by nations around the world is reflected in a broad range of documentation addressing national and international strategies to achieve secure cyber operating environments. U.S. national doctrine is among the most plentiful in this regard:

U.S. International Strategy for Cyberspace: International Development: "Provide the necessary knowledge, training and other resources to countries seeking to build technical and cyberspace capacity. Our goal is to help other states learn from our experience.to build cybersecurity into their national technical development." (May 2011)

Department of Defense Strategy for Operating in Cyberspace: STRATEGIC INITIATIVE 4 - Build robust relationships with U.S. allies and international partners to strengthen international cybersecurity. "Department of Defense (DoD) will work closely with its allies and international partners to develop shared warning capabilities, engage in capacity building, and conduct joint training activities. Engagement will create opportunities for sharing best practices." (July 2011)

*Department of Commerce Cybersecurity, Innovation and the Internet Economy: POLICY RECOMMENNDATION D1: "*The U.S. government should continue and increase its international collaboration and cooperation activities to promote cybersecurity policies"…. (June 2011)

Government Accountability Office (GAO) Briefing to Congressional Staff on the Comprehensive National Cyber Initiative, "Effective federal cybersecurity requires coordinated interaction with other nations. Sharing information for situational awareness – Exchanging information about recent attacks with other nations is critical…to understand vulnerabilities, attack methods, and other current and emerging trends…(and) for coordinating responses to international cyber incidents." (March 2010)

A U.S. Federal Advisory Committee, the President's National Security Telecommunications Advisory Committee, issued a *Report to the President on International Communications* operations in 2007 in which it both declared the critical importance of timely, actionable information sharing among the U.S. and its allies about cyber threats, exploits and attacks, as well as the essential role played by a legitimizing legal framework in establishing an entity to support information sharing.[1]

[1] NSTAC Report to the President on International Communications (Washington, D.C. 2007). http://www.ncs.gov/nstac/reports/2007/NSTAC%20International%20Report.pdf

A. Why Cyber Information Sharing?

The value of information sharing as a keystone element in a nation's cyber defense strategy may not be immediately evident in all of its dimensions. It may be obvious that when one of a government's systems comes under attack, information about the attack—its target, sources, vector and technical configuration are all, to the extent they can be known, valuable to both the mitigation of the damage of that attack and the defense of other systems against similar attacks. It may be less well understood that effective, managed information sharing can also, however, become the cornerstone of a larger evolution in posture of a nation's critical ICT assets, predicated not only in "sound security" but in an active, agile, and even aggressive defensive posture which by its very existence, deters attacks by adversaries, resists attacks when they *are* made, contributes to prompt system recovery and restoration of services, and even supports the evolution of networks to withstand unprecedented attack forms.

It should come as no surprise, therefore, to those who are responsible for maintaining the security and operational integrity of information technology assets that the growing emphasis on Computer Network Defense (CND) for National Security and Intelligence Community information technology assets and operations has a place in the larger Critical Infrastructure information technology community, as an emerging element of the core architecture for *any* secure ICT system.

In the past "computer network defense" was limited in scope to its role as an element of "Computer Network Operations" (CNO), a label applied to a suite of electronic information warfare activities. Over time, it has become evident that in order to be effective and reliable (including as a platform for CNO), a range of defensive and protective security measures and practices, well beyond those implicated in historical CND capabilities such as intrusion detection and perimeter defenses, are not only important, but essential. Robust Cyber Information Sharing capabilities are a critical component of that expanded "CND". The benefits of such practices as continuous network monitoring and capture and analysis of attack data and forensics are becoming understood and accepted across the wider critical infrastructure network community.

While it goes without saying, therefore, that governments will seek to assure the utmost in CND capabilities for their national security and military networks, an important additional emerging opportunity offered by this new-found emphasis on CND as a capability for military and related national security secure networks is to incorporate CND practices and components into networks supporting all critical infrastructures, including civilian government, surface, air and maritime transportation, financial services, telecommunications, water, energy and power.

And, as a keystone element of CND, robust information sharing regarding threats, vulnerabilities, attempted attacks and actual attacks against national networks can become the spearhead to enhanced CND, and by extension, the capacity to conduct computer network operations when confronted by an adversary.

The following table compares CND measures and capabilities as required by DoD directives in 2001 to those required by DoD documentation in 2011 and later:

2001 Department of Defense CND capabilities[2]	***2012 DOD definition: Agile CND[3]***
Network Monitoring	← 2001 Measures, PLUS…
Protective measures	Deploy secure systems [configuration to secure specifications, secure component acquisition]
Situational awareness	Vulnerability assessment
Training	System-wide risk assessment
Configuration response to threat	Incident response process
Capture and secure traffic	Develop, manage, operate catalog of known malware/signatures and other APT vectors
Intrusion detection	Manage risk mitigation, dictated by vulnerability assessment

For those nations and their critical infrastructure communities who choose to deploy it, the establishment of CIS capability can become a useful mechanism in in the achievement of a best-in-breed secure network environment, which, when appropriately configured, may be relied on for the most sensitive applications and the transmission of highly confidential data across all sectors of an economy. This capability may serve such national interests as supporting a stabile investment environment, reliable allocation of technological and other resources, awareness and warning of threats against national infrastructures and institutions and general stability.

[2] DoD Directive O-8530.1 (January, 2001)

[3] CJCSI 6510.01F (February, 2011)

III. Purpose of Report

The purpose of this Report is to facilitate the establishment of CIS organizations outside of the U.S., by nations, groups of nations, international organizations, industry groups or combinations of them, by providing clear advice about the necessary elements of a sufficient legal framework to support CIS an activity. The guidance may also be useful to entities within the United states seeking to establish a CIS capability, such as sub-Federal government institutions, tribal organizations and Non-governmental communities of interest maintaining information networks.

This Report documents key components and considerations in defining, negotiating, creating and executing the essential elements of the legal and policy framework supporting CIS organizations and entities (Information Sharing Organizations [ISOs] or Information Sharing Environments [ISEs]). When organized internationally, these may be referred to as International Regional Cyber Information Sharing ("IRCIS") activities. These organizations are established to define and observe evolving threats to electronic information infrastructures supporting government operations and essential economic activity of nations, defend against these threats, document attacks against infrastructure assets, conduct research on appropriate defenses and share information about threats, attacks defenses and remediation.

Cyber Information Sharing organizations exist and may be organized in various forms and structure, and include organizations established:

- by/within a single national government,
- among several governments directly,
- among governments through existing or dedicated multinational bodies,
- between government and industry, such as national critical infrastructure representatives,
- with peer non-government entities and or industry across national borders, organizing directly,
- as above, but through an organizational surrogate created for the specific purpose, or
- by and among affected industry and non-government organizations (NGOs).

This Report has been prepared as a foundational element in the development of a program by MITRE under its International Operations directorate directorate to utilize MITRE's unique expertise to foster CIS activities on a global basis. This program relies on MITRE's expertise in systems engineering supporting Cyber Security objectives of itself (The MITRE Corporation), the U.S. government and its allies, including MITRE's legacy of high-level involvement in the support of national and economic security concerns arising from threats to critical cyber infrastructures supporting national defense, intelligence operations, civilian government operations including national revenue, air space management and transportation security, and law enforcement.

The Report documents the following:

- Define the scope and key elements comprising an IRCIS "legal framework"
- Identify and validate the elements of existing legal frameworks providing authority and precedent for IRCIS programs
- Associate existing information sharing arrangements with authority types
- Identify opportunities for additional framework elements consistent with scope and mission of existing and planned information sharing organizations
- Propose Cyber Information Sharing enabling mechanisms where gaps exists
- Define Essential steps in forming a Cyber Information Sharing Entity, reflecting the preceding considerations [4]

[4] The essential steps are detailed in Section VII (F).

IV. Elements of Legal Frameworks for IRCIS entities

A. Functions of Legal Framework Elements in General

Any functioning entity—nation state, government agency, business organization, or association of entities—requires an articulation of certain common elements in order to remain viable. These elements typically include, at a minimum, statements of the objectives and activities of the entity and selection and duties of leadership/management. For nations, these are often expressed in a Constitution; for business and membership organizations, in "Articles of Incorporation" or "charter". Many more elements, of course, make up complex governance frameworks of a nation state: bodies of statutes, regulations, treaties, compacts, to name the most common. Business and voluntary entities may have By-laws, operating rules, concept-of-operations, contracts and other evidence of relationships dictating or constraining their operational activities.

Two primary benefits—and thus, purposes—accrue to entities by having a coherent, documented legal framework: the first is its legitimization in the international community; the second is a framework's function in supporting institutions' operational reliability and consistency. Creating conforming practices based on a documented framework also supports institutional expansion or replication and aids in dispute resolution.

These practical consequences derive from at least seven identifiable functional elements and associated benefits, which are often present in the several varieties of instruments comprising legal frameworks for information sharing organizations.

These essential elements and associated benefits, which are discussed in greater detail in Section (C) below, are:

- **Legitimization** of the entity as seen from external communities: by utilizing recognized legal instruments, such as treaties, Memoranda of Understanding (MoUs), or Diplomatic Letters.

- **Characterization**, defining the roles, responsibilities and relationships between participants: as treaty partners, contracting parties (nations, NGOs or any other parties to an instrument), "members" of an entity, donor-recipient, parent-subsidiary, or entity-affiliate.

- **Scope,** defining permissible types of Participating/Affiliating entities with the information sharing organization: nation states, groups of nations, non-governmental organizations, commercial entities, individuals, "statutory" persons, or combinations of these.

- **Defining the Structure** of the information sharing organization: Treaty-defined government activity (operating as "watch-and-warning" centers, CERT, information sharing and analysis centers [ISAC] or similar forms); multilateral government organization, bi-lateral government organization, undefined aggregation of nations, criteria-based organization consisting of selected nation-states; commercial affiliates of any of the foregoing; blended government-and-industry "public-private partnerships"; Academic-affiliates, such as institutional "Centers of Excellence".

- Specifying **Governance** Elements for the entity: Detailing of essential operating rules and any source authority (law, regulation, proclamation or similar); Entity-specific governance instruments (Articles, Charter, by-laws); Management model (Concept of Operations, Operating Rules).

- Defining **Financial Models** for establishment and operation of the entity: defining eligible, available or potential modes and sources of financial support (National grants, fees/"dues" from participating member states/entities, fees from delivery of services); also may define Prohibited Sources of funding (e.g., Individuals, corporations, foreign entities could be identified as inappropriate sources of funding).

- Providing **Operational Guidance** for the conduct of the entity's activities: Operating Rules or Concept of Operations providing detailed statements addressing Mission, Purpose, Management, Participants, Facilities and Resources, Conduct of Operational Activities, Performance Assessment, Milestones, Planning. Depending on the general legal framework of a nation or institutional environment, much more granular and specific operating detail, such as standards and practices, permissions and prohibitions and party roles and responsibilities may be set out in the materials.

B. Role of Framework Elements in Enabling Information Sharing Activities

In certain instances the legal framework instruments which support existing CIS Organizations and activities are largely a reflection of the preexisting situations and environments within which these organizations have evolved, rather than functionally related to their intended Cyber Security activities.

Existing (or in a few instances, now-abandoned) CIS organizations include those organized:

- by individual or among several nations,
- **by groups of nations** or existing international or multi-lateral organizations,
- national capabilities, established at the **national government level** or by individual agencies of a nation,
- capabilities organized by **industry sectors, university and research institutions or other NGOs**, and
- **hybrids** of these, comprised of both government and non-government entities.

[see Appendix 1: **Table of Organizations Hosting/Sponsoring Cyber Information Sharing Activity**]

Several organizational modes of Information Sharing activity operate under now-familiar structures, such as "Centers of Excellence" and "CERTs" (cyber emergency response teams). These will be discussed from an operational perspective.

Arrangements for the sharing by and among nation-states by agencies of government (departments, ministries or similar government agencies) are explicitly "state action." Information sharing by subordinate organizations acting under delegated authority from an agency of government are often performing governmental or "state functions", either by delegation or by individual operating charter. When organized or operated by private sector entities, ISEs may require further specific clarification in a framework instrument of their relationship to the government.

1. INTERNATIONAL/MULTILATERAL ORGANIZATIONS

International Information Sharing capabilities organized by international multilateral organizations may conduct their activities under treaties, pendant agreements or MoUs among contracting parties to a Treaty, or where no treaty exists, multi-nation exchanges of diplomatic letters.

Examples of existing and extinct Multilateral Organizations which have/had Cyber Information Sharing as a major function:	**Organized under**
EU Information Observatory (1989-1997):	
EU European Network Information Security Agency (ENISA)	EU Charter
INTERPOL/G-8: U.S. Department of Justice (DoJ) G-8 IS Activity. U.S. DoJ: Criminal Division/CCIPS (Created TO TAKE ADVANTAGE OF Center of Excellence (CoE) Cybercrime Convention)	Multilateral treaty CoE CCC
North Atlantic Treaty Organization NATO Cyber CoE (CCD COE) Tallinn, Estonia	
ITU CENTER Kuala Lumpur, Malaysia (U.N. affiliate)	ITU Charter

2. NATIONAL INFORMATION SHARING UNDERTAKINGS

Information sharing across national borders has also increasingly been the mission of national Cyber watch and warning activities, organized by industry organizations, individual or inter-agency government processes or hybrids of both non-government and government entities. Examples of these organizations (both U.S.-hosted and non-U.S.) are in the following table:

Examples of existing national CIS Capabilities	
Entity	Authority
U.S.CERT Department of Homeland Security (DHS)	Regulation pursuant to HSPD-7 and Homeland Security Act of 2003
UAE ASICS [successor to aeCERT]	United Arab Emirates

3. Industry and NGO Originated Information Sharing

In the U.S., the earliest examples of ISEs were those organized by industry sectors. At least two of these, in the electric power (ES-ISAC) and telecommunications industry sectors (the National Coordinating Center of the National Communications System [NCC] established by Executive Order 12472), predate the 1998-2001 period during which most of the other ISACs were established. Both of these ISACs have, like their peers in other sectors, evolved into "partnerships" with government agencies, and have been the beneficiaries of several statutory and regulatory initiatives both confirming their legitimacy and defining the scope of some of their activities.

[Of note, even though the Telecommunications NCC was established by Executive Order, all of its participating "resident" members are private corporations. Until 2009, the NCC was collocated near the Pentagon with the DoD Joint Task Force-Global

Network Operations (JTF-GNO) military watch-and-warning center. At that time, the JTF-GNO was moved to Ft. Meade, Md. at the new U.S. Cyber Command Headquarters, while the NCC was moved to new facilities at DHS, collocated with the reestablished US CERT.]

With the issuing of PDD-63 by U.S. President Bill Clinton following the 1998 Report of the President's Commission on Critical Infrastructure Protection (*Critical Foundations),* organizations defined as "information sharing and analysis centers" (ISAC) were launched in at least seven of 11 identified "critical infrastructure" sectors of the U.S. economy. (The seven sectors are: electric power, telecommunications, information technologies, chemicals, water, surface transportation, financial services).

As of this writing, more than 20 ISACs exist, all with the stated purpose of performing watch-and-warning activities of the networks supporting the companies in these sectors, and sharing information on a peer-to-peer basis with other members of the sector, often through sector Security or Network Operations Center "hubs" (SOCs, or NOCs) as well as with government agencies, which will also share relevant threat, attack and defense information.

Examples of existing Industry and NGO Information Sharing Capabilities	
Entity	Authority
Electric Sector ISAC an affiliate of NERC	§214 of Homeland Security Act
National Coordinating Center (NCC)	EO 12472; PDD 63; §214 of H/S Act
IT ISAC	PDD-63; §214 of H/S Act
FS ISAC (c/o VeriSign, Inc., Sterling, Va.)	PDD-63; §214 of H/S Act

4. HYBRID ISEs

Closely related to the ISAC form of ISE are non-government CERTs, which may invite participation or receive other direct government support. The first U.S. CERT was established as a contractor with U.S. Federal government agencies by the Software Engineering Institute of Carnegie-Mellon University in Pittsburgh, Pennsylvania. Although no longer a defense contractor, CERT/CC continues to have an influential role in research about cyber threats, defenses and resilient network architecture. It also continues to have an influential role in the overall U.S. Cyber environment, in part due to its affiliation with a major University computer engineering department.

Examples of Hybrid Information Sharing Capabilities	
CERT/CC (Carnegie-Mellon) CERT/CC Pittsburgh, U.S.A.	Carnegie-Mellon University, SRI, U.S. Department of Justice
Advanced Cyber Security Center Bedford, Mass.	Insight Global Partnerships, MITRE Corp., U.S.Governement.

C. Seven attributes/benefits from legal framework formalization

There are significant benefits which will accrue to the Cyber ISE as a result of adopting a formal framework under recognized legal authority. But among these, two are of primary importance to the on-going operation of the ISE: first, legal frameworks support the ISE's **legitimization in the international community**; second, frameworks function in **supporting institutions' operational reliability and consistency**. These measures will support the effectiveness, credibility and longevity of the entity.

a) Legitimization

Legitimization as used in this context refers to a process, including specific acts of legal formality which **define the basis and authority of organizers to establish the ISE.** Operational watch, warning, analysis and information sharing activities addressing "cyber" assets in the commercial, civilian government and national security environments frequently directly manage and hold data regarding sensitive matters of national importance, including national security-defense-intelligence and economic security. Each of these are of sufficient importance that they establish conditions under which governments will normally seek to support an activity such as an ISE with the formality of a legislative act or similar action denoting the imprimatur of national authority.

Because ISEs and similar sharing structures frequently operate in the international community and engage in activities of notoriety, public and peer-state attention and potential media scrutiny, the resolution of any question of their *authority* to operate is an important precursor to effective operation. In the case of IRCIS entities established exclusively as a government function, such a concern is readily addressed by a simple act of the national authority, whether by a statute, regulation or declaration of the national executive or a delegated agency.

For entities comprised principally or exclusively of non-governmental organizations or commercial entities, formal legitimization process may consist of two steps.

First, the "authorization" and recognition of the entity by an act of government; for example, the national executive may issue a proclamation authorizing the establishment of CIS entities among industry and other non-governmental organizations. Or, the nation may have entered into a treaty arrangement which contemplates the creation of local, national CIS activities, and consistent with that

treaty commitment, the national government may issue a proclamation/executive order, or may seek passage of an authorizing statute by the legislature, or may have a coordinating or "hosting" agency of government issue a regulation specifying the scope of its support for a private sector Information Sharing capability.

Second, the entity itself will establish, through an agreement among its participating organizations, and may seek more formalization, such as through incorporations a "statutory entity". The IRCIS entity will then also develop its own operating rules. These steps are explained more fully in Section (b) below and following.

Of course, nothing in the inherent nature of the CIS form or purpose would prohibit a private organization from taking ONLY this second step and self-declaring its CIS activity and "self organizing." Large multinational NGOs may choose to proceed in this manner. The absence of pre-cursor governmental recognition may suggest the incorporation of a media strategy to declare the existence of the CIS role; on the other hand, in sensitive sectors or those seeking to deflect attention from existing vulnerabilities, this media attention may be unwelcome.

b) Characterization

The organizing documents of an Information Sharing Entity will, in addition to the formal document establishing the entity (whether international agreement, statute or other foundational framework element), normally include more detailed chartering documents, by-laws, contracts or similar materials with more granular definitions of key roles and responsibilities, and relationships between ISE participants. Depending on the structure and establishing authority, elements of these matters may be allocated between the formal authorizing documents and collateral materials.

The designations of ISE participants will typically include:

- *"contracting parties" or "treaty partners"* *(nations in multilateral ISEs)*
- *"members"* *(of any ISE entity)*
- *"donor" or "recipient"* *(of ISE assets/resources)*
- *"corporate parent- or subsidiary"*
- *"Entity-affiliate"*
- *"contracting parties"* *(commercial ISE participants)*

These characterizations of the nature of the entity, participating members and their roles and responsibilities, while flexible, are essential elements of the ISE's operating posture and care should be taken with their selection and expression in instruments and correspondence.

c) Scope of membership; organizational types

Organizing legal framework documents will also **define the permissible member organizations and types of entities participating in the IS organization**: individual nation states, organized pairs or groups of nations, sub-national governmental entities (such as municipalities or other "inferior" jurisdictions)[5], non-governmental organizations, commercial entities, individuals, "statutory" persons, or combinations of these.

Permissible participants will normally be defined in the highest level instrument. For multi-lateral governmental organizations, this will be the treaty or other international agreement; for national ISEs, the national statute, regulation, proclamation or other authorizing measure will specify permissible participants. Non-governmental organizations' participants will be defined in the chartering document: Charter, Articles of organization or incorporation, and may be elaborated in by-laws or similar procedural framework documents.

d) Structure

Along with defining "who" may participate in an ISE, the framework documents, with similar levels of formality, will **specify the structure and operating conditions of the IRCIS entity.** These will span the spectrum from formal multilateral governmental organization and other treaty-defined government activities, ad hoc multilateral government organizations established by sub-treaty agreement, bi-lateral government organization established under a treaty or "inferior" bilateral instrument (such as a MoU, or an exchange of diplomatic letters), an undefined aggregation of nations established by similar non-treaty agreement, and criteria-based organizations consisting of selected nation-states, corporations, universities or other entities.

An IRCIS entity need not be a "new" organization; its creation, and its organizing documents may simply provide for the undertaking of new responsibilities by an existing organization. Especially among ISEs comprised principally of non-governmental bodies, agreements could either establish a dedicated IRCIS entity or **designate an existing entity** among commercial affiliates of any of the foregoing groups of nations (such as national business organizations like Chambers of Commerce); blended government-and-industry "public-private partnerships"; and Academic-affiliates, such as institutional "Centers of Excellence" any of which may have their organization and structure defined in a less-formal instrument, including MoUs, contract or exchange of letters. Indeed, it is entirely possible for an IRCIS organization to be established by oral agreement, memorialized by as informal an "instrument" as a press release.

[5] "Inferior" here refers to non-national political subdivisions, such as provinces, counties, territories, protectorates, municipalities, tax or water districts, or "states" in the U.S.

However, given the keystone purposes of legitimization and functional credibility, as discussed above in sub-section (a) of this section; the more formal the instrument establishing the ISE, the greater the prospect of gaining these important benefits. The fact that scope, structure or other attributes *may* be set out in informal or "inferior" documents should not deter organizers from utilizing the most authoritative instruments available for each expression of organizational and operational considerations.

e) Governance of entity

Another key role for legal framework documentation is to **specify the governance elements for the entity.** Governance elements include matters such as management, leadership, decision-making, delegation of specific authority, and interaction with stakeholders or other external groups such as public bodies or the media. In addition, governance language may also establish financial structures for the entity (see sub section f), Finance, below). These functions are closely linked to specific operating procedures and practices, as discussed in Section g*), below.*

Governance documents will often be subordinate documents to the primary organizing instrument (such as "by-laws" subordinate to a statute or charter), and may also include specification of any other essential operating rules (and any source or delegation of these) in other external authorities (treaties or statutes). Governance documents take many forms, including Entity-specific governance instruments (Articles, Charter, by-laws); management models such as capability maturity documentation or even less traditional documents such as Operating Rules or "Concept of Operations" and other organizational artifacts.

The inherent legitimacy of an ISE is more dependent on the degree of deference accorded by participating entities than the particular type of document in which governance terms are specified. The fact that some specification of governance exists and is followed by the members, is of more importance to the viability of the information sharing organization than any specific type of instrument.

f) Finance

A range of financial issues will face any organization operating as an ISE, whether as a multilateral body, an agency of government or an independent body. The viability of the ISE is dependent on sustaining financial support more than any other operating condition. As a result, clear articulation of the sources of necessary and permissible financing is essential. Whether in the original authorizing documentation, governance documentation or a separate financial instrument, an articulation of financial model for the entity is an essential element of the legal framework. Financial documentation should also **define sources of funds necessary for the establishment and continuing operation of the entity: in particular, it should define eligible or**

permissible, available or potential modes and sources of financial support (National grants, fees/"dues" from participating member states/entities, fees from delivery of services), the entity budgeting process and the consequences of deficiencies (e.g.—entitlement to borrow funds, what constitutes insolvency of the entity).

g) Operating Procedures

The legal framework is also the basis for defining the operating procedures and conditions for the ISE. Whether in charter, by-laws or separately stated operating manual, operating rules, concept of operations or similar documentation, providing Operational Guidance for the conduct of the entity's activities is the seventh and most familiar aspect of the legal framework.

Operational Guidance will allocate roles and responsibilities of participants, staff and other affiliates, and **define continuing, daily and other recurring periodic operational activities, and may restate considerations expressed in a more general form in other Legal framework elements.** Whether in a Concept of Operations, Operating Rules or other instrument, clear documentation providing detailed statements addressing Mission, Purpose, Management, Participants, Facilities and Resources, Conduct of Operational Activities, Performance Assessment, Milestones, Planning, Budget, Staff, Duties and Critical Functions will support the day-to-day operations in a manner contributing to the legitimacy and credibility of the ISE.

V. Overview of Legal framework instruments supporting Cyber ISEs

A. Formal national legal instruments

1. Treaties

Treaties are international agreements entered into by sovereign states expressing obligations of behavior to which they intend to be bound. Treaties are of several discrete scopes:

- **Bilateral treaties:** between two countries, typically expressing mutual obligations and undertakings, such as national recognition and the exchange of diplomats, the conduct of commerce, the recognition of borders, mutual military assistance, treatment of nationals, extradition of criminals, and aviation and navigation.

- **Plurilateral treaties:** between and among groups of more than two nations, frequently within a discrete geographic region, or of a linguistic or other historically significant relationship, and frequently limited to one specific topic, such as military assistance, commerce and trade. Examples include the Gulf States Cooperation Council and the North Atlantic Treaty of 1949 (establishing NATO)

- **Multilateral treaties:** between and among larger groups of nations with a common purpose. Frequently multilateral treaties are used to convene the existence of an organization (The Treaty of Rome establishing the European Common Market; its successor, the Maastricht Treaty, refining the obligations of the members of the European Union), or of a specific subject matter (The Berne Convention on Copyright; the Budapest Agreement or Council of Europe Convention on Cybercrime).

Among the features of Multilateral Treaties, which distinguish them from other non-binding multilateral instruments, are their explicit specification of intent to be bound **(enforceability)** and frequently, a **specification of an authority** or venue for dispute resolution (such as the International Court in Den Hague).

Among the dozens of subject-specific multilateral treaties to which the U.S. is a party, are these examples below:

1963 - Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water

1967 - Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies

1968 - Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space

1973 - Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (1971);

2004 Budapest Convention on Cybercrime

The parties to *all* formal treaties are typically referred to as "contracting" parties, expressing at least a notional intent that the commitments embodied are meant to be binding and enforceable through some mutually agreed mechanism.

The only multinational Cyber Information Sharing activity presently authorized by a multilateral treaty instrument is the ENISA, which is undertaken by the Member States of the European Union pursuant to a specific EU Regulation authorized by the Maastricht Treaty amendments to the Treaty of Rome (ENISA Regulation of 2004).

a) Multilateral instruments

Closely related to multilateral treaties but lacking in expressions of an intent to be bound (and thus, more aspirational than representative of a true "contractual" commitment) are multilateral instruments. Such agreements became more common during the Cold War, as successions of national governments sought to demonstrate their efforts at international diplomacy by entering into "agreements" truly only aspirational in nature, permitting their renunciation with little or no penalty other than a reputational one.

Non-treaty bilateral instruments also serve as a fallback artifact when true treaty negotiations over complex controversial issues, such as disarmament or neutralization of combatants, fail to reach a level of agreement capable of being embodied in a binding treaty instrument.

Examples of such non-treaty bi- and multilateral instruments include the 1975 Helsinki Accords on nuclear disarmament and the Dayton Accords ending the Balkans conflicts.

b) Bilateral treaties

As the name implies, bilateral treaties are agreements between two nations. By far, these are the most common form of international legal instruments of the pre-Modern

era (prior to World War I), and have existed for many centuries as the means by which nations recognize each other's existence, boundaries, territorial waters, colonial/administrative territorial claims, and each other's legal documentation, such as passports and visas, exchange diplomats, authorize trade, permit tourism and otherwise define their mutual participation in the community of nations.

Historically, the most common form of U.S. bilateral treaty is a Treaty of "Friendship, Commerce and Navigation" (FCN) or "Peace, Friendship, Commerce and Navigation". The U.S. has such treaties with over 100 nations. Among those nations with which the U.S. does not have a FCN Treaty, the next most common form of agreement is a treaty of Reciprocal Investment, by which each signatory recognizes the value of each other's currency to permit an exchange rate to be established and commerce to be conducted.

In general, since World War I and the Treaty of Versailles, most large nations have accomplished their recognition of each other's right to exist, territorial limits and boundaries, and conduct other specific acts through multilateral instruments addressing specific topics (see multilateral treaty topic, below).

(1) Use of Bilateral Treaty to Establish IRCIS

When an existing bilateral treaty is sought to be used by two nations to express a new common purpose, an amendment is normally required. Since the architecture of these treaties pre-dates not only the Internet and electronic networks, but even such modern phenomena as aviation, if incorporation of a modern concept is contemplated, such as authorization of a bilateral Information Sharing Entity as an IRCIS or similar entity, their form normally requires an explicit modernization, through:

(a) a formal amendment (uncommon, lengthy, and frequently as complex as original agreement),

(b) adoption of a "protocol", embodying new language reflecting a new agreement, but which frequently is less complex than an original treaty, or

(c) and oral amendment through a "process-verbal" where the change is deemed consistent with an existing provision, which requires only clarification to express the mutual agreement of the parties. (An example would be a treaty with an existing "Information Sharing" process addressing natural disasters, whose purpose is explicitly expanded to include information sharing about Cyber threats.

c) Other bilateral agreements

In some instances, the process of negotiating a treaty may take many years (even decades); the negotiations leading to the 1979 Camp David Accords on the Middle

East are an example. In some instances, prior to reaching an agreement on the terms of a treaty, negotiating states will seek to memorialize the scope of agreements already reached in an "exchange of notes", "diplomatic letter" or other instruments. While these may lack the formality of a treaty, their sufficiency is reflected in the parties' behavior subsequent to their execution. If the two states behave as if they intended to have an agreement, they may be said to have an agreement.

An example of such a bilateral exchange is the material exchanged between President John Kennedy and Soviet Premier Nikita Khrushchev during the course of their meetings prior to the conclusion of the 1963 Nuclear Test Ban Treaty. The "Kennedy-Khrushchev Exchanges" as they are known, embody a variety of commitments following the Cuban Missile Crisis and prior to the execution of the 1963 above-ground Nuclear Test ban. See Kennedy-Khrushchev Exchanges at the Yale University International Law "Avalon Project".

The existence of these "less than treaty" bilateral agreements is important for the Cyber ISE exercise, because the narrow specific purpose of establishing an entity may place it beyond the capacity of the diplomatic community of a small nation. An overly complex process to establish Cyber ISEs may work against the ultimate purpose of the effort and would be counterproductive.

As a general principal, once a commitment among negotiating parties is reached, only such instrumental formalities as are required to embody their intent and bind their participation should be employed.

2. Memoranda of Understanding (MoUs)

Memoranda of Understanding or Agreement (MoU or MoA) are informal instruments which, when utilized by nation states may have similar, though less formal stature and effect in binding parties to their respective commitments as treaty agreements, without the extensive negotiating process or enforcement mechanisms. They are particularly suitable where the subject matter of the agreement has a finite period of existence.

MoUs are frequently employed to document subordinate or derivative activities and agreements between nations which are parties to treaties, and frequently document specific commitments to be executed by peer agencies of the nations' governments. These are typical of nations which have existing close relationships and are in a continuing array of relationships, which may include military and other national security collaborations, and where explicit documentation of subordinate agreements is helpful to maintaining clear allocation of roles and responsibilities of each party in varying operating environments.

The suitability of the MoU to the creation of a Cyber ISE between two or more nations is readily apparent; it is also particularly suitable as the formalizing instrument for associations between nations and non-governmental entities, such as NGOs, industry

groups and or individual business organizations. See additional discussion at Section VII (C) regarding Alternate instruments.

MoUs are particularly familiar as the vehicle for specification of subordinate, non-treaty operating agreements between U.S. national security interests (DoD and subordinate entities) and the defense ministries of NATO partner states. The MoU defining the scope of cyber collaboration between the U.S. DoD and the U.K. Ministry of Defense (MoD) as the "Contact Group" is an example of such a bilateral MoU. MoUs are also frequently utilized in defining relationships between agencies of the U.S. government, such as the Cyber Security collaboration MoU between DHS Infrastructure Protection Directorate, the National Security Agency (NSA) and DoD Cyber Command.

3. Statutes, Proclamations and Regulations: "National" Instruments

This Report addresses IRICIS organizations which are presumed to be concerned with participants' sharing information internationally, across national boarders. In fact, a significant portion of Information Sharing presently engaged in occurs within single countries, between institutions which observe attacks and attempts at intrusion into networks and then share information, warnings, analyses and defenses with other partner institutions and agencies of government.

Entities organized under such authority include national government "Cyber Centers of Excellence" , university-hosted "Academic Centers of Excellence" and industry organized ISACs.

When organized entirely within a single nation, whether as an agency of government or as a private sector or NGO activity, the enabling legal framework element may be a national or even local government action: a statute, a proclamation or similar statement by the national executive (Executive Order in the U.S.) or a regulation issued by an agency of government under delegated authority.

Indeed, under some nation's constitutional or other authority for international and foreign affairs, even though the head of government or head of state may have entered into a treaty arrangement with one or more other nations, a national action, such as ratification of the treaty language by the national legislative body may be required. It is not uncommon in such circumstances for the legislative body to also consider enabling and conforming statutes which bring the nation's body of laws into conformity with the commitments made to third countries in a treaty instrument.

4. Articles of Incorporation and Charters

When CIS activities are organized outside of government, either by NGOs or by commercial companies or their surrogates (such as trade associations) they may

choose to organize in a manner consistent with their commercial identity. Normally, this can be done more easily and efficiently by becoming "incorporated" or "chartered" under the laws of the jurisdiction in which the CIS entity will operate.

Formation of a legal entity provides the organizers with a level of formality equivalent to that provided to nations by a treaty or statute and contributes both to legitimacy and credibility.

Where the entity is established by incorporation or grant of a "charter", the development of an operating rules instrument, whether styled as by-laws, operating rules or other type is an essential element of binding all parties to a common set of practices, and the preservation of consistency, upon which credibility of products and shared data may depend.

5. Contracts and other non-governmental instruments

Where the creation of a formal legal "person" through incorporation is not desirable, combinations of entities may choose to establish their CIS program through a contract or other enforceable legal instrument.

B. Informal arrangements

There may be any number of reasons why the "formalities" of a government-sourced legal instrument are inappropriate for the creation of an Information Sharing entity; the most obvious is the absence of any government role in the IRCIS entity. Even if the creation of IRCIS structures is authorized by a statute or other government action, the make-up of the entity's membership may be entirely non-government organizations, and reliance on government action may be either unnecessary, inappropriate or both. [6]

The IRCIS entity may in fact be developed entirely from non-government efforts, and only choose to share information voluntarily with agencies of government

On the other hand, there may also be situations, because of the nature of the government organizations affiliating with an IRCIS entity that the visibility associated with some forms of framework document development, such as the negotiation and

[6] It should be noted, however, in making such a determination, what the important value of the "imprimatur" of official sanction and delegation of authority may be to the credibility and viability of the IRCIS entity. Even if not "required" some visible government action may be beneficial as part of the development of the legal framework. Indeed, this could evolve the "two part" process of legitimization and operation into a three part process for certain entities, where an action of government "authorizes" the creation of the IRCIS entity, a formal action, such as incorporation "creates" the entity, and the development of an operating document (charter, by-laws) defines the structure, governance and operations of the entity. See discussion of "Legitimization" at IV (C) (a) above.

execution of a treaty among nations, or the passage of a domestic statute through the legislative bodies is not desirable.

In these later situations, a less formal process and legal artifact may be desirable. There is NO inherent reason that a letter or informal "Memorandum" among nations, or between nations and non-governmental entities, or a simple contract or exchange of letter among industrial and other non-government organizations will not accomplish what a treaty, statute or the creation of a "statutory person" through incorporation would otherwise accomplish.

1. Memorialization

The essential feature of less formal means of establishing an IRCIS organization is that, irrespective of its lesser apparent "formality" when compared to a treaty or statute, the instrument/document serves as a memorialization, as a tangible evidence of the intentions of the party to define and commit to the creation of an entity.

There are most certainly differences in complexity and in specific attributes between official action of a nation and exchanges of letters among corporations. Treaties in all likelihood will have specific dispute resolution provisions; these may be incorporated in a multi-national MoU or exchange of letters as well. Statutes may have delegations of authority to individual agencies of government, both participants in an IRCIS and others, perhaps sharing information with an IRCIS entity. But, any provision which typically is part of a "formal" instrument" may be included in a less formal instrument.

VI. Examination of Specific CIS Arrangements

A. Models/capabilities of information sharing

Once the decisions are made by the parties to the ISE regarding the operating form and an instrument is chosen to memorialize the agreement-in-principal, the other essential task in creating the ISE's legal framework remains; that is selecting the operating model and practices of the organization and creating a document or documents to reflect those decisions.

These decisions are essential, and **must be made early in the framework process,** since in some instances, options as to affiliation will be foreclosed by choice of form, or forms may be foreclosed by choice of first-order instrument.

For example, if a determination is made to operate the ISE as a "Center of Excellence" house in a national university, existing limitations on the scope of activities of the university may limit to scope of activity of the ISE. If, for example, the university may not contract with commercial for-profit businesses for professional services (i.e., all of its faculty must be employees of the university—a not-uncommon restriction among government-sponsored universities) then taking advantage of collaborations with existing Cyber industry organizations may be difficult. To avoid such a restriction, a "Center of Excellence" may best be sponsored by an agency of government or a new entity created for the purpose, which may invite the participation of academic subject matter experts.

Thus, it is essential to define who the participants in the ISE are expected to be, and what other entities the ISE will seek to affiliate to accomplish its stated objectives. *Both* the *form* and the *instruments* must be carefully chosen.

1. Generic Capabilities: Statement of Purpose

Whether relying on an existing entity and existing authority to launch an IRCIS activity, or whether following a full development program with the creation of a new legal framework including authority and operating rule instruments, one common unifying factor will exist across all ICRIS activities. That is, the primary artifact of any IRCIS activity will be information about threats, attacks, exploits and other "insults" to networks supporting critical infrastructures.

It is essential to bear this in mind during the organizational formation process; frequently, "standard" form documentation for the execution of Articles of Incorporation, by-laws and other framework instruments require the specification of the "purpose" of the entity being evolved. A concise statement reflecting the cyber information sharing purpose should be developed.

2. Information Sharing Capability within existing entity (government agency or private entity)

Some practices associated with Information Sharing will typically require no new authority and may be engaged in by any entity.

a) Incident reporting: Receiver only

The most basic Information Sharing action is also an illustration of the most basic approach to controlling information produced by the staff or members of an IRCIS entity. It is the passive reception of the work product of an IRCIS entity. Being a recipient of unrestricted information should normally pose no special requirements if no further action is normally to be taken by recipient organizations.

b) Incident reporting: Receiver/disseminator

If the information carries redistribution or other use restrictions, then some means of assuring compliance with those restrictions is necessary and the concept of associate or affiliate membership serves the purpose of creating a basis for the IRCIS entity to enforce the restriction on redistribution or other limitation on the use of the information. The authority to redistribute IRCIS-generated data may require not only proper status as an affiliate of the IRCIS, but, especially for agencies of government, specific authority to act as a source of such information being distributed to its own further network of recipients. Of course, such redistribution should be properly authorized by the governance documents of the IRCIS organization.

c) New capability/government: amending existing authority

Frequently, the very novelty of the issue of cyber security, as well as of the act of information sharing will mean that the entity hosting the IRCIS capability will not have previously engaged in the various activities associated with the function, whether as a primary sponsoring or hosting agency for the IRCIS or simply as a participating member.

Not only will the entity require developing the legal framework instruments associated with the IRCIS, but its own authorizing structure—whether statute, regulation, or proclamation --should also be examined to determine the scope of its authority includes the authority to engage in IRCIS hosting and operational activities.

"Amending" the existing authority of an agency of government may not be a trivial task; depending on the nation's constitutional requirements and any terms of an existing authorizing statute, permitting a role in an IRCIS entity (whether founding, participating as a member or simply receiving reports or data from an IRCIS entity) for an agency of government could require a legislative action, a proclamation by the

national executive, or, if within the scope of the agency's existing authority, might be authorized by a simple declaration of the agency head (minister or secretary) or his/her delegate.

3. Dedicated Information Sharing Activity: IRCIS Structures

a) "Center of Excellence"

The Center of Excellence model is most commonly associated with academic institutions, such as universities, and other NGOs. In the U.S., the designation of an institution as an "Academic Center of Excellence" in a discipline may in fact be a statutory designation made only upon a finding by an agency of government or other authority that an institution possesses specific attributes (e.g., course offerings, publishing, research accomplishments). For example, the U.S. Homeland Security Act includes a provision allowing the Secretary, upon recommendation, to designate a university as a "Homeland Security Academic Center of Excellence." [7]

The DoD also has programs of Centers of Excellence in fields such as Health Sciences. The NSA sponsors and supports Information Assurance (IA) centers of excellence involving hundreds of universities organized under 13 centers on topics such as Imagery.[8]

In 2008, the government of Estonia, in the wake of the highly publicized attacks against its network infrastructures from hosts in neighboring Russia, established a "Cyber Center of Excellence", which was subsequently recognized (as distinct from "adopted") by NATO as "a NATO Cyber Center of Excellence." In that capacity, it has conducted a program of research and publishing, and has hosted 4 highly respected annual international conferences. However, the Estonian Cyber Center of Excellence is NOT actively engaged in the management of real-time threat/attack information sharing.

NATO's own official watch-and-warning network defense capability in this area is conducted by its still-forming NATO Cyber Incident Response Center (NATO CIRC), an

---

[7] Section 308 of the Homeland Security Act of 2002, Pub. L. 107-296, (HSA) (6 U.S.C. §188), as amended by the Consolidated Appropriations Resolution, 2003, Pub. L. 108-7, div. L, § 101(1), directs the Secretary of Homeland Security to sponsor extramural research, development, demonstration, testing and evaluation programs relating to homeland security. As part of this program, the Department of Homeland Security (DHS) is to establish a university-based center or centers for homeland security (Homeland Security Centers of Excellence or Centers).

[8] See NSA Academic Centers of Excellence. http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml (last visited 5/2/2012)

engineering-based capability being developed at NATO Headquarters and expected to be fully operational during 2012.[9]

b) ISAC Capability—Information sharing and analysis centers

ISACs have become one of the most visible forms of CIS organizations in the U.S.. Because 18 present ISACs have official recognition by the U.S. DHS through its Partnership for Critical Infrastructure Security program, which itself is comprised of the Sector Coordinating Councils for each industry sector, ISACs have gained visibility beyond the U.S. as well. ISACs were initially developed in 11 "critical infrastructure" sectors in the late 1990s following the issuance of PDD-63.

Later, following the 9/11 attacks in 2001, two Homeland Security Presidential Directives, HSPD-5 and HSPD-7, provide specific direction to the newly established DHS to support the maintenance of the sector-specific "ISAC" functions in critical infrastructure sectors, and designated agencies of government with preexisting relationships and responsibilities regarding these sectors as "sector specific agencies" to engage with and support the industry information sharing activities of the ISACs.[10]

As discussed in Section IV (B) (3) above, two ISACs (the Telecommunications ISAC, originated as a spin-off of the National Coordinating Center, an NSTAC affiliate hosted at DoD's Defense Information Systems Agency (DISA), and the electric power sector ISAC, developed under the North American Electricity Reliability Council (NERC), an affiliate of the Department of Energy) both predate the 1998 PDD-63, and served as models for the private sector staffed Information Sharing architecture across the economy.

In each instance of the present 18 U.S. industry ISACs, the constituency of the ISAC consists of companies within the industrial sector. ISACs are organized and managed by the sector, and provide their data both to their industry sector peers and to their sector specific agency.

The present alignment of U.S. critical infrastructure sectors with their coordinate sector specific agencies is set out in the **following table from the U.S. Department of Homeland Security.** Each of the identified sectors has a Sector Coordinating Council, which is affiliated with the Partnership for Critical Infrastructure Security. Sixteen of the eighteen independent ISACs for each critical infrastructure[11] sector are affiliated through the ISAC Council.

---

[9] NATO Cyber Incident Response Center,
http://www.nato.int/cps/en/natolive/news_85161.htm?selectedLocale=en
(last visited 7 May 2012)

[10] HSPD-7 2003, at http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1

[11] ISAC Council,
http://www.isaccouncil.org/index.php?option=com_content&view=article&id=83&Itemid=195

Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture[1] Department of Health and Human Services[2]	Agriculture and Food
Department of Defense[3]	Defense Industrial Base
Department of Energy	Energy[4]
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water and Water Treatment Systems
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cyber Security and Telecommunications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard[5]	Transportation Systems[6]
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

c) CERT-Computer/Cyber Emergency Response Team

CERTs have a relatively long history in the U.S. and have increasingly been developed outside of the U.S. The first "CERT" format was initiated at Carnegie-Mellon University (CMU) in 1988 and for many years functioned under the CMU Software Engineering Institute's (SEI) Federally Funded Research and Development Center (FFRDC). CMU/SEI continues to operate CERT, CERT/CC and CSIRT (Computer Security Incident Response Team).[12]

The important feature about CERTs is their grounding in hard network engineering and the orientation towards real-time incident identification and response, based in an operations-center environment. The information they produce—and presumably, share-is intended to reflect this technical rigor.

When the European Union's ENISA Center was under development, it was frequently described as the "EU's CERT" because of its planned maintenance not only of a network of information sharing vehicles, but because it would root that information and develop data in an engineering-based 24/7 operations center.

The CERT architecture for a CIS entity is appropriate when significant engineering resources are available and a commitment to a 24/7 watch and warning center can be supported by the IRCIS participants.

(1) Other approaches to establishing CIS

A number of other options are available to nations and their agencies in determining how to establish a CIS Center. They all involve "hybrid" approaches, borrowing elements from various structures discussed above. As discussed elsewhere in this report, the issue for IRCIS organization developers is not being bound to any particular architecture, but to establish an effective platform for actionable timely CIS.

Notwithstanding that these hybrid structures may be challenging in their initial set-up, if they offer organizers the structure and flexibility they seek to maximize effective information sharing, that objective should control their decision.

[12] CMU/SEI/CERT-CC See FAQs at http://www.cert.org/faq/cert_faq.html

4. Multi-function CIS architectures

Multi-function CIS architectures can include selected elements of Center of Excellence, CERT-based information sharing and incident response, cyber forensics, law enforcement support, intelligence gathering/sharing and research. Agencies of government seeking to maximize the capabilities of a CIS function may choose to "bundle" several or all of the various capabilities discussed in this Report, into a single capability. This ambitious architecture could, as with the EU's ENISA, or the new International Telecommunications Union Cyber Center in Kuala Lampur evolve into a fully staffed agency, employing dozens or hundreds of professional staff across many disciplines and carrying out multiple missions related to the organizers objectives.

VII. Analysis of Available Legal Framework Instruments and Creation of "new" instruments to support Cyber ISE relationships

A. Operationalizing the Legal Framework Concepts

The forgoing discussion is dense with legal and policy concepts which are important during the decision-making process of the IRCIS organization. Once these decisions are made, however, and the IRCIS organization is up, running and operational, these considerations normally fade into the background, and the actual functioning of the ICRCIS activity, and its ability to serve the organizers' objectives in sharing actionable information about Cyber events is the paramount consideration.

There may, nevertheless, be instances both during the development period and once established when it is useful to quickly characterize the essential features of the IRCIS organization.

In addition, as the entity matures, it may be desirable to evolve legal framework elements; for example, an IRCIS entity comprised only of industry entities may wish to add government agencies as participants, or vice-versa. Or, an entirely domestic, single nation organization may seek to join with neighboring states. The following sections assist in characterizing the key elements of an existing IRCIS activity, both during development and during operations, and suggest approaches which may be useful in evolving an entity to account for expanded membership or other changes in scope and structure.

1. Summary Analytical Framework Template

The following template utilizes an existing Information Sharing Entity, the U.S. IT ISAC as an example of the summary analytical process, which provides a "snap shot" of the essential characteristics of an IRCIS entity and permit a prompt determination if further development is required or useful in supporting the operations of the entity.

Framework Analysis for: **U.S. Information Technology Information Sharing & Analysis Center** (*IT ISAC Articles and By-laws documents*)		
CRITERION	**SOURCE**	**VALUE**
IRCIS Pedigree		
Nationality		U.S.
Founded		1998
Shares with	E,O., Statute	DHS, other designated government agencies; ISAC Members; PCIS Members
Attributes		
Legitimization/delegation	PDD-63 (1998)	Sector representative of structure authorized by E.O. for all critical infrastructures
Participants	LLC Charter (Comm. of Virginia)	Domestic corporate membership entity (state charter: "Limited Liability Company"
Scope	Charter	For-profit companies within industry sector
Structure	Charter	Information sharing & analysis center
Governance	Charter/By-laws	Elected Board of Directors under state charter; By-laws
Finance	Charter	Dues paid by members
Operating Rules	By-laws	
Affiliations	Statute	Homeland Security Act of 2002 defines ISAC responsibilities; participation in cross-infrastructure "Partnership for Critical Infrastructure Security" hosted by Department of Homeland Security
Key organizing steps *[applicable to IRCIS entities under development]*		
Parties		IT sector private companies
Authority Document		[2-step] National government: "E.O." PDD-63 (1998); Entity: Articles of Incorporation (LLC)
FORM		Information Sharing &Analysis Center (ISAC)
Operating Rules		By-laws document

a. Alternate structures

Among the most flexible means of structuring organizational relationships in complex technical areas are two devices common in the U.S.

One is essentially contractual, and involves relationships between agencies of government and private institutions (both corporations and NGOs (including universities)): that is the Cooperative Research and Development Agreement or "CRADA".

The other instrument offering great flexibility, especially between governments, or between agencies of government, or agencies of government of multiple nations, is the Meomorandum of Agreement- "MoU" described above in relation to Treaty agreements

Further benefits and utility of each are discussed briefly here.

(1) CRADA

CRADAs were first authorized by Congress under a statute, the National Cooperative Research Act of 1984, [13] and became the means under which innovative structures and "national challenge" and "hard problem" activities could go on under "sole source" contracts with the U.S. Federal government and private entities, including groups of market competitors who might otherwise be barred from collaboration by the antitrust laws.

The CRADA form is particularly suitable as an authorizing instrument for IRCIS activities involving both agencies of government and private industry, as well as entities consisting principally of private companies which are competitors, either as an industry-only organization or organized under the "hosting" or primary reporting/information sharing recipient.

(2) MoUs

As discussed earlier in connection with Treaties, MoUs may be of particular utility to pairs or groups of nations which seek to commit to a particular action, such as an IRCIS organization, but which for any reason determine that the formality of a treaty

[13] First emerging as "Cooperative Research Center" agreements between NSF and universities under the Stevenson-Wydler Technology Innovation Act of 1980 (P.L. 96-480), CRADAs became more common after the founding of the two Austin centers, MCC and SemiTech in 1986, both including many competitive semiconductor companies operating under one roof, pursuant to the National Cooperative Research Act (P.L. 98-462) in 1984. This legislation clarified the antitrust laws and eliminated treble damage awards for those research ventures found in violation of the antitrust laws if prior disclosure (as defined in the law) has been made. Between 1985 (when the law went into effect) and August 2009, 1,343 joint ventures have filed with the Justice Department. The provisions of the National Cooperative Research Act were extended to joint manufacturing ventures by P.L. 103-42, the National Cooperative Production Amendments Act of 1993.

is not appropriate (considerations might include whether development of a treaty instrument may be too time consuming, too "permanent", or there may be uncertainty as to duration or other operational or structural considerations).

Whatever the reason the parties determine a treaty is unsuitable as a legal instrument, the MoU offers flexibility in structure, terms and execution, as well as relative informality, making it a highly useful option.

b. Essential steps in creating a new CIS Entity

This Report has described the elements of a deliberative process which should be engaged in by any parties contemplating the establishment of a CIS entity. The steps are summary; they embody a substantial number of considerations discussed in the Report, but their essential elements may be described by the following four key elements.

Once the desired operating objectives for the ISE are defined by the organizing party, the ensuing process of establishing the entity is not prescribed or specific, but it will normally incorporate at least the following **four elements which are necessary considerations in the establishment of the entity**:

1. Identification of the parties to the organization:

- nation states, or their proxies (e.g., an agency of government)
- Non-governmental organizations
- Universities (national, public or private)
- industry organizations
- individual companies

2. Selection of the major framework document:

- a treaty or non-treaty agreement (nations or agencies of government)
- a Memorandum of Understanding or Agreement
- a contract
- informal governmental instruments

3. Selection of operating structure:

- Information Sharing Agency
- Information Sharing and Analysis Center
- Center of Excellence
- Hybrid entity
- Informal entity: "coalition" "consortium" "council"

4. Selection of an operating instrument reflecting the chosen structure, and considerations analyzed in Section IV (A):

- Charter

- By-laws
- Operating agreement, Concept of Operations (CONOPS)

VIII. Recommendations

A. Process

Identify and execute the four key minimum elements (Sec.7(d)) essential to establishment of the proposed ISE: constituent parties, authorizing legal instrument, operating structure, operating guidance.

- Identify the participants/members of the organization
- Select the form of the organization
- Select and execute an authorizing instrument
- Define and memorialize the operating rules & guidance (both structural rules [leadership, divisions of labor (committees, other roles)] and substantive rules [what information will be shared, how will it be structured for sharing, with whom will it be shared]).

B. Formality

Once a commitment among negotiating parties is reached, only those instruments/legal formalities required to express their intent and bind their participation need be employed. Minimalism will reduce complexity and permit a focus on the key mission of the entity: sharing of actionable information about cyber events.

C. Use of existing agreements

Where the IRCIS function is proposed to be hosted from an existing organization, care should be taken to alter existing authority appropriately to insulate the function from challenges to its legitimacy and credibility.

Particular attention should be paid to associating amendments and additions or changes to existing authority with the proper instrument, and to utilize the proper means (e.g., amendment of existing statute or regulation, proclamation, statement by head-of-agency, contractual or MoU amendment). In the case of existing contracts and similar documents, obtaining the consent of all existing parties may be essential to making any agreement effective).

Appendix 1: Organizations Hosting/Sponsoring Cyber Information Sharing Activity

Title	THAILAND: Computer Emergency Response Team
Organization	National Electronics and Computer Technology Center (NECTEC)
Description	In April 2001, the National Electronics and Computer Technology Center (NECTEC) established Thai Computer Emergency Response Team (ThaiCERT) as an electronic discussion forum on cyber security. Its members include governmental agencies and companies in the
Website	http://www.thaicert.nectec.or.th

Title	JAPAN: Establishing the government entities to address information security issues
Organization	National Information Security Center
Description	To address the issue of information security, the Information Security Policy Council (ISPC) and the National Information Security Center (NISC) has been established in Japanese Government since 2005. ISPC has been established under the IT Strategic Head
Website	http://www.nisc.go.jp.eng

Title	KOREA: Self-Purification for Clean Internet
Organization	Korea Internet and Security Agency
Description	KCC and KISA started the 'Making a Beautiful Internet World' campaign to promote sound internet culture, and to improve information credibility by protecting copyright, privacy and security, managing search quality, and bringing openness to online communications
Website	
Coverage	National

Title	SWITZERLAND: Public Private Partnership in the field of Information Assurance
Organization	Foundation InfoSurance
Description	InfoSurance is a Foundation funded by the federal government and the industry. The focus of the activities is Awareness, Prevention and Networking in Switzerland in the field of Information Assurance.
Website	http://www.infosurance.ch/
Coverage	National

Title	EU: ENISA -the European Network and Information Security Agency
Organization	European Commission
Description	As communication networks and information systems grow ever more complex, they become increasingly subject to accidents, mistakes and malicious attacks, challenging progressively the benefits expected from the development of information and communication
Website	http://enisa.europa.eu/
Coverage	Regional

Title	UAE Computer Emergency Response Team (aeCERT)
Organization	Telecommunications Regulatory Authority (TRA)
Description	The United Arab Emirates Computer Emergency Response Team (aeCERT) is the cyber-security coordination center in the UAE. It will be established by the TRA as an initiative to facilitate the detection, prevention, and response of cyber security incidents.
Website	http://www.aecert.ae
Coverage	National

Title	OMAN: ITA signs contract to establish Omani National Computer Emergency Response Center (CERT)
Organization	Information Technology Authority (ITA)
Description	The Information Technology Authority (ITA) of Oman signed a contract with E-COP PTE Ltd., Singapore (E-Cop) to set up the National Computer Emergency Response Center (CERT) of the Sultanate. H.E. Mohammed Nasser Al Khasibi, Secretary General, Ministry
Website	http://www.ita.gov.om/ITAPortal/MediaCenter/NewsDetail.aspx?NID=250
Coverage	National

Title	ETHIOPIA: Regional Strategy Guidelines for CEEAC and CEMAC.
Organization	United Nations Economic Commission for Africa (UNECA)
Description	The activities are aimed at adopting a regional strategy on the Information and knowledge society for the two regional integration institutions of Central Africa, which are CEEAC and CEMAC.
Website	
Coverage	Regional
Status	Ongoing

Appendix 2: MITRE Support for Development of Policy Guidance, Legal Instruments and Governance Documents for Information Sharing Organizations

MITRE staff includes recognized subject matter experts skilled in technology issues relevant to Cyber Information Sharing Organizations. MITRE staff also includes individuals with expertise in the specific policy and legal framework requirements detailed in this Report, which will define the **authority, structure, scope of operations and operating rules** of national or sector-specific Cyber Information Sharing activities.

A. Support to Organizers: Policy and Legal Framework Capabilities

This Report makes it clear that an essential precursor to a viable CIS activity is the development of an appropriate framework of policy and procedures for the organization.

MITRE support can initially aid organizers of IRCIS entities on the selection of an operating form for the Cyber Information Sharing entity.

Once that decision is made, MITRE can support organizers' decisions regarding the appropriate legal framework instruments to employ and the essential contents of those instruments, the communication of those decisions to stakeholders and other interested parties. MITRE can also assist the new entity in gaining visibility with other international bodies' Cyber Information Sharing activities, and participation in organizations representing IRCIS entities.

[Documentation describing MITRE professional staff credentials is available upon request.]

These capabilities include MITRE direct support for the following steps encompassing the formulation, development and initial operations of a national CIS organization:

1. Selection of IRCIS entity operating structure

The selection of an entity operating structure will be the product of a number of factors, including the desired *scope of the entity* (number of participating nations/organizations) and the *complexity of cyber information to be shared* (a basic "watch and warning" capability will require significantly less structure and complexity than an entity seeking to do cyber forensic analysis on observed events/attacks and to provide participants with actionable intelligence products.

Based on interviews with entity organizers, MITRE Subject Matter Experts (SMEs) can conduct an assessment and develop an options document which provides a basis for informed selection of an operating structure, including options for evolution or

migration of the structure as operational experience is accumulated or the number of organizational participants expands.

2. Drafting and publication of a high level organizing instrument

NATIONS: MITRE staff can support deliberations leading to the selection of the instrument type under which of the information sharing organizations will operate. For state-based or agency-based entities this will depend on the selected operating structure: if a multi-lateral multi-nation entity is contemplated, then at a minimum the organizing authority will be a MoU prepared by the originating state(s), in consultation with anticipated partner states, and often, capable of being executed pendant to an existing multilateral agreement among the parties.

If no such prior treaty or arrangement exists, the parties have a choice of alternative means of establishing an entity. MITRE staff can assist with the drafting and management of execution of many types of multi-party instruments.

These include: **exchange of diplomatic letters,** (typically between Foreign Ministers or by resident ambassadors in each capitol], representing more formality than an MoU but less binding commitment and rigor of formation than a treaty; proceeding under the less formal **MoU or similar agency-to-agency arrangement**, or a simple **multi-party agreement expressed in an exchange of letters** by authorized representatives . The MoU or letter form offers the convenience of execution, permits the easy inclusion of non-government participants in the Information Sharing entity, and offers the benefit of relative ease of repudiation should a party seek to withdraw.
NGOs: For information sharing organizations established under other-than-governmental authority, MITRE staff can manage development and draft necessary national operating authorities such as Charters or Articles of Incorporation. Similarly, for industry, university, NGO or other Information Sharing entities not principally hosted by government, MITRE staff can support the negotiation, drafting and execution of appropriate contractual instruments. This support may include the identification of and management of the services provided by local counsel and other experts necessary to assure the most appropriate structure.

3. Drafting Operating Rules, Charters, By-laws and similar instruments

MITRE's SMEs have extensive experience in the support of government, NGO and private sector entities' governance structures, including the analysis of desired organizational structure, intended governance models and documentation to support these.

Examples of By-laws, MoU and other operating instruments are available to assist sponsoring nations in making determinations regarding the optimal form to conduct ISE operations. MITRE SMEs can provide recommendations supported by analyses

based on individual circumstances, and can draft specific language to achieve desired objectives.

D. Support for Cyber ISE Operations

In addition to the foundational activities of developing and gaining approval for legal framework documentation for a CIS entity, MITRE technical professionals are also capable of providing foundational and continuing technical support for ISE operations. MITRE staff includes recognized SMEs skilled in technology areas essential to the effective operations of a CIS Organization, such as network architecture, threat identification and analysis, incident management, data base security and network forensics.

MITRE staff can provide support for the development of these capabilities during the organizational phase of an ISE, as well as support for the operating programs, on a participatory or consulting basis.

Appendix 3: Considerations in development of IRCIS Framework

The following issues may be present during the consideration by entity founders and sponsors regarding the form of legal instrument to select, the nature of entities participating in a sharing activity, and for sharing organizations based on existing structures, the extent of modification necessary to support an information sharing environment.

Nature of Organizing Parties and Proposed Entity

What form does the founding group wish the IS entity to take?

Is the form appropriate for the organizers and proposed operating model? (e.g., Are a group of companies proposing to operate as a "National Cyber Security Research and IS Center" ?)

Will the IRCIS be individually structured—perhaps not relying initially on framework instruments ?

The responses to these lines of inquiry, and other foundational decisions may define the scope of SME support required during founding and launch phase of IRCIS development. Other considerations include options regarding nature, number and representation of participants, level of authority of management or other IRCIS leadership, and duration of entity existence (e.g., permanent, term of years).

Considerations Regarding Existing Programs

Does the proposed entity qualify for financial or structural support under existing programs?

Examples: Warsaw Initiative, Reconstruction Funding, Regional development Agreements, non-DoD mechanisms (e.g., DoS, DoD-affiliated; USAID Training programs

Will existing legal framework instruments support establishment of an IRCIS?

Do existing instruments reflect legal sufficiency for an IRCIS entity ?

1. **Legal sufficiency to support consulting role among participants ?**
2. **FFRDC implications: May MITRE be the recipient of consulting fees under an existing instrument ?**

For new instrument(s):

3. **Overall assessment: "Fit" : adapting instrument to opportunity: least complex structure to accomplish program objectives**
4. **Legal sufficiency for consulting role**
5. **Financial structure**
6. **FFRDC impact**

An organization's legal framework instrument will define its structure and mode of agreement. These will be dictated by specific aspects of the organizational situation.

Appendix 4 Acronyms

ACSIC	Abu Dhabi Security Information Center
APEC	Asia-Pacific Economic Council
APT	Advanced Persistent Threat
CIRC	Cyber Incident Response Center
CBI	Caribbean Basin Initiative
CERT	Computer (or Cyber) Emergency Response (or Readiness) Team
CERT/CC	CERT Coordination Center
CIS	Cyber Information Sharing
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CMU	Carnegie Mellon University
CND	Computer Network Defense
CNO	Computer Network Operations
CoE	Center of Excellence
CONOPS	Concept of Operations
CRADA	Cooperation Research & Development Agreement
CSIRT	Computer Security Incident Response Team
DISA	Defense Information Systems Agency
DHS	Department of Homeland Security
DoD	Department of Defense
DoJ	Department of Justice
ENISA	European Network Information Security Agency
EU	European Union
FCN	Friendship, Commerce and Navigation
FFRDC	Federally Funded Research and Development Center
FS	Financial Services
GAO	Government Accountability Office
GSOC	Government Security Operations Center
IA	Information Assurance
ICT	Information and Communications Technology
INTERPOL	International Criminal Police Organization
IRCIS	International Regional Cyber Information Sharing
ISAC	Information Sharing and Analysis Center
ISE	Information Sharing Environment
ISO	Information Sharing Organization
ITU	International Telecommunications Union
JCS	Joint Chiefs of Staff
JTF-GNO	Joint Task Force – Global Network Operations
MoA	Memorandum of Agreement
MoD	Ministry of Defense
MoU	Memorandum of Understanding
NAFTA	North American Free Trade Agreement

NATO	North Atlantic Treaty Organization
NERC	North American Reliability Council
NCC	National Coordinating Center of the National Communication Systems
NGO	Non-Government Organization
NOC	Network Operations Center
NSA	National Security Agency
NSTAC	National Security Telecommunications Advisory Committee
SEI	Software Engineering Institute
SME	Subject Matter Expert
SOC	Security Operations Center
US	United States